

# Products

## Connectivity



### Internet

*Powered by over 150 Providers*



### Wireless

*Choose from AT&T, T-Mobile & Verizon*



### SD-WAN

*Powered by VMware*



### Cloud Wi-Fi

*Powered by Sophos*

## POTS Alternative



### Alert+

*Fire, life & safety lines with voice*



### SD-WAN POTS

*Managed Plain Old Telephone Service with Software-Defined WAN*

## Misc Services



### Fax Solutions

*Cloud, UCaaS, VoIP & POTS*



### Managed

*Infrastructure hardware, switches, routers, firewall & more*



### TSaaS

*Site assessment, cabling & hardware installation*

## Collaboration



### Microsoft Teams Integrations

*Bring everything together in Teams*

## Voice



### Hospitality Voice

*Easy to manage VoIP guest services phone system*



### Integrated Voice

*Analog-to-VoIP, IP-PRI & SIP Trunking*



### Talk

*Local, LD, International & Toll-Free*



### UCaaS

*Unified Communications*

## Security



### Defend

*Cloud Security Powered by Zscaler*

## Lingo's Odds & Ends

Partner portal: <https://www.mybullseyeaccount.com/login>

Quotes: [partnersupport@lingo.com](mailto:partnersupport@lingo.com)



# TALK

*Local, Long Distance and Toll-Free*

## - POTS Lines & Aggregation

### What is POTS?

**P**lain **O**ld **T**elephone **S**ervice (POTS), or plain ordinary telephone service, is a retronym for voice-grade telephone service employing analog signal transmission over copper loops.

- Can offer POTS lines in most markets across the US
- Bring any and all POTS lines over to Lingo
- Remember Lingo's **P2V**
- Check for availability...less & less true POTs (Copper) options. Should be looking at migrating to VoIP options, such as hosted voice, integrated voice, or POTs-in-a-Box replacement (EPIK)



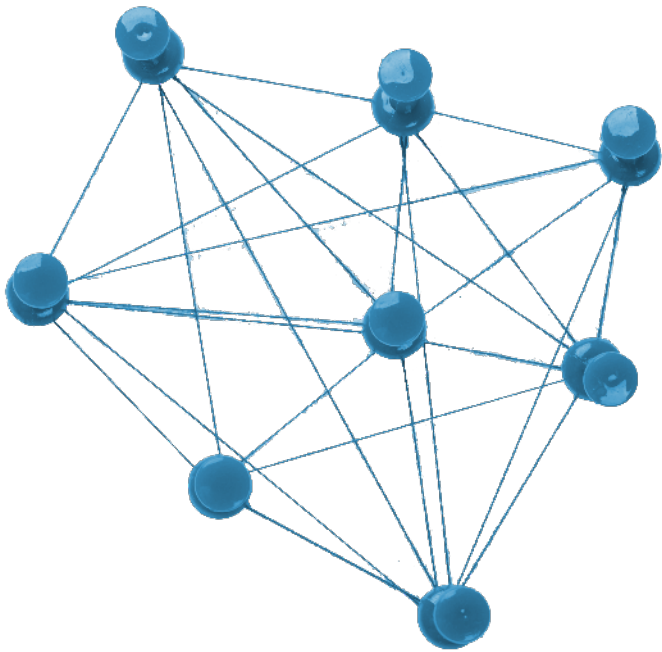
# TALK - POTS Lines & Aggregation

*Local, Long Distance and Toll-Free*

## What is POTS?

**P**lain **O**ld **T**elephone **S**ervice (POTS), or plain ordinary telephone service, is a retronym for voice-grade telephone service employing analog signal transmission over copper loops.

- Can offer POTS lines in most markets across the US
- Bring any and all POTS lines over to Lingo
- Remember Lingo's **P2V**
- Check for availability...less & less true POTs (Copper) options. Should be looking at migrating to VoIP options, such as hosted voice, integrated voice, or POTs-in-a-Box replacement (EPIK)



# CONNECTIVITY





# INTERNET - Bandwidth Aggregation

Powered by over 150 providers

Lingo has partnerships with over 150 underlying providers. Enabling best options for delivering the needed bandwidth at locations all over the United States.

- T1
- Fiber Optic lines
- EOC
- DSL
- Cable
- Fios
- AT&T U-Verse
- Microwave (WISPs)
- LTE - all Carriers
- Satellite

Powered by Partners like:

COX



Viasat

EarthLink

WOW!



suddenlink

kinetic  
by windstream

/Sparklight

T Mobile

TPX  
COMMUNICATIONS

zayo

Spectrum

Sprint

CenturyLink

Frontier

comcast

Google Fiber

LUMEN

Rise  
Broadband



# WIRELESS - Lingo's Cellular Options

*Powered by AT&T, Verizon and T-Mobile*

## Powered by Partners:



**T Mobile**



## Options:

- LTE Options
- 5G Options
- Pooled Plans
- Pay per MB Plans
- Modems
- Routers
- BYOD



# WIRELESS

*Powered by AT&T, Verizon and T-Mobile*

Our wireless failover solution supports your voice communications and any mission-critical applications that are dependent on Internet connectivity with a cost effective & affordable data plan.

## Solution Highlights:

- Cross carrier pooling provides the best service available regardless of location
- Both “Pooled” and “Pay-As-You-Go” options available
- A wireless data plan is easily deployed and managed via the cloud for easy integration with your existing systems.
- Avoid expensive cabling costs for seasonal or rapid deployment of Internet connectivity when using wireless as your primary data source
- Be anywhere your customers are by easily deploying pop-up retail/store-in-a-store/kiosks
- Power your digital signage and make frequent updates on your specials



## What is SD-WAN?

**SD-WAN** is an acronym for **S**oftware-**D**efined Networking in a **W**ide **A**rea **N**etwork. SD-WAN simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism.

## Reasons to utilize SD-WAN:

- MPLS Replacement
- Bandwidth Aggregation
- Network Enhancement
- HIPAA & PCI Compliance
- Auto Failover & failback
- Application Control



# SD-WAN - Right-size Your Edge

Powered by VMware

Powered by  
**vmware**<sup>®</sup>  
by **Broadcom**

vmware <sup>®</sup>		VCE	TUNNEL SIZE OPTIONS									
Max Throughput	Max Tunnels	Edge/BW	10 M	30 M	50 M	100 M	200 M	500 M	1 G	2 G	10 G	40 G
350 Mbps	50	Edge 710-W	*	*	*	*	*	*				
350 Mbps	50	Edge 710-5G	*	*	*	*	*	*				
750 Mbps	100	Edge 620	*	*	*	*	*	*	*			
1 Gbps	400	Edge 640				*	*	*	*	*		
1.5 Gbps	400	Edge 720	*	*	*	*	*	*	*	*	*	
2 Gbps	800	Edge 680				*	*	*	*	*		
2.5 Gbps	800	Edge 740				*	*	*	*	*	*	
2.5 Gbps	4000	Edge 3400					*	*	*	*	*	
5 Gbps	6000	Edge 3800							*	*	*	*



# SD-WAN - VCE-510 & VCE-510-LTE

Powered by VMware

Powered by  
**vmware**<sup>®</sup>  
by **Broadcom**



## SD-WAN Edge

- (4) LAN / WAN Assignable RJ-45 ports
- (2) USB 3.0 ports
- LTE SIM slot (Optional LTE)
- Integrated Wi-Fi
- 100 Mbps Max Throughput



# SD-WAN - VCE-610

Powered by VMware

Powered by  
**vmware**<sup>®</sup>  
by **Broadcom**



## SD-WAN Edge

- (6) LAN / WAN Gigabit RJ-45 ports
- (2) SFP WAN Ports
- (2) USB 3.0 ports
- Integrated Wi-Fi
- 350 Mbps Max Throughput



# SD-WAN - VCE-710-W

Powered by VMware

Powered by  
**vmware**<sup>®</sup>  
by **Broadcom**



## SD-WAN Edge

- (4) LAN / WAN Gigabit RJ-45 ports
- (1) 2.5 Gbps SFP Port
- (1) USB 3.0 port
- Integrated Wi-Fi 6
- 350 Mbps Max IMIX Throughput





# SD-WAN - VCE-710-5G

Powered by VMware

Powered by  
**vmware**<sup>®</sup>  
by **Broadcom**



## SD-WAN Edge

- (4) LAN / WAN Gigabit RJ-45 ports
- (1) 2.5 Gbps SFP Port
- (1) USB 3.0 port
- Dual 5G SIM slots
- Integrated Wi-Fi 6
- 350 Mbps Max IMIX Throughput



# SD-WAN - VCE-720

Powered by VMware

Powered by  
**vmware**<sup>®</sup>  
by **Broadcom**



## SD-WAN Edge

- Intel Atom 4C AZB processor
- 16GB DDR5 Memory
- 256GB eMMC Storage
- (6) LAN / WAN Gigabit RJ-45 ports
- (2) 10 Gbps SFP+ Ports
- (2) USB 3.0 ports
- Tunnel Scale up to 400



# SD-WAN - VCE-740

Powered by VMware

Powered by  
**vmware**<sup>®</sup>  
by **Broadcom**



## SD-WAN Edge

- Intel Atom 8C AZB processor
- 16GB DDR5 Memory
- 256GB eMMC Storage
- (6) LAN / WAN Gigabit RJ-45 ports
- (2) 10 Gbps SFP+ Ports
- (2) USB 3.0 ports
- Tunnel Scale up to 800



# SD-WAN - VCE-620

Powered by VMware

Powered by  
**vmware**<sup>®</sup>  
by **Broadcom**



## SD-WAN Edge

- (6) LAN / WAN Gigabit RJ-45 ports
- (2) SFP WAN Ports (supports SFP+ 1/10Ge modules)
- (2) USB 3.0 ports
- Integrated Wi-Fi
- 750 Mbps Max Throughput



# SD-WAN - VCE-640

Powered by VMware

Powered by  
**vmware**<sup>®</sup>  
by **Broadcom**



## SD-WAN Edge

- (6) LAN / WAN Gigabit RJ-45 ports
- (2) LAN / WAN 1G/10G SFP+ ports
- (2) USB 3.0 ports
- Integrated Wi-Fi
- 1 Gbps Max Throughput



# SD-WAN - VCE-680

Powered by VMware

Powered by  
**vmware**<sup>®</sup>  
by **Broadcom**



## SD-WAN Edge

- (6) LAN / WAN Gigabit RJ-45 ports
- (2) LAN / WAN 1G/10G SFP+ ports
- (2) USB 3.0 ports
- Integrated Wi-Fi
- 2 Gbps Max Throughput



# SD-WAN - VCE-3400

Powered by VMware

Powered by  
**vmware**<sup>®</sup>  
by **Broadcom**



## SD-WAN Edge

- (6) LAN / WAN Gigabit RJ-45 ports
- (2) LAN / WAN 1G/10G SFP+ ports
- (2) USB 3.0 ports
- 2.5 Gbps Max Throughput



# SD-WAN - VCE-3800

Powered by VMware

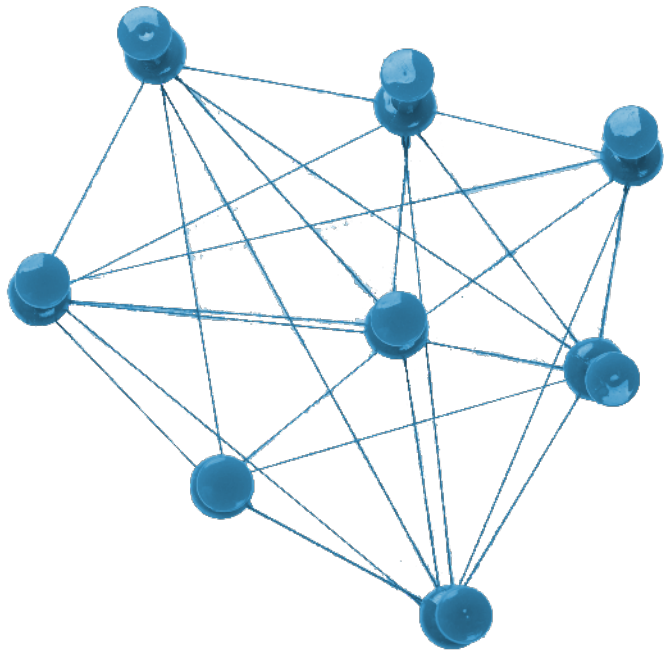
Powered by  
**vmware**<sup>®</sup>  
by **Broadcom**



## SD-WAN Edge

- (6) LAN / WAN Gigabit RJ-45 ports
- (2) LAN / WAN 1G/10G SFP+ ports
- (2) USB 3.0 ports
- 5 Gbps Max Throughput





# SECURITY SOLUTIONS



# What is a Managed Firewall?

In computing, a firewall is a network security system that monitors, and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

With Lingo's Managed Firewall option, we can manage one of our onsite or cloud-based firewall options for you. All of Lingo's Firewalls options can be self-managed via their appropriate cloud portals.

## Reasons to utilize a Managed Firewall:

- Have limited staff
- Don't have time to keep up on product upgrades & changes
- Rather have product Subject Matter Expert handle for me



# Firewall & Security Options

---



**DEFEND**

*Cloud Security Powered by Zscaler*



# What is a Next Generation Firewall?

---

A next-generation firewall is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functions, such as an application firewall using in-line deep packet inspection, an intrusion prevention system.

## Reasons to utilize a NexGen Firewall:

- Network Security
- Site-to-site VPN
- Client VPN
- HIPAA & PCI Compliance
- Auto Failover & failback
- Better Data Control

**Market Leader** **300** of the Forbes Global 2000  
Nasdaq: ZS

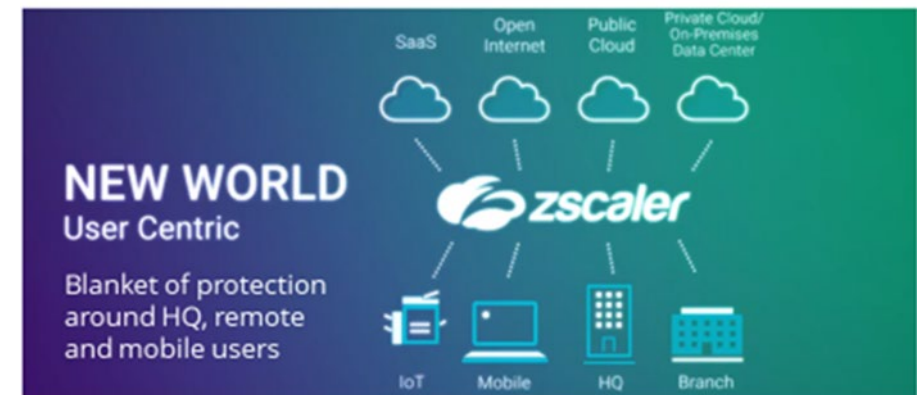
**Global Presence** **100+** data centers across 6 continents

**Proven Scale** **60B+** transactions processed daily

**15X** what Google processes on a daily basis!



## Gartner SWG MQ



## Cyberthreat Protection

[Secure Internet Access \(ZIA\)](#)

[Secure Private Access \(ZPA\)](#)

[Zero Trust Firewall](#)

[Sandbox](#)

[Zero Trust Browser](#)

## Data Protection

[Web & Email DLP](#)

[Multi-Mode CASB](#)

[Endpoint DLP](#)

[Unified SaaS Security](#)

[Public Gen AI Security](#)

[Microsoft CoPilot Data Protection](#)

[DSPM](#)

[BYOD Security](#)

## Zero Trust Networking

[Zero Trust SASE](#)

[Zero Trust SD-WAN](#)

[Zero Trust Device Segmentation](#)

[Zero Trust Cloud](#)

[Zero Trust IoT/OT](#)

[Digital Experience \(ZDX\)](#)

## Risk Management

[Data Fabric for Security](#)

[Asset Exposure Management](#)

[Risk360](#)

[Unified Vulnerability Management](#)

[Deception](#)

[Breach Predictor](#)

[Identity Protection](#)

[External Attack Surface Management](#)

[Managed Threat Hunting](#)



# DEFEND - Cyberthreat Protection

Cloud Security Powered by Zscaler



**Zscaler Internet Access™** delivers the world's most deployed [security service edge \(SSE\)](#), built on [a decade of SWG leadership](#). Replace legacy network security solutions with zero trust for secure connectivity, a great user experience, and administrative visibility and control.

## Strengthen security without sacrificing performance



### Stay safe from ransomware and other threats

Minimize the attack surface, stop compromise, eliminate lateral movement, and prevent data loss.



### Reduce costs and complexity

Simplify your network with fast, secure, direct-to-cloud access that removes the need for edge and branch firewalls.



### Protect data

Prevent loss of data from users, SaaS apps, and the public cloud due to accidental exposure, theft, or [double extortion ransomware](#).

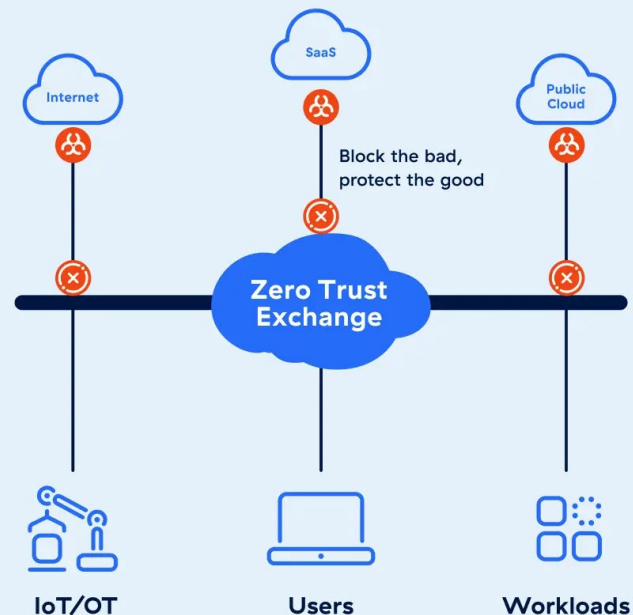


### Secure your hybrid workforce

Empower employees, customers, and third parties to securely access web apps and cloud services from anywhere, on any device—with a great digital experience.

## Zscaler Zero Trust Exchange Platform

250K Unique Daily Security Updates





# DEFEND - Cyberthreat Protection

Cloud Security Powered by Zscaler



## Zscaler Internet Access™

### KEY OFFERINGS

#### Secure Web Gateway (SWG)

Deliver a safe, fast web experience while detecting and preventing advanced attacks with real-time, AI-powered analysis and URL filtering.

#### Intrusion Prevention System (IPS)

Get complete protection against botnets, advanced threats, and zero days alongside contextual user, app, and threat intelligence.

#### Advanced Threat Protection

Stop advanced threats like botnets, ransomware, command-and-control, risky sharing, malicious active content, cross-site scripting, fraud sites, and more.

#### DNS Security

Filter risky and malicious domains and stop the use of DNS tunneling to transfer malicious payloads and sensitive data.

#### AI-Powered Phishing Detection

Know when patient zero phishing attacks are attempting to infiltrate your business with advanced AI-based inline detection.

#### AI-Powered Cloud Sandbox

Stop unknown malware inline with protections sourced from more than 400 billion daily transactions, including zero day threat quarantine.

#### Dynamic Risk-Based Policy

Stop active attacks and future-proof your defenses with continuous user, device, app, and content risk analysis fueling dynamic access controls.

#### AI-Powered Browser Isolation

Isolate web sessions in the user's own browser, delivering a near-native web experience without the risk of data loss or infection.



Cloud Security Platform Features	Secure Internet Platform (25 User Minimum)	ZIA Professional Bundle (10 Seat Minimum)	ZIA Business Bundle (10 Seat Minimum)	ZIA Secure Transformation Bundle (10 Seat Minimum)
High Availability Data Center Access w/latency SLAs	√	√	√	√
Security Policy Follows the User Anywhere	√	√	√	√
Traffic Forwarding - GRE, PAC, Proxy Chaining, IPSEC	√	√	√	√
Authentication - SAML, Secure LDAP, Kerberos	√	√	√	√
ZScaler Application for Mobile Traffic	√	√	√	√
Real-Time Reporting and Logging: 6 Months & Real Time Reporting	√	√	√	√
NSS Log (Nanolog) Streaming Service	Add-On	Add-On	√	√
NSS Log Recovery Web Mgmt Fee	Add-On	Add-On	Add-On	Add-On
NSS Log Recovery Firewall Mgmt Fee	Add-On	Add-On	Add-On	Add-On
SSL Inspection	Add-On	Add-On	√	√
Cloud Security Services				
Content Filtering	√	√	√	√
Standard Cloud Firewall: Rules by Location, IP, Ports & Protocols	√	√	√	√
Advanced Cloud Firewall & Logging	Add-On	Add-On	Add-On	√
Inline Anti-Virus & Anti-Spyware	Not Available	√	√	√
Advanced Threat Protection	Not Available	Add-On	√	√
Cloud Apps Control: Discover, Monitor & Control of Web Applications	Add-On	Add-On	√	√
Web Access Control	Add-On	Add-On	√	√
Bandwidth Control: Protect Key Apps & Limit Recreation Apps Policies	Add-On	Add-On	√	√
Mobile Applications & Devices: Granular Policy Setting & Reporting	Not Available	Not Available	√	√
Standard Cloud Sandbox: .exe and .dll from unknown & suspicious sites	Not Available	√	√	√
Advanced Cloud Sandbox: all file types, Quarantine Policy, Reports	Not Available	Add-On	Add-On	√
IPSec Encrypted VPNs	Not Available	Not Available	Not Available	Add-On
Basic DLP: True File Type Control by Users, Groups & Destinations	√	√	√	√
DLP Enhanced, ICAP for DLP, DLP Exact Data Match Daily Prioritization for Top 100 Domains, Dedicated Proxy Port on Entire Cloud	Add-On	Add-On	Add-On	Add-On



# DEFEND - ZIA Plan Pricing Example

Cloud Security Powered by Zscaler



	Monthly Per User Pricing									
Product Name	Up to 99	100+	500+	1,000+	2,500+	5,000+	10,000+	25,000+	50,000+	100,000+
Secure Internet Platform	\$1.80	\$1.13	\$0.81	\$0.75	\$0.68	\$0.63	\$0.57	\$0.53	\$0.51	\$0.45
ZIA Professional Bundle	\$5.04	\$3.31	\$2.50	\$2.10	\$1.91	\$1.75	\$1.60	\$1.47	\$1.37	\$1.27
ZIA Business Bundle	\$8.08	\$5.30	\$4.00	\$3.37	\$3.06	\$2.80	\$2.56	\$2.36	\$2.20	\$2.04
ZIA Secure Transformation Bundle	\$14.83	\$9.73	\$7.34	\$6.18	\$5.62	\$5.14	\$4.70	\$4.33	\$4.04	\$3.75
ZIA Enterprise License Agreement	Minimum 10,000 seats						\$7.68	\$6.11	\$5.37	\$4.83



# DEFEND - Cyberthreat Protection

Cloud Security Powered by Zscaler



**Zscaler Private Access™ (ZPA)** offers seamless zero trust connectivity for all users, with AI-powered user-to-app segmentation and context-aware policies. The world's most deployed ZTNA solution, ZPA can replace legacy tools like VPNs and VDI in just hours.

ZPA brokers direct, one-to-one connections between authorized users and specific apps. Unlike with a VPN, users never access the corporate network, and apps are never exposed to the public internet.



## Replace vulnerable VPN solutions

Reduce the attack surface and eliminate lateral movement by connecting users directly to applications—not the network, elevating your security posture.



## Prevent private app compromise

Minimize the risk of app compromise and data loss with full inline inspection of private app traffic and data loss prevention.



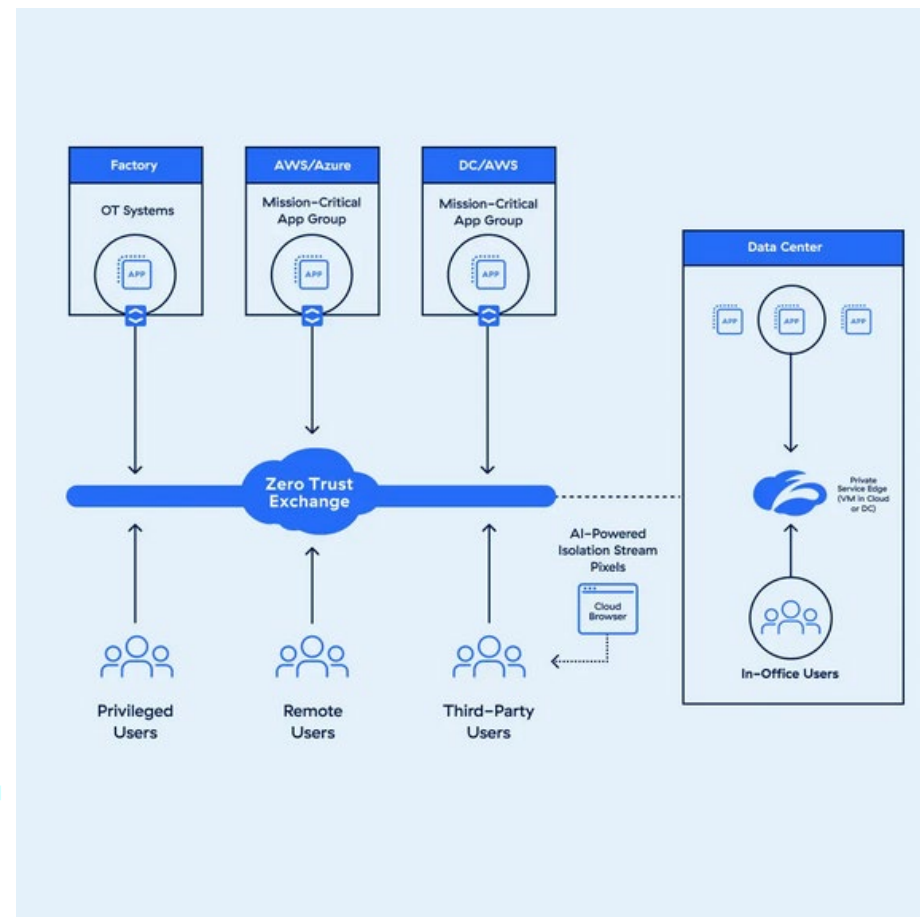
## Empower your hybrid workforce

Seamlessly extend lightning-fast access to private apps across remote users, HQ, branch offices, and third parties.



## Reduce cost and complexity

Offer secure, optimized access, without costly and complex point products, through a unified, cloud native ZTNA platform for users, workloads, and IoT/OT.





# DEFEND - Cyberthreat Protection

Cloud Security Powered by Zscaler



## Zscaler Private Access™

### KEY OFFERINGS

#### AI-Powered App Segmentation

Discover applications automatically. Use AI-generated recommendations on app segments and policies to reduce your attack surface and prevent lateral movement.

#### Workload-to-Workload Segmentation

Secure cloud workload communications across hybrid and multicloud environments such as AWS and Azure.

#### Privileged Remote Access

Give remote workers and third parties clientless remote access to sensitive RDP, SSH, and VNC production systems.

#### Browser Access

Enable seamless user-to-app connections using lightweight, infrastructure-agnostic software, paired with browser access capabilities.

#### Private Service Edge

Bring ZTNA to on-premises users with direct user-to-app, least-privileged access to private applications.

#### Business Continuity

Ensure uninterrupted, policy-enforced access to mission-critical applications during connectivity outages and black swan events.

#### Extranet Application Support

Enable zero trust access to business partner and vendor applications hosted in their networks.

#### Digital Experience Monitoring

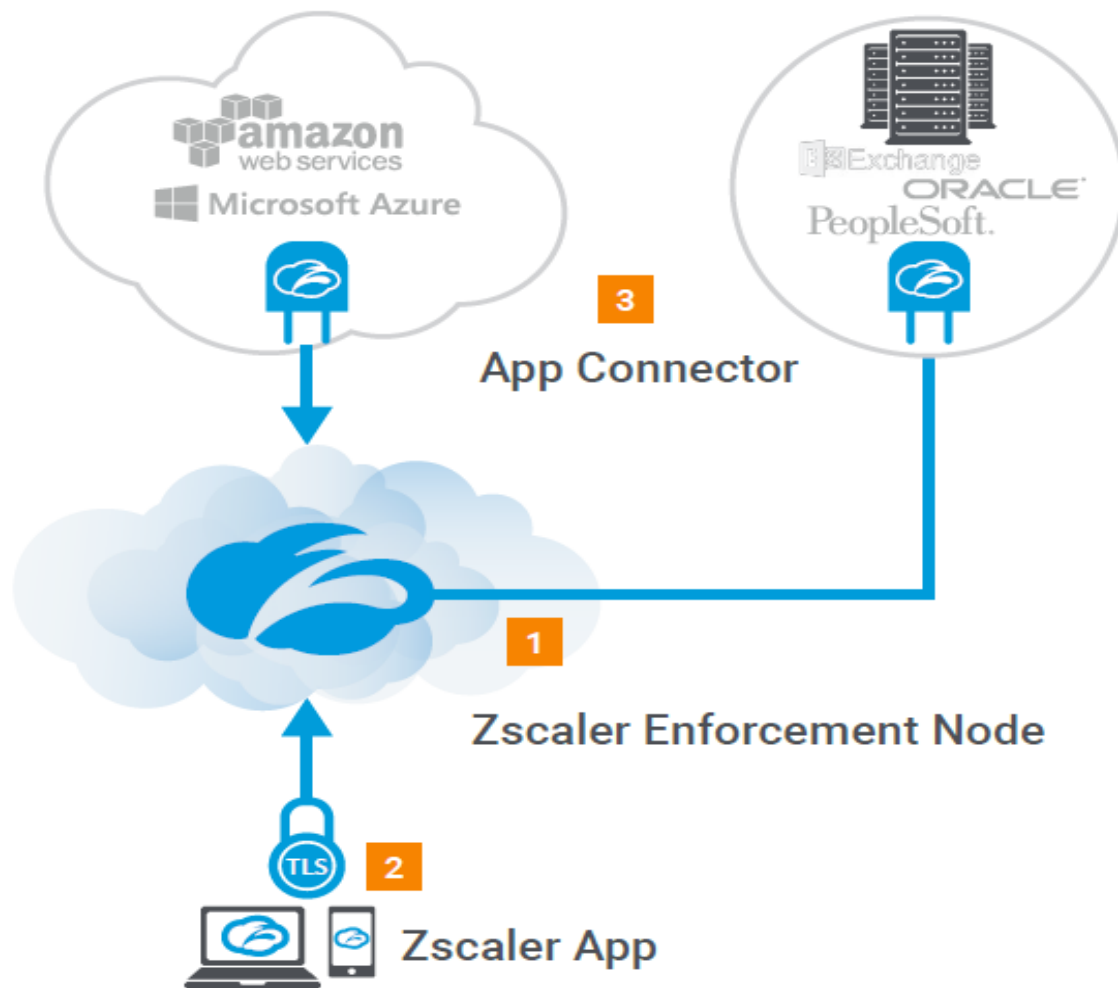
Optimize your digital experiences to keep users productive by rapidly detecting and resolving app, network, and device issues.



# DEFEND - Remote Access

Cloud Security Powered by Zscaler

Powered by  
**zscaler**



## 1. Zscaler Enforcement Node

- Hosted in cloud
- Used for authentication
- Customizable by admins
- Brokers a secure connection between a Z-App and a Z-connector

## 2. Zscaler App

- Mobile client installed on devices
- Requests access to an app

## 3. App Connector

- Sits in front of apps in Azure, AWS, and other public cloud services
- Listens for access requests to apps
- No inbound connections



FEATURE	PROFESSIONAL	BUSINESS	ENTERPRISE
Global visibility for users and application — Single pane of glass shows which users are accessing private, internal apps	✓	✓	✓
Secure Private Application access — Access to unlimited private internal applications (whether public/private/hybrid cloud or legacy datacenters) without exposing the network to users or applications to the Internet	✓	✓	✓
App and server discovery — Wildcard policy shows application and server locations as they are requested by users	✓	✓	✓
Enterprise DarkNet with DDoS protection for applications — Applications are only visible to users that are authorized to connect to them	✓	✓	✓
Single console for policy definition and management — All policy for global deployment via a single pane of glass	✓	✓	✓
Passive health monitoring — Application health is monitored when access is requested	✓	✓	✓
Zscaler App — Lightweight application used to provide access to Zscaler Internet Access and Zscaler Private Access	✓	✓	✓
Microsegmentation by application (up to 5 application segments) — Granular access control by user or group for up to five specific application definitions, each of which may contain multiple hosts and/or ports.	✓		
Microsegmentation by application (up to 10,000 application segments) — Granular access control by user or group for up to 10,000 specific application definitions, each of which may contain multiple hosts and/or ports.		✓	✓
Continuous health monitoring — Application health is continuously monitored to ensure that ports are available and users can connect to the app		✓	✓
Basic device posture enforcement — Checks the registry, existence of file system and posture certificate for each device	✓	✓	✓
Browser access — allows use of web browser for user authentication and app access over ZPA	✓	✓	✓
*Customer-provided PKI — Customer-provided certificates ensure complete privacy			✓
*Double encryption — Provides encryption to microtunnel using customer's PKI			✓
Real-time user transaction view — Instantaneous logs for end-user support			✓
*Log Streaming Service — Automatically streams logs to SIEM provider		✓	✓



# DEFEND - Remote Access

Cloud Security Powered by Zscaler



**Zscaler Private Access (ZPA)** is a cloud service from Zscaler that provides zero trust, secure remote access to internal applications running on cloud or data center. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity versus extending the network to them.

		Monthly Per User Pricing									
Product Name	SKU	Up to 99	100+	500+	1,000+	2,500+	5,000+	10,000+	25,000+	50,000+	100,000+
ZPA Browser Access Only	ZPA-BBA	\$4.00	\$3.00	\$2.16	\$2.00	\$1.80	\$1.68	\$1.52	\$1.40	\$1.36	\$1.20
ZPA Professional Suite	ZPA-PRO	\$6.60	\$4.95	\$3.56	\$3.30	\$2.97	\$2.77	\$2.51	\$2.31	\$2.24	\$1.98
ZPA Business Suite	ZPA-BUS	\$13.54	\$10.16	\$7.31	\$6.77	\$6.09	\$5.69	\$5.15	\$4.74	\$4.60	\$4.06

*ZPA Pricing is not supported or quotable using BOSS. ZPA service may be quoted with Engineering concurrence using PDF Editor.*

## ZPA's unique design is based on four key tenets:

- Connect users to applications without placing users on the network
- Never expose applications to unauthorized users
- Enable app segmentation without network segmentation
- The internet is the new corporate network



## Zero Trust Firewall

# Secure web and non-web traffic for all users, apps, and locations

To protect users, apps, and data everywhere, you need security that can adapt to the dynamic needs and unique risks of distributed environments. Modernize your security with a zero trust cloud firewall that enables you to:



**Stop threats and inspect  
100% of traffic**

even encrypted traffic



**Centralize policy  
management**

for all users and traffic



**Seamlessly connect to  
SaaS apps**

like Microsoft 365 and Zoom



**Cut costs and complexity**

without compromising  
performance





## What sets Zscaler Zero Trust Firewall apart?

### Traffic inspection

Terminate malicious connections and prevent threats with unlimited inline traffic inspection and native TLS/SSL decryption.

### Wildcard domains

Create flexible access policy to cloud services and PaaS/IaaS with centralized policy management.

### Always-on cloud IPS and custom signatures

Enrich SecOps workflows with adaptive behavioral IPS signatures, including custom signatures, that work in real time and are easily shared.

### Bandwidth control

Prioritize business-critical apps, provide a better user experience, reduce costs, and simplify IT with cloud-delivered bandwidth control.

### Advanced attack detection

Quickly identify and intercept evasive and encrypted cyberthreats hiding in traffic on nonstandard ports.

### DNS performance and security

Sustain superior performance and keep your users and endpoints safe from malicious sites with localized resolutions and DNS tunneling.

### Secure work-from-anywhere users

Leverage unparalleled user- and app-aware threat protection with dynamic, follow-me policies on and off the corporate network.

### Secure internet breakouts

Improve user experiences with scalable, fast, secure direct-to-internet connections for all hybrid and branch traffic.

[Zerto Trust Firewall Data Sheet](#)



# DEFEND - Cyberthreat Protection

Cloud Security Powered by Zscaler



**Zscaler Cloud Sandbox** delivers unlimited, latency-free inspection to block threats before they reach your endpoints. Cloud native and fully inline, it provides real-time analysis and verdicts to prevent threats from spreading—without ever compromising productivity.

## Advanced threat protection with productivity built in



### Prevent zero day infections in seconds

Stop unknown threats with inline malware and advanced threat detection, including AI-driven instant verdicts.



### Bolster security and preserve productivity

Automatically detect and quarantine threats, and integrate with Zero Trust Browser to keep users productive during file scans.



### Optimize SOC workflows

Seamlessly integrate malware protection into SOC workflows with out-of-band file analysis, third-party threat detection tools, and fully patched VMs for threat investigation.



### Deploy easily, scale globally

Eliminate management overhead—simply configure policies for immediate value, driving strong ROI that lets you focus on strategic growth.



## Zscaler Cloud Sandbox

Comprehensive malware protection with seamless productivity and scalability



### Layered malware detection

Stop malware and advanced threats with unlimited, latency-free TLS/SSL inspection. Get low-latency, high-performance protection with our Single Scan, Multi-Action engine.



### AI-powered security

Get instant, high-confidence verdicts from enhanced AI/ML models trained on 600M+ samples. Fight AI-enabled phishing with inline AI/ML PhishCatch.



### Static and dynamic analysis

Use static and dynamic analysis to inspect code structure at rest, detonate files, and analyze secondary samples. Update cloud databases instantly when malicious files are detected.



### Zero Trust Browser integration

Allow users to securely interact with original files during sandbox analysis, ensuring productivity. Files flagged as malicious can be flattened into PDFs or disarmed to remove harmful content.



### API-driven analysis

Send out-of-band files directly to the sandbox via API integration, streamlining investigations. Access Cloud Sandbox analysis data via API, ingest into SIEM/SOAR, or share with EDR solutions, enabling actionable insights and seamless SOC workflows.



### Granular policy control and reporting

Tailor sandbox policies to user roles, locations, and categories. Get contextual, in depth, and pre-configured reporting, including MITRE ATT&CK mapping, to meet compliance and audit requirements.



# DEFEND - Cyberthreat Protection

Cloud Security Powered by Zscaler



**Zscaler Zero Trust Browser** streams web page content from our cloud native security platform, delivering near-native web experiences, free of threats, that provide:



## AI-driven threat protection

Protect users from web threats with AI-based isolation of suspicious internet content and high-risk users.



## Sandbox integration and file preview

Enable full productivity with no risk—users can access instant previews of files in Zero Trust Browser as they're analyzed in the sandbox.



## Protected storage with safe preview

Enable employees to temporarily store documents in the cloud browser, upload files to another sanctioned corporate app, or download secure flattened PDFs using Content Disarm and Reconstruction (CDR).



## Fully integrated data loss prevention

Protect data, even on BYOD endpoints, with controls (clipboard, print, upload/download, read-only, etc.) that block data leakage, stop risky actions, and even watermark data.



## Browser access integration

Extend agentless access to web-based and SaaS applications via the cloud browser with data security controls for employees or contractors on unmanaged or BYOD endpoints.



## FedRAMP Authorized

Confidently meet compliance and mandates with our FedRAMP Moderate and High authorized solution.



## Zscaler Zero Trust Browser

# Cyberthreat protection

### Safer web experiences

Automatically reduce the overall risk of web-based threats and zero-day vulnerabilities to keep users safe and productive on any device. Leverage user risk score, device posture, or AI-powered Smart Isolation.

### File isolation

Safely render productivity documents as PDFs to ensure malicious macros and other active content can't reach users. Allow download of secure flattened PDFs using CDR.

### Generative AI protection

Secure the use of AI by preventing data leakage via AI prompts, and restrict potentially harmful actions like upload/download or cut/paste.

# Data protection

### BYOD productivity and data protection

Extend productivity to unmanaged devices, including mobile devices, so employees can access necessary SaaS or private web apps while also prioritizing data security.

### VDI alternative

Turn to an agentless cloud browser instead of complex and expensive VDI for contractors and third-parties working on SaaS or private web apps.

### Streamlined M&A with data protection

Quickly give newly acquired employees access to apps they need for their work—with data security every step of the way.



## Web & Email DLP ...Welcome to the future of data protection!

Say goodbye to protection gaps and complex administration.  
Redefine how you secure data with innovative auto data discovery  
and data loss prevention (DLP) across all channels.



### Protect all data and users

Secure internet, email, endpoint, IaaS, private apps, and risk posture in one simple platform.



### Secure email with ease

Quickly scale DLP to emails and attachments without configuration changes via SMTP relay.



### Discover data automatically

Easily find data risks with AI-powered data discovery across endpoint, inline, and clouds.





## Web & Email DLP ...Unified DLP for web, endpoint, and email!

Securing data today requires a unified approach that provides fast, consistent protection for users and data, wherever they are.

Zscaler DLP is an enterprise data loss prevention solution, natively integrated in the world's largest inline security cloud. As part of a complete security service edge (SSE), it eliminates the costs and complexity of point products while providing:



### Centralized policy

across web, endpoint, email, SaaS, public cloud, private apps, and BYOD



### Identical protection

and enforcement, no matter the location or type of data



### Scalable TLS/SSL

inspection from the world's largest inline security cloud



### Streamlined workflows

and operations with ML-powered data discovery



## Strengthen SaaS security with **Multimode CASB!**

A multimode cloud access security broker (CASB) empowers organizations to secure any sanctioned or unsanctioned SaaS app or IaaS platform. Inline, real-time security and out-of-band scanning functionality allows admins to:



**Configure one automated policy for consistent security**



**Retire costly, outdated point products**



**Reduce IT complexity with a cloud-based architecture**



**Unify SaaS data inspection**





# DEFEND - Data Protection

Cloud Security Powered by Zscaler



## Multimode CASB ...Protect SaaS & IaaS with ease!

Zscaler CASB secures SaaS like Microsoft 365 and Salesforce as well as IaaS offerings like Amazon S3, preventing risky sharing that leads to sensitive data loss or noncompliance.

### Consistent data protection

Stop accidental or risky file shares, as well as internal threats like intellectual property theft, with granular policies applied across cloud apps.

### Complete threat protection

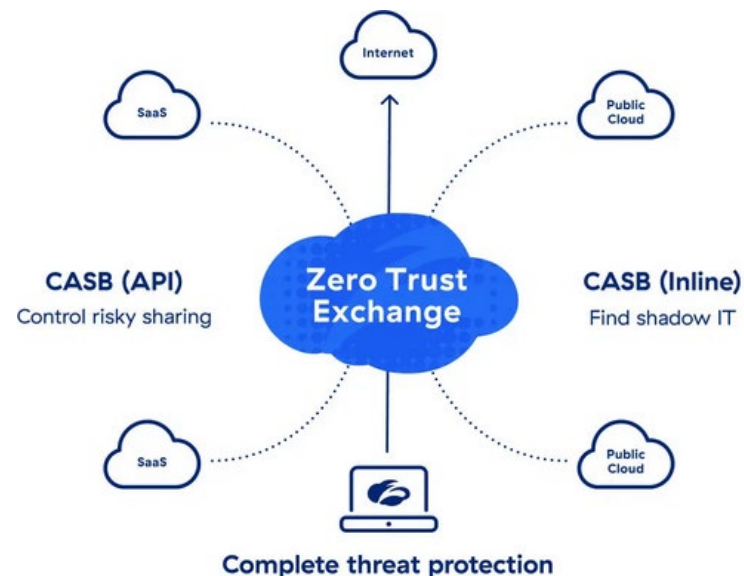
Automatically remediate zero-day malware with threat protection with cloud sandboxing refined by 200B transactions and 150M threats identified daily.

### Comprehensive visibility

Consolidate ease of use, enhanced intelligence, and auditing with integrated visibility and thorough reporting across all SaaS apps and IaaS platforms.

### Unified compliance

Adhere to regulations and mitigate violations across SaaS apps and cloud service providers with full compliance visibility in a single pane of glass.





# DEFEND - Data Protection

Cloud Security Powered by Zscaler



**Zscaler Endpoint DLP** gives you holistic, always-on protection along with a host of other capabilities to give your security team the advantage against threats.

## Powerful protection with simple deployment!



### Deploy rapidly

Use your existing DLP policies to quickly protect endpoint devices and prevent unauthorized users from gaining access.



### Protect key channels

Enforce DLP policies over key exfiltration channels like removable storage, network shares, and printing.



### Control cloud storage sync

Stop sensitive data loss to native cloud storage apps like Dropbox, Box, and OneDrive.



### Leverage powerful dashboards and workflows

Speed up incident response with in-depth dashboards, forensics, and integrated workflow automation.



# DEFEND - Data Protection

Cloud Security Powered by Zscaler



**Zscaler Endpoint DLP** ...Deliver unified, consistent endpoint protection!

Part of the complete Zscaler Data Protection solution, Zscaler Endpoint DLP provides the visibility and control you need over device data while reducing the cost and complexity of data security.



## Enjoy simple, powerful policies

Deliver one consistent DLP policy everywhere—endpoints, inline, and in the cloud—with the power of the cloud native Zscaler platform.



## Use a single lightweight agent

Unify everything into one agent for airtight protection on and off the corporate network, regardless of connection status.



## Deliver unified visibility

Maintain a single source of truth and consistent alerting across all endpoint and cloud data, built around a centralized classification engine.



# DEFEND - Data Protection

Cloud Security Powered by Zscaler



**Unify SaaS Security with CASB and SSPM...**Simple, holistic, cost-effective protection!

Safeguard data across your SaaS platforms without the complexity or high costs of point security tools. Get everything you need to govern and secure SaaS data and posture with a single, powerful approach.



## Secure SaaS data

with a multimode cloud access security broker (CASB)



## Harden your security posture

with SaaS security posture management (SSPM)



## Govern your SaaS supply chain

with in-depth shadow IT discovery and audits



## Respond to identity risks

with a zero trust, least-privileged access approach



## Accelerate your CTEM projects

with rich SaaS posture insights



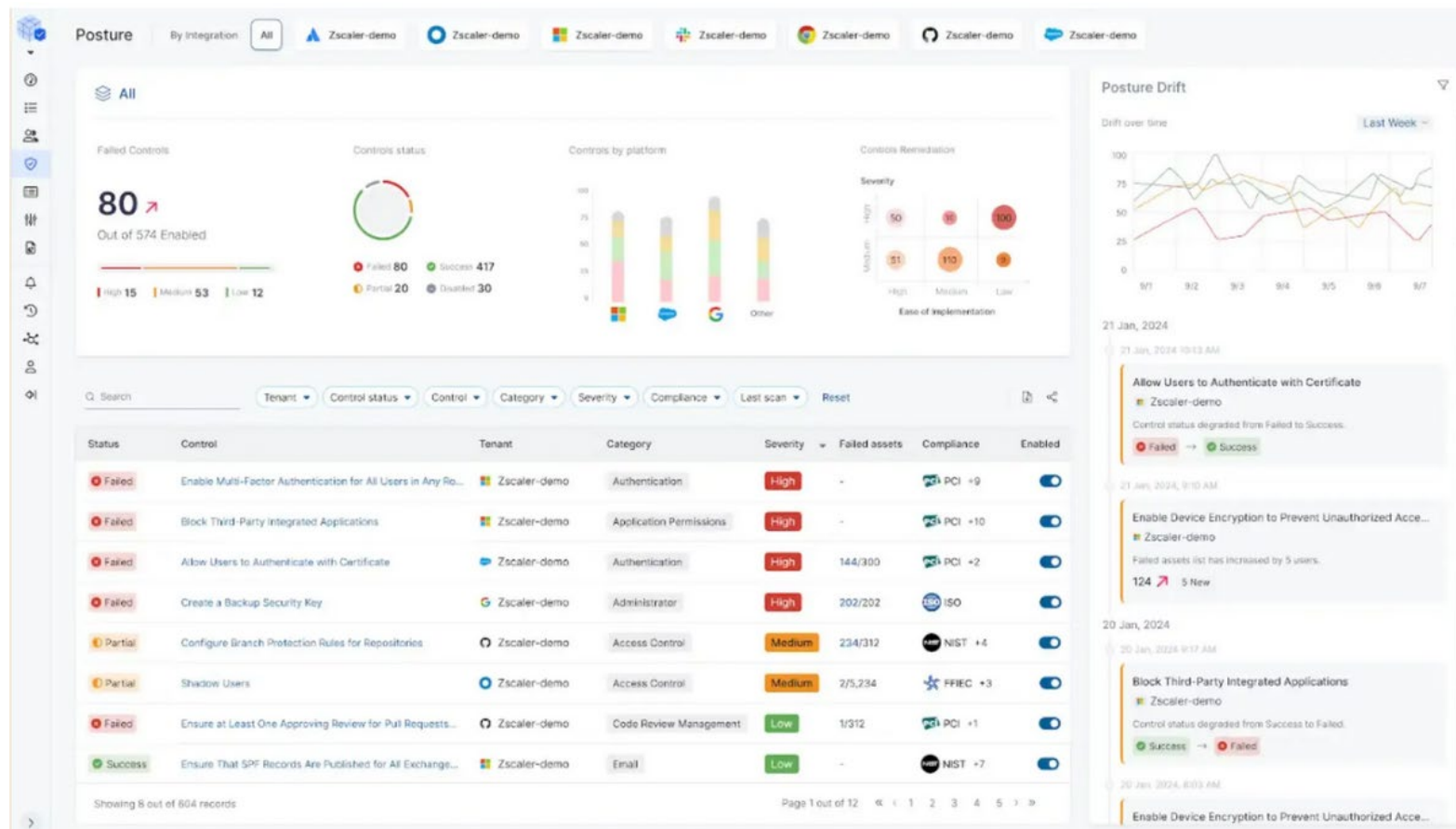
# DEFEND - Data Protection

Cloud Security Powered by Zscaler



**Zscaler Advanced SSPM** is a unified solution that delivers complete security across SaaS apps and platforms. From data visibility to posture control and data governance, it enables IT teams to quickly identify SaaS risks and prevent compromises.

## What Is SaaS Security Posture Management (SSPM)?





# DEFEND - Data Protection

Cloud Security Powered by Zscaler



**Zscaler Generative AI Security**...Keep your data safe and users productive!

Create and enforce policies around the generative AI tools your users can access and how they can interact, directly or via browser isolation, to protect your sensitive data.



## Spark productivity and creativity

Accelerate your growth and differentiation with responsible use of AI, confident that every prompt or query is secure.



## Let data drive your business—not breaches

Keep your sensitive data safe from breaches, and avoid regulatory issues and fines, with granular policy enforcement.



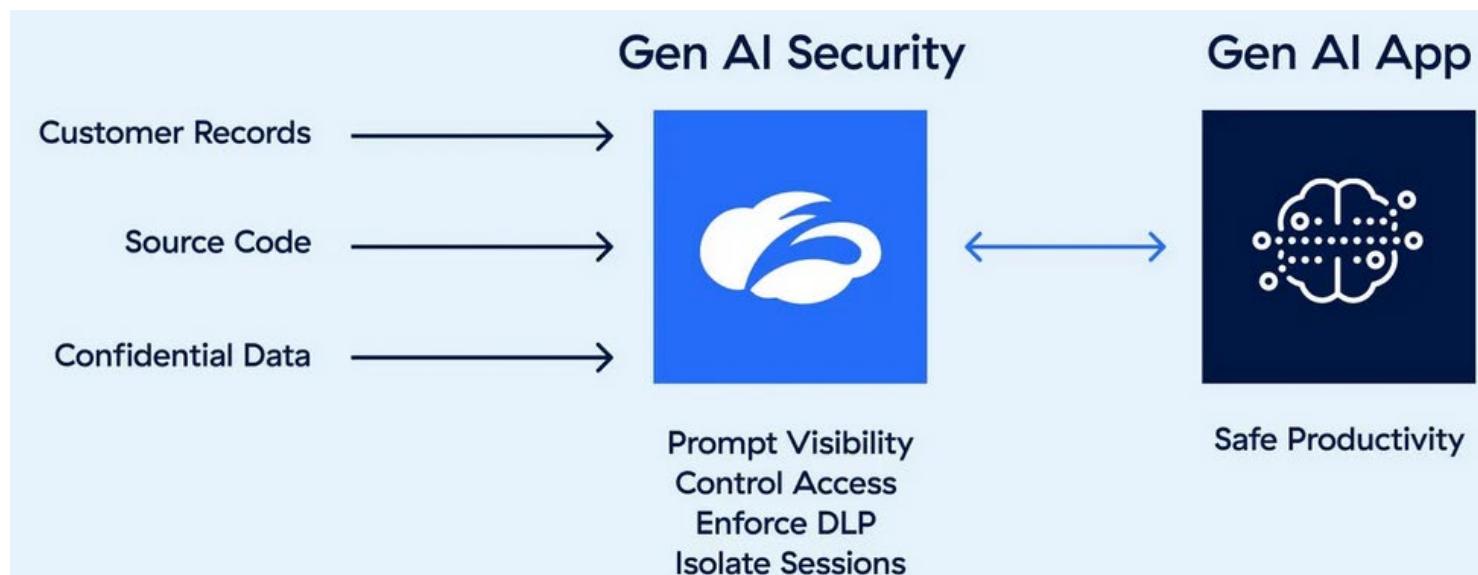
# DEFEND - Data Protection

Cloud Security Powered by Zscaler



## Zscaler Generative AI Security...Unlock safe AI productivity!

Prevent data loss while unleashing new creative workflows across your users with Zscaler Generative AI Security. Get complete control over all aspects of GenAI use—from prompts to which apps are allowed—so you can safely spark creativity and productivity.







**Microsoft Copilot Data Protection...**Ensure OneDrive, Purview, and Microsoft 365 operate at their best, helping control Copilot oversharing and misconfigurations!

## Copilot presents an oversharing challenge

Microsoft Copilot can offer substantial boosts to productivity. Unfortunately, it can also overconsume and share sensitive data with underprivileged users. Microsoft provides Copilot Security options, yet several challenges remain:



### OneDrive permissions

Improperly permissioned data can be consumed and shared too widely.



### Purview labeling

If users fail to label sensitive data properly, it's open to access by Copilot prompts.



### Copilot misconfigurations

Gaps in Microsoft 365 and Copilot configurations can expose data to risks.





# DEFEND - Data Protection

Cloud Security Powered by Zscaler



## Microsoft Copilot Data Protection...Deliver powerful Copilot data security!

Zscaler takes a unique approach to API and inline security that enables robust control over Copilot deployments, ensuring proper access constraints around sensitive data across your Microsoft tenant.

### See and control prompts:

Get full visibility into Copilot user prompts, and block sensitive data inputs with DLP.

### Fix OneDrive data permissions:

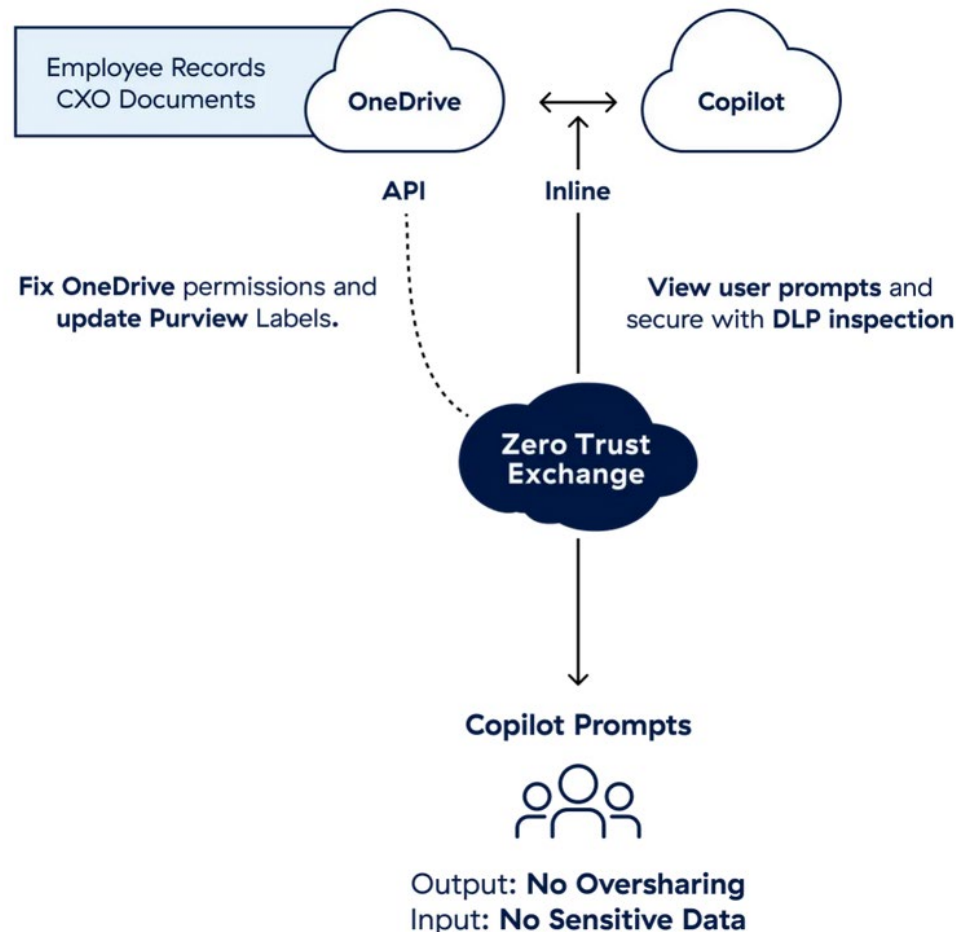
Prevent Copilot oversharing by removing excessive sharing permissions.

### Update Purview labels:

Add missing Purview sensitivity labels to data in order to restrict Copilot access.

### Close dangerous misconfigurations:

Find and close Copilot or Microsoft 365 configurations that expose data.





# DEFEND - Data Protection

Cloud Security Powered by Zscaler



## Zscaler Data Security Posture Management (DSPM)...Prevent and remediate cloud data breaches at scale!

Zscaler DSPM provides granular visibility into your cloud data, classifies and identifies data and access, and contextualizes data exposure and security posture.



### A comprehensive data protection platform

Get best-in-class data security for web, SaaS, on-premises apps, endpoints, BYOD, and public clouds. Leverage seamless integration with AI-powered data protection, built around a centralized DLP engine.



### AI auto data discovery

Automatically discover, classify, and identify data, without any configuration, while drastically speeding up deployment and operations with an agentless approach.



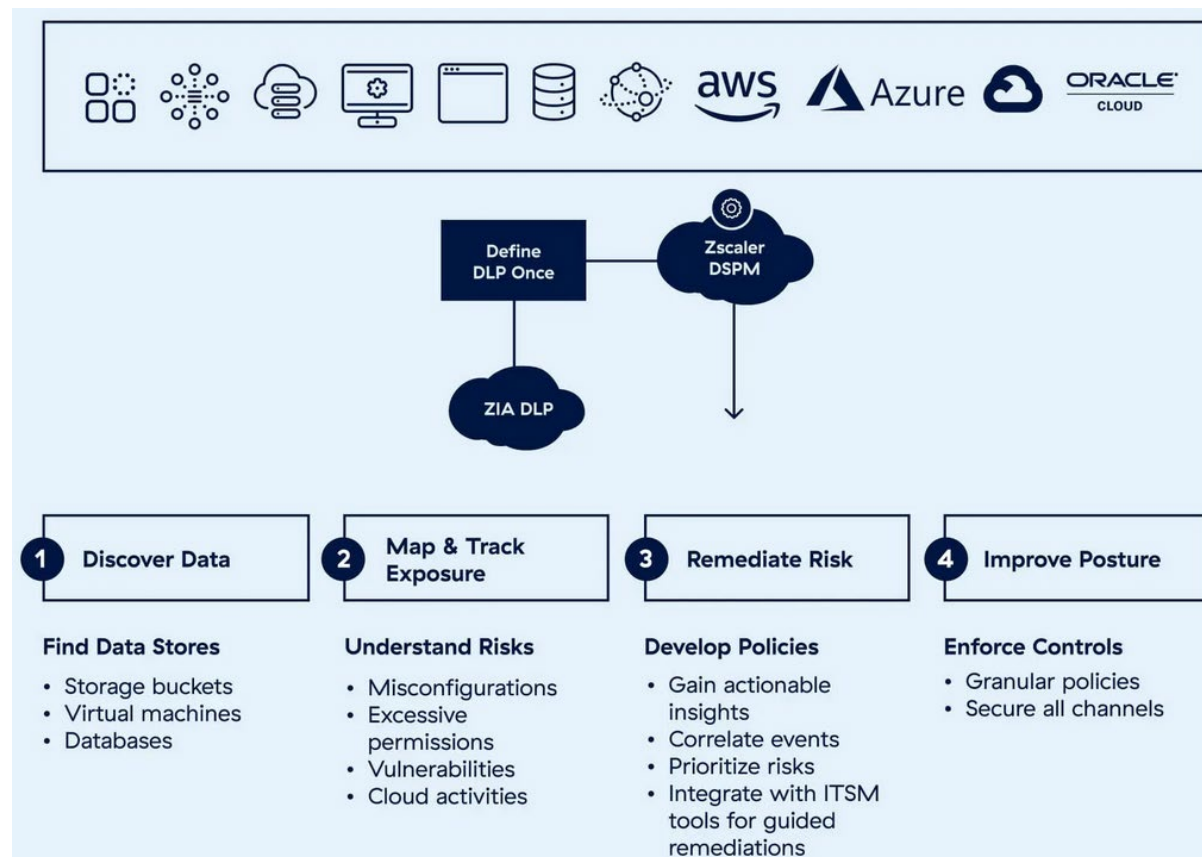
### Empowered teams and simplified operations

Greatly reduce alert overload with powerful threat correlation that uncovers hidden risk and critical attack paths. Save time for your team so they can focus on the risks that matter most.



### A richer data foundation to drive CTEM initiatives

Bring together data security posture details with other types of posture gap data to create a prioritized, actionable set of risk reduction insights and accelerate continuous threat exposure management projects.





# DEFEND - Data Protection

Cloud Security Powered by Zscaler



## Zscaler BYOD Security...Enable Safe Third-Party Access and BYOD Security!

### Provide seamless application access without VDI or network integrations

Contractors, partners, and other third parties need SaaS and private app access to get work done. Options like VDI, VPN, enterprise browsers, or extending network access are difficult, expensive, and not built to protect data. Give third parties secure, agentless app access—from the browser they already use—with data security included.



#### Enable productivity on unmanaged devices

with browser-based app access



#### Prevent data exfiltration and risky user actions

with robust data security controls



#### Provide direct user-to-app access with no VPN

for built-in app segmentation



# DEFEND - Data Protection

Cloud Security Powered by Zscaler



## Zscaler BYOD Security... Easily minimize third-party risk with Zscaler!

Take a user- and application-centric approach to security with Zscaler Third-Party Access. Provide only authorized users with access to specific apps—with great user experiences, integrated data security and private AppProtection; and no software agents, new dedicated browsers, or VDI—all without granting network access.

It works seamlessly with any device, including bring-your-own-device (BYOD), in the user's browser of choice, while your IT team maintains granular control. Authorized users gain secure access to the apps and data they need, and nothing else.



### Security

Segment application access with direct user-to-app connections, preventing lateral movement. Restrict risky actions like copy/paste or document downloads to unmanaged devices to protect against web-based risks and block data exfiltration.



### Simplicity

Grant users seamless access to authorized applications from their own web browser, on any device. No need to install agents or deploy a separate browser for enterprise use.



### Integration and value

Maintain consistent policies and ease of management from a single, unified platform. Eliminate costly technologies like VDI to drive down costs many times over.



## Zscaler Zero Trust SASE...Networking and Security Made Simple with Zero Trust SASE!

Zero Trust SASE builds on the industry's leading SSE platform with a fresh approach to SD-WAN that reduces business risk.



### Prioritize your mission

Provide secure connectivity for your workforce and locations, so you can focus on your goals.



### Improve cyberthreat protection

Better protect your crown jewels with superior security built for today's dynamic organizations.



### Lay a strong base for IoT adoption

Securely adopt IoT and OT without widening your attack surface or complicating policy enforcement.



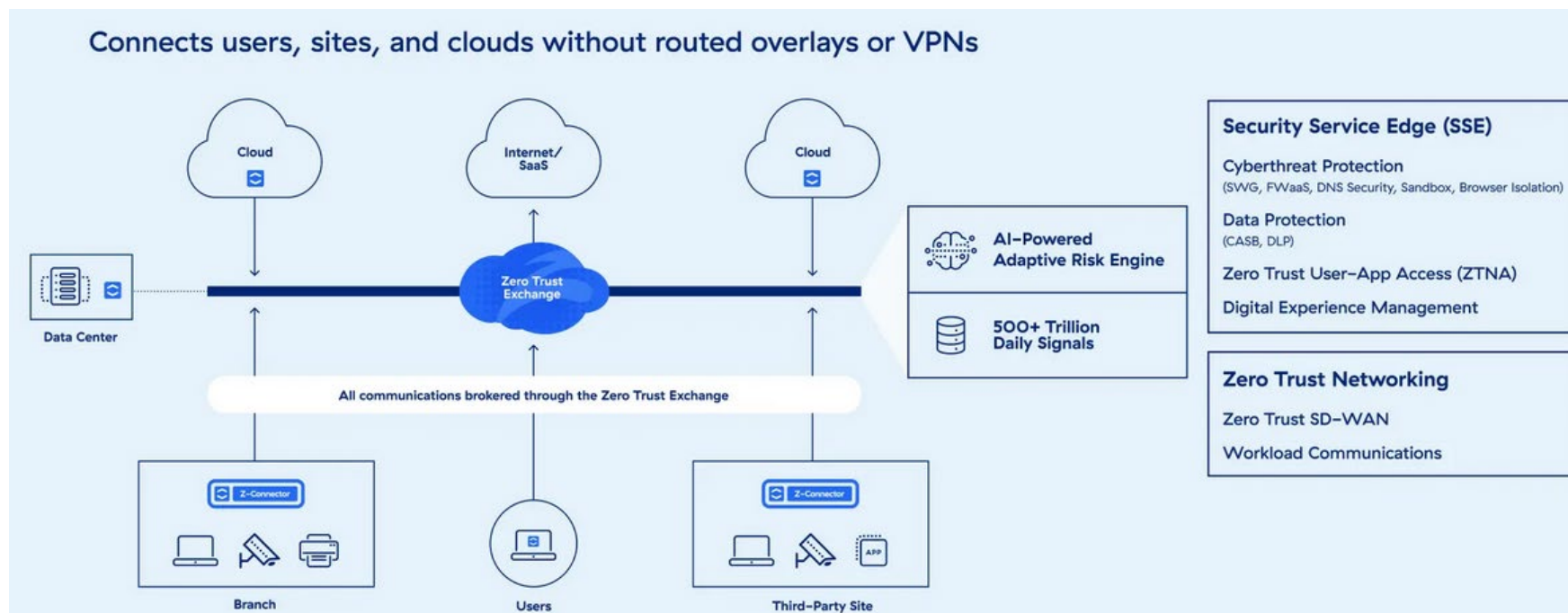
# DEFEND - Zero Trust Networking

Cloud Security Powered by Zscaler



## Zscaler Zero Trust SASE...The first SASE platform built on zero trust!

Zscaler Zero Trust SASE builds on the leading AI-powered security service edge (SSE) platform with a new approach to SD-WAN that securely and reliably connects users, locations, and cloud services via the Zscaler Zero Trust Exchange™.







# DEFEND - Zero Trust Networking

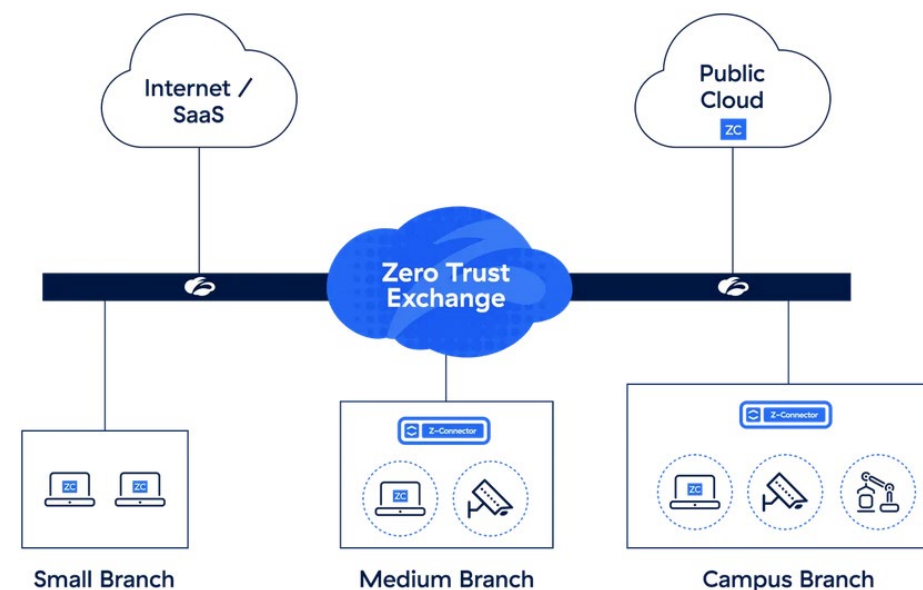
Cloud Security Powered by Zscaler



**Zscaler Zero Trust SD-WAN...**Enable café-like branches: strengthen security and simplify access!

Zscaler Zero Trust SD-WAN provides branches and data centers fast, reliable access to the internet and private applications. With a direct-to-cloud architecture, it offers stronger security and greater operational simplicity than traditional hybrid WAN. Users and IoT/OT devices connect directly to apps through the Zscaler Zero Trust Exchange™ platform.

Zero Trust SD-WAN automatically forwards branch traffic to the Zero Trust Exchange for real-time policy enforcement, including full security inspection and identity-based access control. Trusted app traffic can be sent directly across the internet with direct internet breakout.





# DEFEND - Zero Trust Networking

Cloud Security Powered by Zscaler



## Zscaler Zero Trust SD-WAN...Connect and protect your entire ecosystem!



### Improve user experience and productivity

Replace complex site-to-site VPNs with a direct-to-cloud architecture that improves application traffic flow and performance.



### Minimize the internet attack surface

Hide your private applications behind the Zero Trust Exchange, where they can't be discovered or attacked from the internet.



### Prevent lateral threat movement

Provide direct access to applications, not your network, unlike the open attack surface inherent to site-to-site VPN.



### Deploy and integrate with ease

Replace multiple products (e.g., routers, firewalls, VPNs) with a plug-and-play appliance that extends zero trust to all users and devices.

Rapidly deploy Zero Trust SD-WAN with Zscaler Edge appliances, available in a physical or virtual form factor, in one-armed mode or inline gateway mode. All Zscaler Edge appliances feature:

- Zero touch provisioning and automated deployment
- App-aware path selection and ISP link management
- Granular forwarding policy for internet, private app, and direct WAN traffic
- URL filtering, file type control, and cloud firewall policies for internet-bound traffic
- Zero trust policies for IoT devices and servers
- Centralized visibility and logging





# DEFEND - Zero Trust Networking

Cloud Security Powered by Zscaler



**Zscaler Zero Device Segmentation**...Extend zero trust inside your branch, factory, and campus –in hours!

Agentless zero trust segmentation eliminates the risk of lateral movement inside your network by isolating every endpoint into a secure "network of one."



**Easily segment IoT and OT**



**Eliminate east-west firewalls and NAC**



**Deploy in hours with no outages, agents, or VLAN changes**

## What sets Zero Trust Device Segmentation apart?



**No lateral movement**

Stop lateral threat movement by isolating every connected endpoint without taking them offline.



**No endpoint agents**

Fully segment legacy servers, headless machines, and IoT/IoMT devices that can't accept agents.



**No legacy firewalls or networking**

Eliminate the cost and IT tickets of east-west firewalls, NAC, branch DHCP, and complex switches.



**No OT downtime**

Deploy in just hours, and integrate into your running network with no agents, hardware upgrades, or VLAN readdressing.



## **Zscaler Zero Device Segmentation...**Deploy Zero Trust Device Segmentation in hours, without east-west firewalls!

The Zscaler Zero Trust Exchange™ protects thousands of organizations with zero trust segmentation for users, applications, workloads, and locations. With Zero Trust Device Segmentation, we eliminate lateral threat movement inside your network. Instantly reduce complexity and risk with seamless deployment—and no need for endpoint agents.

### **Stop lateral threat movement**

Enforce policy on every endpoint without adding software. Segment every IP device into a network of one—no agents, no east-west firewalls, or NAC required.

### **Automate incident response with our Ransomware Kill Switch™**

Instantly block risky protocols to reduce the blast radius of a breach with granular controls, including pre-programmed and custom policies.

### **Discover every device on your network**

Automatically discover and classify every device with accurate, real-time auto-mapping.



# DEFEND - Zero Trust Networking

Cloud Security Powered by Zscaler



## Zscaler Zero Trust Cloud ...Multi-Cloud Workload Security Without Firewalls!

Secure internet-bound traffic and enable secure workload-to-workload connectivity



**Achieve consistent threat and data protection**



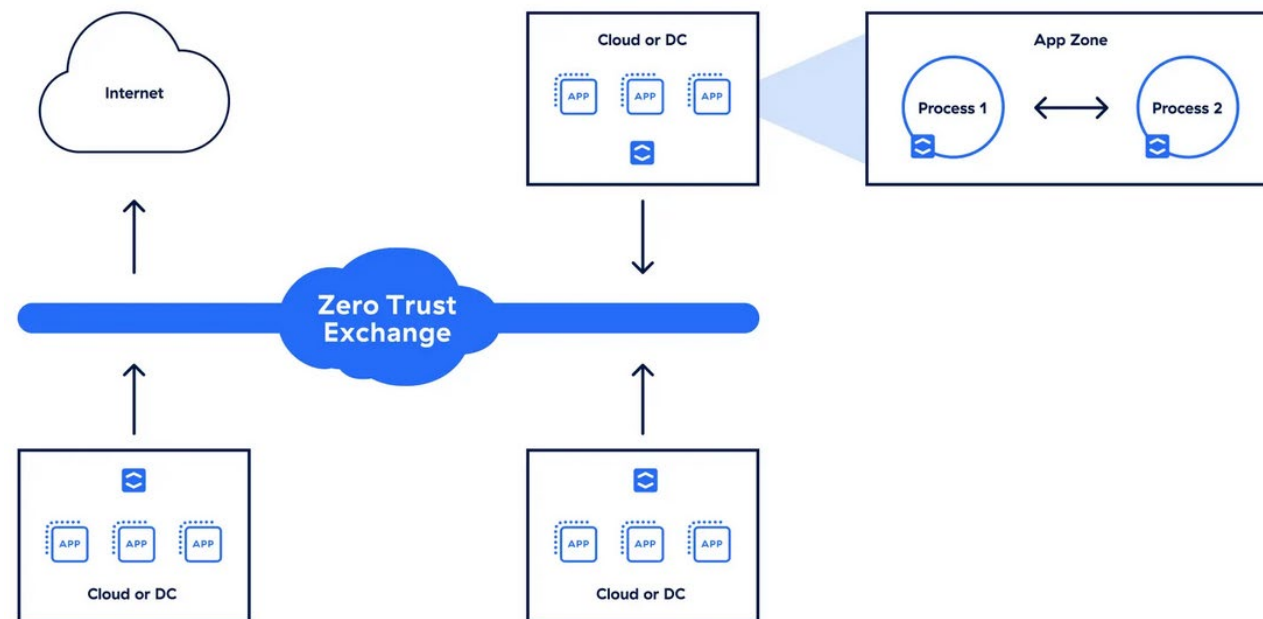
**Eliminate lateral threat movement between workloads**



**Reduce costs and complexity vs. legacy architectures**

## Enable superior cloud workload security with Zero Trust Cloud

Achieve comprehensive zero trust security for your cloud workloads with the Zscaler Zero Trust Exchange™ platform. It inspects all traffic inline to guard against cyberthreats and data loss, segments workloads across multiple clouds, and protects traffic to internet, SaaS apps, or other workloads.





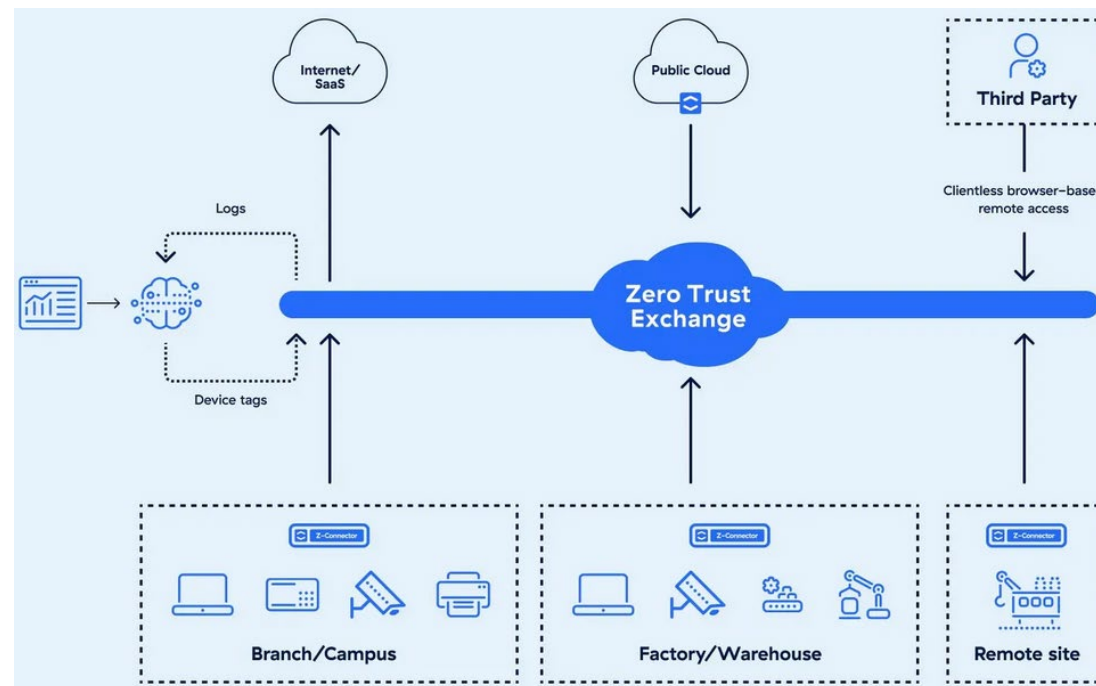
# DEFEND - Zero Trust Networking

Cloud Security Powered by Zscaler



## Zscaler Zero Trust IoT/OT...Secure your IoT and OT with zero trust!

Zscaler IoT and OT Security solutions can help your organization discover, classify, connect, and segment devices to protect your operations. Avoid the complexity of firewalls, ACLs, NAC, and device agents with the power of the Zscaler Zero Trust Exchange™ platform.



### Discover and classify

Identify and tag all IoT/OT devices in your organization using AI/ML-powered behavioral identity and risk classification.

### Segment and secure

Isolate every device into a “network of one” and securely connect to the internet and private apps, without exposed ports, firewalls, or agents.

### Manage and supervise

Enable privileged remote access to IoT/OT devices for remote management, with full cybersecurity and governance controls.



# DEFEND - Zero Trust Networking

Cloud Security Powered by Zscaler

## Zscaler Zero Trust IoT/OT



### Secure your connected future



#### Ensure business continuity

Enable secure, fast connectivity for IoT/OT devices to minimize downtime and eliminate vendor risk.



#### Improve people and plant safety

Prevent compromise and lateral threat movement to stop ransomware attacks and protect critical infrastructure.



#### Reduce operational complexity

Eliminate complex legacy technology, including VPNs, firewalls, NAC agents, and proprietary switches.

### A complete platform to serve your whole organization



#### Discover and classify

Maintain complete visibility and control of all IoT devices, servers, and unmanaged user devices across your business.



#### Segment and secure

Fully isolate IoT/OT devices into a network of one, without firewalls or agents.



#### Manage and supervise

Secure third-party vendor and remote user connectivity to OT equipment from any location.



# DEFEND - Zero Trust Networking

Cloud Security Powered by Zscaler



**Zscaler Digital Experience (ZDX)**...Optimize user experiences across all locations, devices, and apps!

Your users and apps are everywhere, and poor performance can impact their productivity. Ensure satisfied users and flawless performance with digital experience monitoring (DEM).



**Get unified visibility across devices, networks, and apps**



**Detect issues early and quickly pinpoint root causes using AI**



**Collaborate effectively using data across IT operations, support, and security teams**





**Zscaler Digital Experience (ZDX)**...Ensure great user and customer experiences across all locations, devices, and apps!

Zscaler Digital Experience™ (ZDX) helps IT operations and service desk teams keep users productive. By monitoring performance from within users' devices, across networks, and to SaaS, cloud, or data center applications, IT teams can rapidly detect, troubleshoot, and resolve issues that impact the user and customer experience. Consolidating multiple monitoring tools reduces costs while helping you achieve:



**52% faster mean time to resolution for IT issues**



**20% fewer work hours lost to IT-related downtime**



**End-to-end visibility across your zero trust environment**





# DEFEND - Risk Management

Cloud Security Powered by Zscaler



## Zscaler Data Fabric for Security...Correlate disparate data for more effective exposure management!

The Zscaler Data Fabric for Security aggregates and unifies data across all your security tools and business systems. This rich source of security data truth serves as the foundation for the Zscaler Exposure Management portfolio, powering feedback loops between products to drive even richer insights.



### Connect all your security data sources

Seamlessly connect data from any source and harmonize, deduplicate, correlate, and enrich it to construct a unified view of risk across your environment.



### Apply your business logic

Quickly create custom scoring, automated workflows, and grouping rules that reflect your unique business processes and organizational structure.



### Report on the metrics that matter

Create the view you need with dynamic dashboards in a few clicks to showcase any combination of data from the fabric, using any factor or measurement.



### Get more from your Zscaler investment

Benefit from robust feedback loops between the Data Fabric and your deployed Zscaler solutions, driving even deeper exposure insights and automated risk reduction.



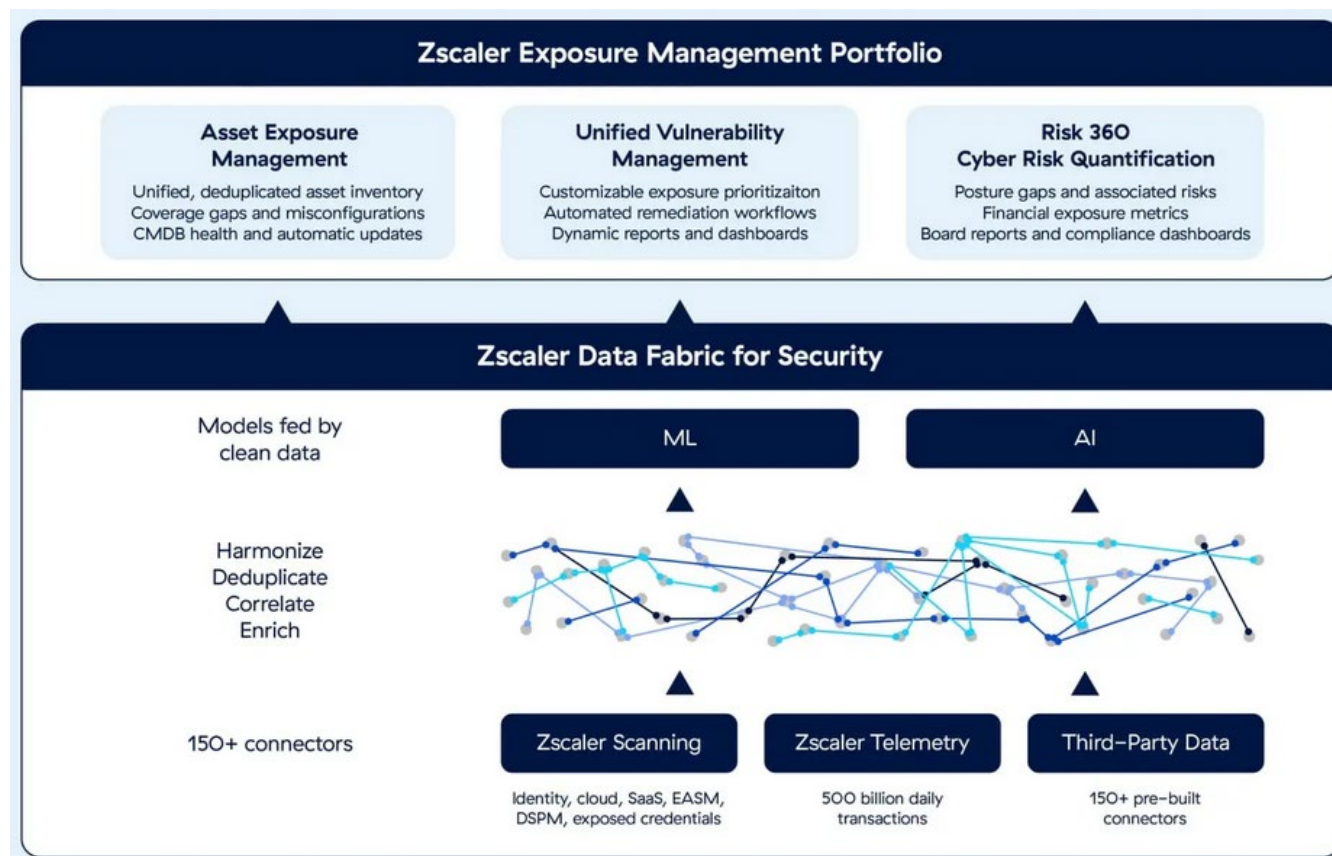
# DEFEND - Risk Management

Cloud Security Powered by Zscaler



**Zscaler Data Fabric for Security**...Drive your risk program with a flexible, extensible security data fabric!

The Zscaler Data Fabric for Security provides foundational capabilities that fuel current and future Zscaler applications. Built for the complex nature of security data, our customizable data model has the unique ability to add any data source, create advanced automated workflows, and build dynamic reports on any element.





# DEFEND - Risk Management

Cloud Security Powered by Zscaler



## Zscaler Asset Exposure Management...Reduce Risk with Asset Exposure Management (CAASM)!

### Get a high-fidelity “golden record” of all your assets

Achieve a complete, accurate, and context-rich asset inventory through a fundamentally different approach to CAASM, empowering you to reduce asset risk like never before.



Identify coverage gaps



Automate CMDB hygiene



Generate workflows for mitigation





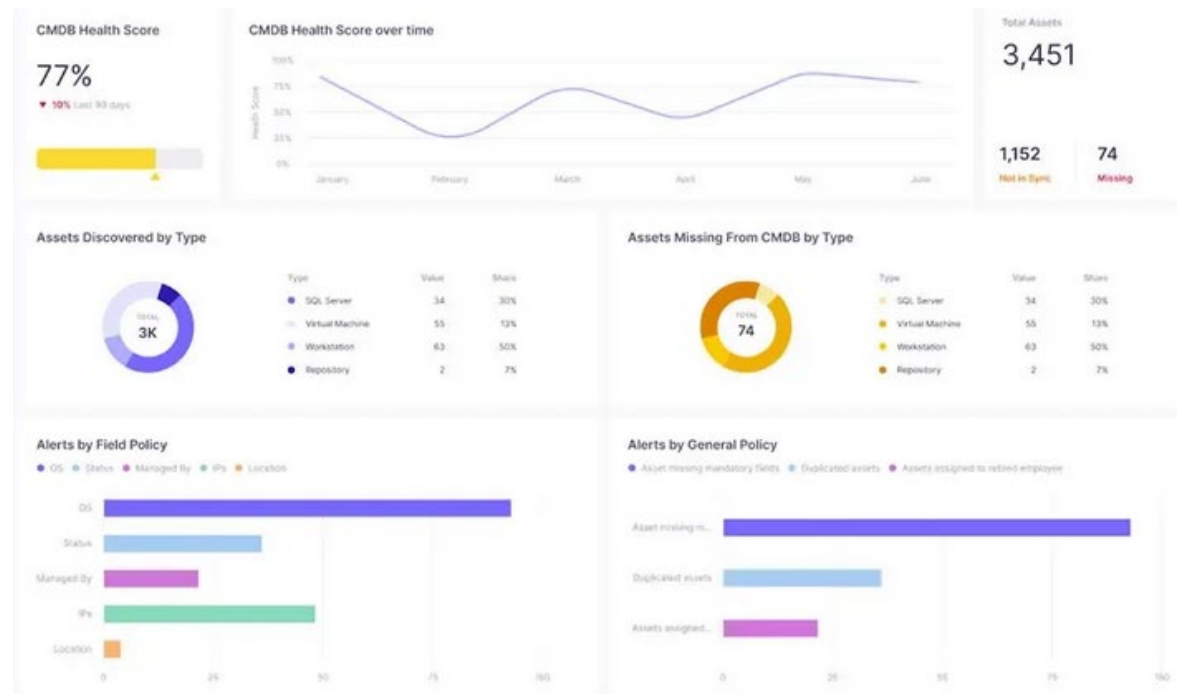
# DEFEND - Risk Management

Cloud Security Powered by Zscaler



## Zscaler Asset Exposure Management...Gain accurate and actionable CAASM insights!

Zscaler Asset Exposure Management provides rich visibility into organizational assets, enabling you to understand coverage and hygiene levels. Security, IT, and more can draw upon this single source of asset "truth" to help improve security and compliance outcomes.





# DEFEND - Risk Management

Cloud Security Powered by Zscaler



**Zscaler Risk 360...Cyber Risk Assessment and Quantification!**

**Enhance enterprise exposure management with an actionable risk framework**



**Gain a holistic understanding of risk exposure and top risk drivers**



**Investigate and initiate fixes for critical issues with guided workflows**



**Enhance executive and board-level reporting and guidance**



**Map to MITRE ATT&CK and the NIST Cybersecurity Framework**



**Accelerate CTEM projects with financial risk metrics and compliance insights**



# DEFEND - Risk Management

Cloud Security Powered by Zscaler



**Zscaler Risk 360...** Understand the financial impact of your cyber risk exposure!

Zscaler Risk360™ is a comprehensive and actionable risk management framework that delivers powerful cyber risk quantification by ingesting data from 150+ external sources and your existing Zscaler deployment, Risk360 creates a detailed view of your cyber risk posture and provides clear, actionable insights you can immediately apply to reduce risk.



**Intuitive risk visualization**



**Granular risk factors**



**Financial exposure detail**



**Board-ready reporting**

## An actionable risk framework built on the leading zero trust platform

### Unified dashboard

Replace multiple tools and spreadsheets with an interactive, data-driven dashboard that provides a holistic view of risk.

### Expansive correlation

Leverage our cloud native platform for correlated risk views of your workforce as well as third-party users, applications, and assets.

### Deeper risk insights

Turn data insights into actionable, policy-driven mitigation recommendations to improve your risk score and ultimately your risk posture.

### Financial risk mapping

Map risk directly to your potential financial exposure, including Monte Carlo simulations, for better decision-making and prioritized remediation.





# DEFEND - Risk Management

Cloud Security Powered by Zscaler



**Zscaler Risk 360...**Unparalleled visibility for unique risk insights and effective mitigation!



## Risk scoring

See a single risk score across your whole organization, tracked over time. Risk360 breaks down this score and measures it against the four key stages of a cyberattack.



## Contributing factors

Get accurate risk assessments based on risk factors across your IT environment. Risk360 continuously monitors, normalizes, and accounts for 100+ predefined as well as custom factors.



## Total visibility

Understand your entire risk profile with a global view across your environment. Risk360 enables you to go in depth on any risk and start mitigating it instantly.



## Actionable insights

Reduce the time from investigation to action with detailed insights about the issues driving your risk factors so you can quickly mitigate gaps and adjust policies.





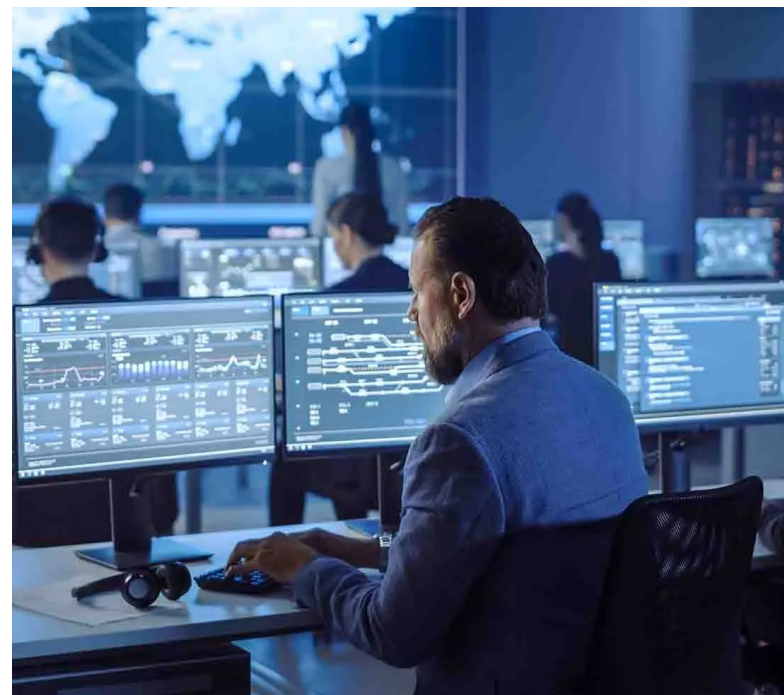
# DEFEND - Risk Management

Cloud Security Powered by Zscaler

Powered by  
**zscaler**

**Zscaler Unified Vulnerability Management...** Understand and address all your risks in one place!

The heart of managing risk is an effective risk-based vulnerability management program. Leverage Unified Vulnerability Management, built on our Data Fabric for Security, to prioritize your biggest risks, automate remediation workflows, and showcase your security posture improvements.





# DEFEND - Risk Management

Cloud Security Powered by Zscaler



**Zscaler Unified Vulnerability Management...**Efficiently address security gaps with contextual risk scoring and flexible workflows!

The Zscaler Unified Vulnerability Management solution taps into an aggregated, correlated data set to fuel a more effective and efficient vulnerability management program. UVM is powered by our Data Fabric for Security, which ingests data from traditional vulnerability and exploitability sources—as well as Zscaler and third parties—leveraging 150+ prebuilt data connectors. It correlates security findings and context spanning identity, assets, user behavior, mitigating controls, business processes, organizational hierarchy, and more. These rich insights bring your most important security gaps into focus, empowering you to meaningfully reduce your risk.

**80%**

of "critical" issues downgraded to "medium"

**6 mos.**

of custom integration work avoided

**10x**

triage capacity with complete context



# DEFEND - Risk Management

Cloud Security Powered by Zscaler



## Zscaler Unified Vulnerability Management...What sets Unified Vulnerability Management apart?



### Identify which security gaps and vulnerabilities to fix first

Prioritize risks in the context of your own risk factors and mitigating controls, based on input from 150+ data sources.



### Get always-up-to-date reports and dashboards

Get dynamic insights into your risk posture, KPIs, SLAs, and other metrics in one correlated, context-rich data set.



### Automate workflows to streamline remediation

Accelerate triage with custom workflows that provide remediation details and rationale, and automatically reconcile tickets.



# DEFEND - Risk Management

Cloud Security Powered by Zscaler



**Zscaler Deception...** Turn the tables on advanced attackers inside your network!

Attackers who gain access to your environment undetected think they've already won. Deploy deception technology for a proactive defense that lures and reveals sophisticated bad actors through realistic decoys.



## Stop lateral movement

by cutting off attackers with convincing honeypots



## Disrupt ransomware early

in any stage of an attack, limiting the blast radius



## Detect compromised users

and the abuse of stolen credentials



# DEFEND - Risk Management

Cloud Security Powered by Zscaler



**Zscaler Deception...**Detect advanced threats that bypass existing defenses!

Zscaler Deception deploys realistic decoys across your environment to lure, detect, and intercept active attackers. When a compromised user interacts with a decoy, your team gets an immediate alert—attackers never know they've been caught until it's too late.

As part of the cloud native Zscaler Zero Trust Exchange™ platform, Deception can rapidly and seamlessly deploy high-fidelity threat detection throughout your enterprise.



## De-risk your attack surface

Divert malicious actors away from critical targets like endpoints, identity systems, networks, applications, and the cloud.



## Detect threats that matter, faster

Detect compromised users, lateral movement, and ransomware with high-confidence IOCs and near-zero false positives.



## Contain threats in real time

Leverage zero trust access policies to dynamically limit or cut off access to sensitive SaaS services and internal applications.



# DEFEND - Risk Management

Cloud Security Powered by Zscaler



**Zscaler Deception...**Take a fresh approach to targeted threat detection!



## Protect users and applications with decoys

Silently detect threats and attacker activity with endpoint lures as well as decoy applications, servers, users, and other resources.



## Speed up incident response and reduce alert fatigue

Rapidly notify your security team of confirmed threats and breaches, with no false positives or added operational overhead.



## Put the burden of success back on attackers

Replace your attack surface with convincing fake targets attackers can't resist, and catch them the moment they take the bait.



# DEFEND - Risk Management

Cloud Security Powered by Zscaler



**Zscaler Breach Predictor...** Identify current attacks and anticipate potential breaches with the first preemptive threat detection and response solution!



## Contain attacks using real-time insights

with the visibility to stop emerging threats across petabytes of security data



## Predict and prevent potential breaches

by surfacing predictive attack paths that leverage ML analytics into unknown threats



## Reduce cyber risk and false positives

by empowering your threat hunting and SOC teams with context for faster remediation

## Reduce breach risk and improve security posture



## Improve attack awareness

Gain real-time visibility into attack pathways and malicious activity, including impacted users, to identify and contain attacks.



## Gain preemptive security

Identify and close potential attack paths with AI-powered breach probability scoring, reducing your overall cyber risk.



## Enhance SOC efficiency

Spend less time triaging false positives, and reduce the number of events requiring SOC responses, with optimized SOC workflows.





# DEFEND - Risk Management

Cloud Security Powered by Zscaler



**Zscaler Breach Predictor...**Preemptive security detection and response with AI-driven threat insights!



## AI-enriched by 500T daily signals

Harness the insights of AI/ML engines trained on extensive threat intelligence and security data from the world's largest security cloud, which processes 500 trillion daily signals.



## Full attack path visibility

Visualize malware attack patterns (with IOCs mapped to MITRE TTPs) and the impact on users in a single dashboard, enabling targeted threat mitigation and faster remediation.



## Quantified breach probability risk

Generate a breach probability score, based on advanced algorithms, that forecasts the likelihood of a breach and an attacker's next tactics, helping prioritize security efforts.



# DEFEND - Risk Management

Cloud Security Powered by Zscaler

Powered by  
**zscaler**

## Zscaler Identity Protection...Keep identities out of attackers' sights!

Know when attackers exploit, misuse, or steal enterprise identities and identity infrastructure. Reduce the risk of identity-based attacks with real-time identity threat detection and response (ITDR).

**Get full visibility** into misconfigurations, risky permissions, and exposed credentials

**Detect and respond** to attacks that abuse credentials and bypass MFA to move laterally

**Remediate and investigate** faster with SOC workflow and access policy integration





# DEFEND - Risk Management

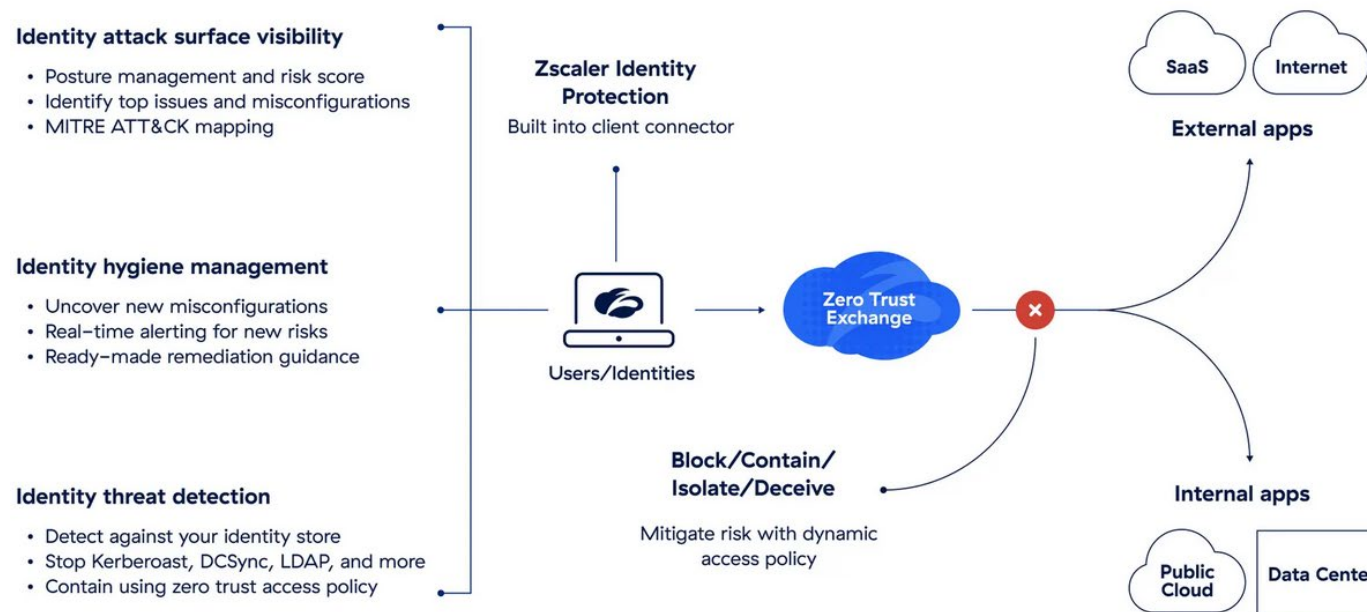
Cloud Security Powered by Zscaler

Powered by  
**zscaler**

## Zscaler Identity Protection...Unlock identity-first security!

Zscaler Identity Protection (ITDR) protects users with continuous visibility into identity configurations and risky permissions. Built into Zscaler Client Connector, our lightweight endpoint agent, it's a simple, low-touch approach to stopping identity-based attacks.

Set up Identity Protection in just minutes, and start improving your security posture immediately. Rapid assessments and alerts give your security team valuable insights into identity-related vulnerabilities and changes that increase your risk of a data breach.





# DEFEND - Risk Management

Cloud Security Powered by Zscaler



**Zscaler Identity Protection...**Reduce the risk of user compromise and privilege exploitation!



## Quantify and track identity risk

Understand how, why, and where you're vulnerable with identity security assessments, which include an intuitive risk score.



## Find and fix risky configurations

Uncover issues that open new attack paths, such as shared password exposure, stale passwords, and unconstrained delegation.



## Remediate with step-by-step guidance

Understand the issue, its impact, and affected users. Improve identity hygiene with remediation guidance in the form of video tutorials, scripts, and commands.



## Monitor changes in real time

Get timely alerts when configuration and permissions changes in identity systems introduce new risks.



## Detect identity attacks

Defend against vulnerabilities you can't remediate. Detect and stop attacks like DCSync, DCShadow, kerberoasting, and more when a compromise occurs.



## Contain identity threats

Use native integrations with Zscaler Private Access™, SIEMs, and leading EDRs to contain identity attacks in real time or use alerts as part of your SOC workflow.



# DEFEND - Risk Management

Cloud Security Powered by Zscaler



**Zscaler External Attack Surface Management...** Take action to reduce your attack surface!

**Discover your known and unknown internet-facing assets and prioritize findings with a comprehensive external attack surface management (EASM) solution.**

- See all perimeter-facing assets, including unknown assets
- Remediate risks before attackers can exploit them
- Save time and effort with automation and recommendations

## Identify, contextualize, and remediate attack surface risks



### Gain unmatched visibility

Get a complete, accurate view of your entire external attack surface, including known and unknown assets.



### Proactively manage risk

Stay ahead of bad actors by identifying and mitigating security risks before attackers can exploit them.



### Reduce your attack surface

Uncover shadow IT and unsecured assets that increase your exposure to cyberthreats.



### Increase team efficiencies

Automate asset discovery, risk scoring, and remediation guidance so your security team can focus on the most critical threats.



# DEFEND - Risk Management

Cloud Security Powered by Zscaler

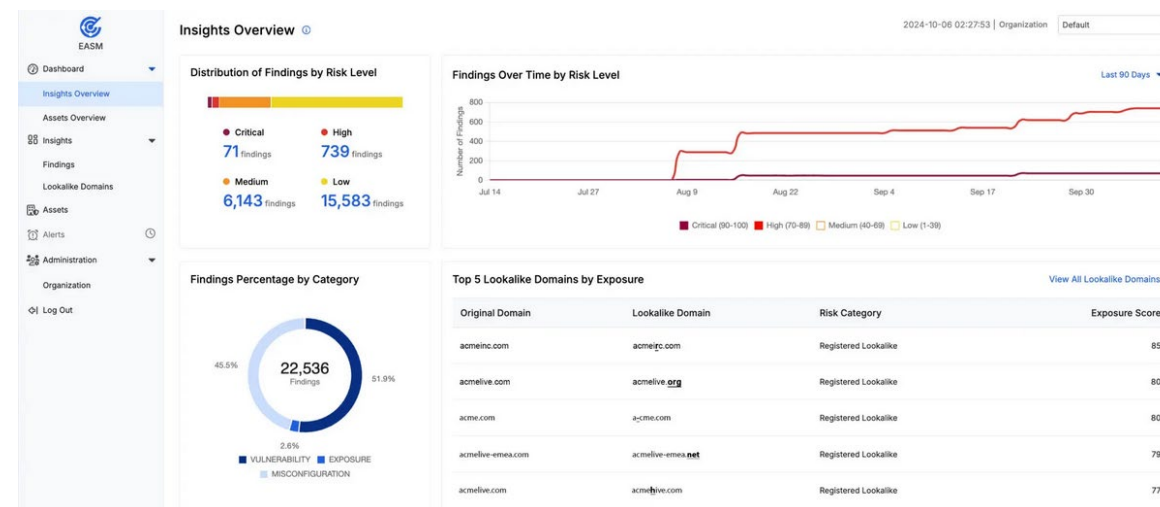


**Zscaler External Attack Surface Management...** Proactively secure your external digital footprint!

Reduce the exposure of your internet-facing assets with continuous visibility, risk assessment, and recommended remediation actions from Zscaler EASM.

Identify and analyze your exposed assets, and get the alerts and findings you need for proactive defense. Our EASM platform provides deep insights by uniquely combining:

- Open source intelligence (OSINT)
- Advanced scanning techniques
- Zscaler ThreatLabz research







# DEFEND - Risk Management

Cloud Security Powered by Zscaler



## Zscaler Managed Threat Hunting...Discover the power of Zscaler Threat Hunting!



Our expert threat hunters work 24/7 to uncover anomalies, sophisticated threats, and signs of malicious activity that evade traditional tools.

Using data from the world's largest security cloud alongside custom machine learning models, we proactively seek out, analyze, and neutralize threats.

## Empower your team to focus on what matters



### Hunt and detect advanced threats

Disrupt emerging and advanced persistent threats (APTs) by harnessing the expertise of our human-driven hunt team, powered by our global platform.



### Make our experts your experts

Reduce alert fatigue with our proprietary tooling and 24/7 hunt team. We distill billions of raw transactions into context-rich alerts and actionable insights for SecOps.



### Stop threats early in the attack chain

By analyzing web traffic rather than endpoint data, our threat hunting program detects and disrupts attacks earlier, before they breach your endpoints and cause damage.



### Gain customized expertise and insights

Zscaler Threat Hunting Advanced provides personalized onboarding, strategic briefings, tactical reports, and ongoing threat hunting support.





# DEFEND - Risk Management

Cloud Security Powered by Zscaler



## Zscaler Managed Threat Hunting...Our threat hunting methodology!

Our hunters collect, correlate, and monitor across our global install base, leveraging cloud-scale telemetry to identify and defend against emerging threats, exploits, and tactics based on:

- Zero trust principles
- Threat intelligence
- Hypothesis testing
- Custom playbooks
- AI + human expertise





# DEFEND - Risk Management

Cloud Security Powered by Zscaler



## Zscaler Managed Threat Hunting...A proven cyberthreat hunting approach!

### Telemetry

Our best-in-class secure web gateway (SWG) processes more than 400 billion transactions per day, offering our threat hunters unparalleled real-time visibility.

### Refine

With the help of AI, our hunters refine, enrich, and enhance billions of transactions with threat intelligence. Using custom tools and threat hunting playbooks, we can detect threat actors trying to blend in with legitimate network traffic.

### Analyze

Our threat hunters zoom in and out of different enriched data views, conducting round-the-clock structured, unstructured, and situational hunting operations with advanced telemetry.

### Context

Combining internal and external intelligence, our threat hunters piece together contextual and supporting information into clear insights.

### Escalate

Once all relevant information and intelligence is stitched together, a member of our hunting team escalates actionable alerts to your SOC/IR team.

### Revise

Our team continually learns, documents, and develops new playbooks to enhance our products and our threat hunting efficiency.



# MANAGED - Lingo Router & Switch

*Infrastructure hardware, Switches, Routers, Firewall, etc*

Remote management  
of onsite infrastructure  
hardware



Virtual Tech



Managed Router



Managed Switch



Managed Firewall



Managed Wi-Fi



# What is a Virtual Tech?

---

A **Virtual Tech** is a Lingo networking device that allows our Support Engineers to securely remote access your network to do testing on your computer networks current issue and help get it resolved much faster than waiting for a Tech to be deployed onsite.

## Reasons to utilize a Virtual Tech:

- 🌱 Customer has a lot of locations that want to deploy any of Lingo's many VoIP options and need assistance in running Lingo's **V**oice**R**eadiness**T**esting and remediate the issues with the under-lying broadband carrier.



# What is a Managed Router?

---

A **Router** is a networking device that forwards data packets between computer networks. **Routers** perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or e-mail, is in the form of data packets.

## Reasons to utilize a Managed Router:

Customer wants / needs a managed Edge Device but already has a firewall. This can be added to any broadband connection.



## Managed Router

- (3) LAN / WAN Gigabit RJ-45 ports



## Managed Router

- (3) LAN / WAN Gigabit RJ-45 ports
- (1) SFP WAN/LAN assignable port





# MAX-BR1-MINI-LTE-US-T-M

Powered by  
**peplink**



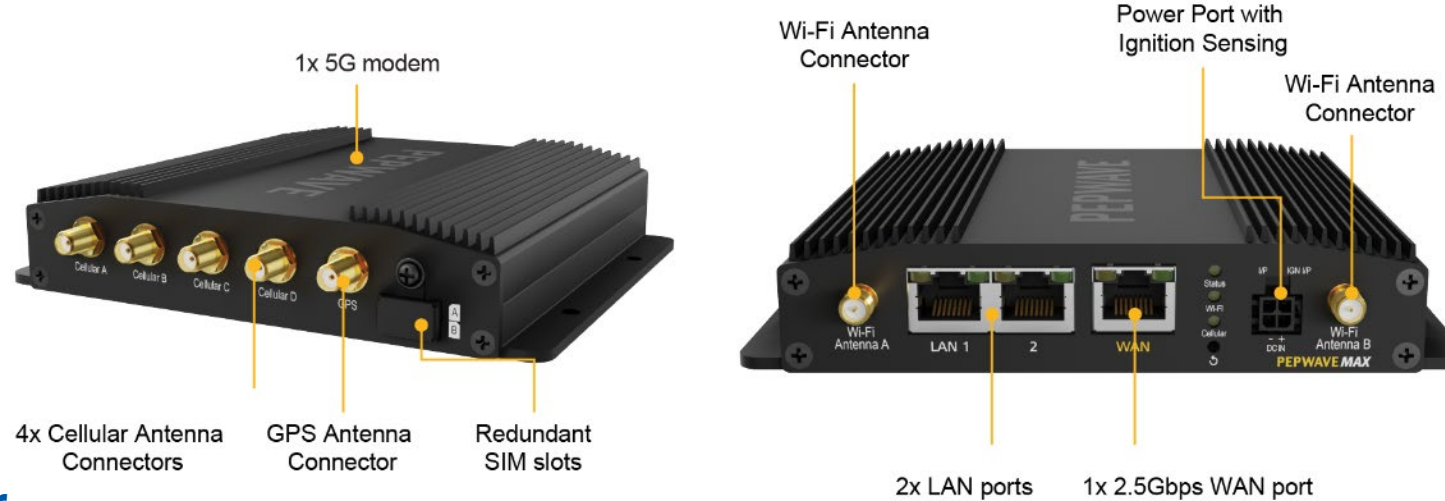
## Managed Router

- 1x Industrial-Grade 4G LTE Router
- 1x Embedded 4G LTE Modem (for use in the US)
- 1x Optional Ethernet WAN
- Optional WAN Failover
- No Wi-Fi no GPS



# MAX-BR1-PRO-5G-T-PRM

Powered by  
**peplink**



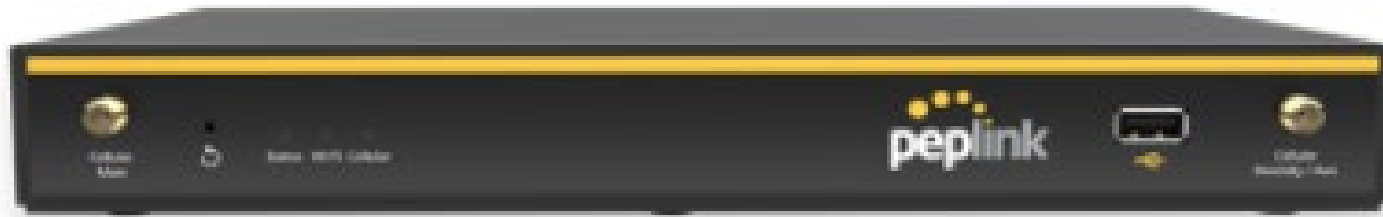
## Managed Router

- Internet Connections Supported: 1 Embedded 5G/Cat 20 LTE, 1 Wired WAN, Wi-Fi as WAN\*
- Networks Supported for Embedded Modem: 5G (NSA) Sub 6Ghz: n1, n2, n3, n5, n28, n41, n66, n71, n77, n78, n79; 4G bands: B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B42, B46, B48, B66, B71
- Certifications: AT&T, FirstNet, T-Mobile, Us Cellular, Verizon, and Verizon CBAND
- Wi-Fi Standard: Wi-Fi 6, 2X2 MU-MIMO
- Wi-Fi Range: 250-300' through walls, much greater unobstructed (variable depending on interference from other electronics and physical interference such as walls and ceilings)
- Ethernet ports: 2 GbE LAN + 1 GbE WAN
- The BR1 Pro 5G uses a 4FF Nano SIM (not 2FF like many other routers)



# BPL-021X-LTE-US-T-PRM

Powered by  
**peplink**



## Managed Router

- 1x GE WAN ports
- 4x GE LAN ports
- 1x LTE modem (CAT-4)
- 900Mbps Router Throughput



# What is a Managed Switch?

---

A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer of the OSI model.

## Reasons to utilize a Managed Switch:

- PoE+ Power for Access Points & IP Phones
- Traffic Shaping (Voice)
- Additional ports needed
- VLAN Segmentation



# Sophos C18CTCH (CS101-8FP) PoE Switch

Powered by  
**SOPHOS**

The Sophos Switch CS101-8FP is a switch with 8 gigabit ports. It also has 2x 1G/10G SFP+ ports. Additionally, there is a variant with PoE. The Sophos Switch CS210-8FP delivers a PoE budget of up to 110 watts on 8 ports.



Number of 10 GE SFP+ Ports:	2
Number of GE 10/100/1000 RJ45 Ports:	8
PoE Budget:	110 Watt
Switch Throughput:	20 Gbps



# Sophos C28CTCH (CS210-8FP) PoE Switch

Powered by  
**SOPHOS**

The Sophos Switch CS210-8FP is a switch with 8 2.5 Gig ports. It also has 2x 1G/10G SFP+ ports. Additionally, there is a variant with PoE. The Sophos Switch CS210-8FP delivers a PoE budget of up to 240 watts on 8 ports.



Number of 10 GE SFP+ Ports:	2
Number of GE 10/100/1000/2.5 Gig RJ45 Ports:	8
PoE Budget:	240 Watt
Switch Throughput:	120 Gbps



# Sophos CS110-24FP (C12CTCH) PoE Switch

Powered by  
**SOPHOS**

The Sophos Switch CS110-24 is a switch with 24x GE ports. It also has 4x 1G/10G SFP+ ports. Additionally, there is a variant with PoE. The Sophos Switch CS110-24FP delivers a PoE budget of up to 410 watts on 8 ports.



Number of 10 GE SFP+ Ports:	4
Number of GE 10/100/1000 RJ45 Ports:	24
PoE Budget:	24 (15.4W) /13 (30W)
Switch Throughput:	128 Gbps





# Sophos CS210-24FP (C22CTCH) PoE Switch

Powered by  
**SOPHOS**

The Sophos Switch CS210-24 is a switch with 16x GE ports & 8 2.5 Gig ports. It also has 4x 1G/10G SFP+ ports. Additionally, there is a variant with PoE. The Sophos Switch CS110-24FP delivers a PoE budget of up to 410 watts on 8 ports.



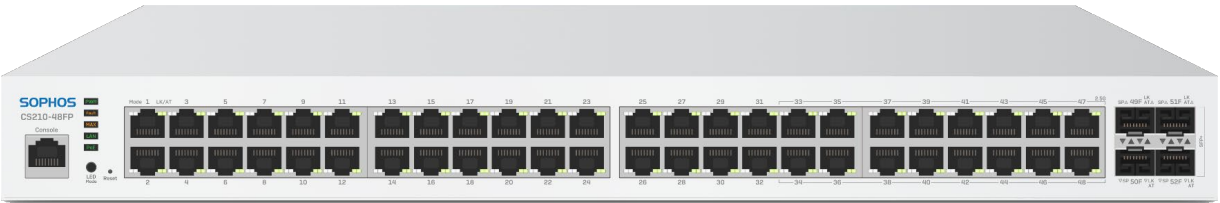
Number of 10 GE SFP+ Ports:	4
Number of GE 10/100/1000 RJ45 Ports:	16
Number of GE 2.5 Gig RJ45 Ports:	8
PoE Budget:	410 Watt
Switch Throughput:	128 Gbps



# Sophos C14CTCH (CS110-48FP) PoE Switch

Powered by  
**SOPHOS**

The Sophos Switch CS110-48FP is a switch with 48x GE ports. It also has 4x 1G/10G SFP+ ports. Additionally, there is a variant with PoE. All the 48 ports are PoE-capable.



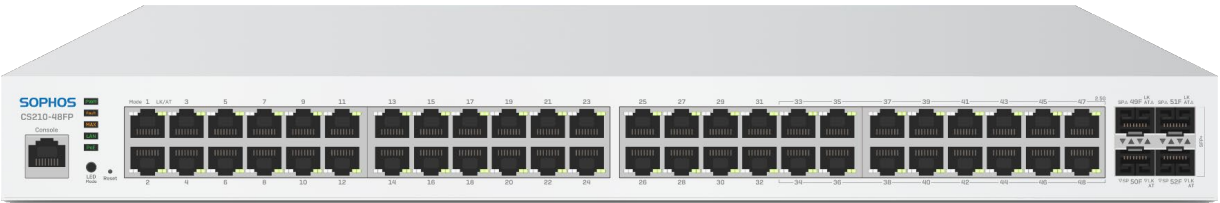
Number of 10 GE SFP+ Ports:	4
Number of GE 10/100/1000 RJ45 Ports:	48
PoE Budget:	740 Watt
Switch Throughput:	176 Gbps



# Sophos C24CTCH (CS110-48) PoE Switch

Powered by  
**SOPHOS**

The Sophos Switch CS110-48 is a switch with 32x GE ports & 16 2.5 Gig ports. It also has 4x 1G/10G SFP+ ports. Additionally, there is a variant with PoE. All the 48 ports are PoE-capable.



Number of 10 GE SFP+ Ports:	4
Number of GE 10/100/1000 RJ45 Ports:	32
Number of GE 2.5 Gig RJ45 Ports:	16
PoE Budget:	740 Watt
Switch Throughput:	176 Gbps



# JetStream TL-SG2210MP

Powered by  
**TP-LINK®**

TP-Link JetStream Gigabit Smart Switch TL-SG2210MP is equipped with 8 gigabit RJ45 ports, all RJ45 Ports support the 802.3af/at (PoE+) standard with a total PoE power budget of 150W and useful PoE power management features.



Number of Gigabit SFP Ports:	2
Number of Gigabit PoE+ RJ45 Ports:	10 PoE+
PoE Budget:	150 Watt
Switch Throughput:	104 Gbps



# NetVanta 1560-08-65W

Powered by  
**Adtran**

The NetVanta 1560 Series of enterprise-class, fully managed Gigabit PoE+ switches are the best switches for supporting highly resilient IoT, cloud applications, and Voice over IP (VoIP).



<b>Number of Gigabit SFP Ports:</b>	2
<b>Number of Gigabit PoE+ RJ45 Ports:</b>	8 PoE+
<b>PoE Budget:</b>	65 Watt
<b>Switch Throughput:</b>	176 Gbps



# PoE+ ES-8-150W SWITCH

With a comprehensive user interface and support for fiber connectivity the EdgeSwitch 8-Port 150-Watt Managed PoE+ Gigabit Switch with SFP from Ubiquiti Networks is a full featured networking solution. Along with the two 1 Gbps SFP Ethernet ports, you can take advantage of 8 Gigabit Ethernet ports supporting a max power over Ethernet wattage of 34.2 watts per port.



Number of Gigabit SFP Ports:	2
Number of Gigabit PoE+ RJ45 Ports:	8 PoE+
PoE Budget:	150 Watt
Switch Throughput:	20 Gbps



# GS752-TPv2 SWITCH

Powered by  
**NETGEAR**

The Netgear ProSAFE GS752TPV2 48-Port PoE+ Cloud Managed Smart Switch is designed to be the central control point of networks, allowing you to upgrade your network with simple plug and play installation, while still maintaining control over your network.



<b>Number of 10 GE SFP+ Ports:</b>	4
<b>Number of Gigabit PoE+ RJ45 Ports:</b>	48 PoE+
<b>PoE Budget:</b>	380 Watt
<b>Switch Throughput:</b>	104 Gbps





# GS728TP PoE+ Switch

Powered by  
**NETGEAR**

The NETGEAR PoE+ Gigabit Smart switches with Remote/Cloud management provides a great value, with configurable L2 network features like VLANs and PoE operation scheduling, allowing SMB customers to deploy PoE based VoIP phones, IP cameras, video over-IP endpoints and wireless access points simply and securely



<b>Number of 10 GE SFP+ Ports:</b>	4
<b>Number of Gigabit PoE+ RJ45 Ports:</b>	24 (16 PoE, 8 PoE+)
<b>PoE Budget:</b>	192 Watt
<b>Switch Throughput:</b>	56 Gbps



# What is a Managed Wi-Fi?

---

A Wi-Fi network is simply an internet connection that's shared with multiple devices in a home or business via a wireless router. The router is connected directly to your internet modem and acts as a hub to broadcast the internet signal to all your Wi-Fi enabled devices. This gives you flexibility to stay connected to the internet as long as you're within your network coverage area.

## Reasons to utilize a Managed Wi-Fi:

- Have limited staff
- Don't have time to keep up on product upgrades & changes
- Rather have product Subject Matter Expert handle for me



# CLOUD WI-FI

*Powered by Arista, Sophos & Ubiquiti*

Powered by  
**SOPHOS**



Wi-Fi POWER OPTIONS








# Secure Employee Facing Wi-Fi

Powered by  
**SOPHOS**

Sophos AP6 Series with Wi-Fi 6, broad device support is guaranteed with all AP6 models offering support for the 2.4 and 5 GHz bands.

Improved performance and better security with WPA3 add to the benefits of this WLAN generation. Wi-Fi 6E extends the capabilities and features of Wi-Fi 6 into the 6 GHz band

Model	AP6 420	AP6 420E	AP6 840	AP6 840E	AP6 420X
					
WLAN Standards	802.11ax Wi-Fi 6	802.11ax Wi-Fi 6/6E	802.11ax Wi-Fi 6	802.11ax Wi-Fi 6/6E	802.11ax Wi-Fi 6
Management	Sophos Central (see management and support below). Local web interface (single AP6 only) AP6 Series access points cannot be managed from any Sophos firewall.				
Deployment	Indoor; desktop, wall, or ceiling mount				Outdoor; pole/wall mount IP67
Radios*	<b>Dual Radio</b> 1 x 2.4 GHz single-band 1 x 5 GHz single-band	<b>Tri-radio</b> 1x 2.4 GHz single-band 1x 5 GHz single-band 1x 6 GHz single-band	<b>Dual Radio</b> 1x 2.4 GHz single-band 1x 5 GHz single-band	<b>Tri-radio</b> 1x 2.4 GHz single-band 1x 5 GHz single-band 1x 6 GHz single-band	<b>Dual Radio</b> 1x 2.4 GHz single-band 1x 5 GHz single-band
Antennas	Internal omnidirectional	Internal omnidirectional	Internal omnidirectional	Internal omnidirectional	External omnidirectional
Antenna Options	-	-	-	-	120° Sector, 30° Directional
DFS	✓	✓	✓	✓	✓
Performance	2 x 2:2	2 x 2:2	4 x 4:4	4 x 4:4	2 x 2:2
Interfaces	1x 1GE w/PoE+	1x 2.5G w/PoE+	1x 2.5G w/PoE+	1x 2.5G w/PoE++ 1 x 2.5G without PoE	1x 2.5G w/PoE+
Power (max.)	17.5 W	24.25 W	30 W	45 W	30 W
Power-over-Ethernet (min.)**	802.3at (PoE+) Suitable PoE+ injector or switch available for separate purchase	802.3at (PoE+) Suitable PoE+ injector or switch available for separate purchase	802.3at (PoE+) Suitable PoE+ injector or switch available for separate purchase	802.3bt (PoE++) Suitable PoE++ injector or CS210-8FP switch available for separate purchase	802.3at (PoE+) Suitable PoE+ injector or switch available for separate purchase
Dimensions Width x Height x Depth	183 x 35 x 183 mm 7.2 x 1.38 x 7.2 inches	183 x 35 x 183 mm 7.2 x 1.38 x 7.2 inches	225 x 43 x 225 mm 8.86 x 1.54 x 8.86 inches	225 x 43 x 225 mm 8.86 x 1.54 x 8.86 inches	260.5 x 69 x 180 mm 10.26 x 2.72 x 7.09 inches
Weight	0.7 kg	0.7 kg	1.2 kg	1.2 kg	1.6 kg
Certifications and Compliance	CB, UL, CE, FCC, ISSED, RCM, TEC EN 60601-1-2 (Medical Equipment Directive)	CB, UL, CE, FCC, ISSED, RCM, TEC Plenum-rated (UL2043) EN 60601-1-2 (Medical Equipment Directive)	CB, UL, CE, FCC, ISSED, RCM, TEC Plenum-rated (UL2043) EN 60601-1-2 (Medical Equipment Directive)	CB, UL, CE, FCC, ISSED, RCM, TEC Plenum-rated (UL2043) EN 60601-1-2 (Medical Equipment Directive)	CB, UL, CE, FCC, ISSED, RCM, TEC EN 60601-1-2 (Medical Equipment Directive)



# UCaaS - What is Hosted Voice?

Voice Over Internet Protocol



UCaaS POWER OPTIONS



Lingo Voice Difference

- With analog phone systems, one phone is connected to another via a PSTN (Public Switched Telephone Network). The phone uses electrical signals to generate audio in the speaker at the receiving end.
- Hosted Voice, on the other hand, transfer voice data over the internet.
- It starts with an IP Phone that turns your live voice communication into data packets. Unlike an on-site VoIP solution, the data packet first travels to one of many data centers.
- If you already have a PBX in place, you maybe able to take advantage of VoIP features with SIP Trunking.



# D815WB Desk Phone

Powered by  
**snom**

## Higher End 10-line phone VoIP Desk Phone

An outstanding feature of the Snom D815WB is the large, high-resolution display, which offers unrivalled image quality. Whether for displaying call information, speed-dialling contacts or settings - the D815WB ensures that all information is displayed clearly and concisely. The Snom D815WB also has nothing to fear in terms of audio: thanks to the integrated dual band Wi-Fi & Bluetooth, calls are always transmitted in excellent voice quality.

### Call Handling Features

- Large 5-inch IPS color display
- 2x USB 2.0 high-speed connection
- 10 programmable function keys
- Integrated dual-band Wi-Fi
- Integrated Bluetooth
- Antibacterial housing





# D810WB Desk Phone

Powered by  
**snom**

## Lower End 4-line phone VoIP Desk Phone

The Snom D810WB is the medium sized high-end display, which offers unrivalled image quality. Whether for displaying call information, speed-dialling contacts or settings - the D810WB ensures that all information is displayed clearly and concisely. The Snom D810WB also has nothing to fear in terms of audio: thanks to the integrated Wi-Fi & Bluetooth, calls are always transmitted in excellent voice quality.

### Call Handling Features

- 3.36" (320x240) color LCD 2x USB 2.0 high-speed connection
- 4 (12) configurable self-labeling multicolor LED keys
- 1 USB port
- Integrated Wi-Fi
- Integrated Bluetooth
- Electronic Hook Switch (EHS) support for wireless headsets
- 2-port Gigabit Ethernet switch (RJ45)







# D8C Expansion Module

Powered by  
**snom**

## 60 Programmable buttons on 3 tabs

Connected to the telephone via USB using plug and play, the Snom D8C expands the D8xx series telephones with an additional large screen and a wide range of application options. With the help of the 20 physical (60 virtual) freely programmable and multi-colored LED function keys, the status of colleagues, for example, can be quickly identified and a call quickly forwarded. If the corresponding line or the LED function line lights up red or yellow, the person in question is inactive or busy.

## Call Handling Features

- 6.8 Zoll (17.2 cm) TFT color screen
- Expansion module with 60 programmable buttons on 3 sides
- Plug-and-play
- Expandable with up to two additional modules (total of 3 modules)



**The M500 Pro DECT Multicell Base Station brings scalability and an enhanced user-experience through programmable keys in a solution that can fit all business needs.**

Minimalistic sleek design with reliable range and offering audio-enhancing technologies, the M500 Pro Series is your one-stop shop. Experience true team transparency for easy call handling. Intuitive to use, the illuminated keys provide visibility for efficient call management and provisioning to expand to multiple base stations has never been easier. Snom handles your office needs so you can focus on what matters most. The M500 Pro can be paired with up to 2 base stations for expanded DECT range and call capacity. Offering both color handsets and desk phones, each equipped with programmable buttons to customize speed dials, busy monitoring and other programmable functions. Over-the-air updates keep all the handsets and desk phones up-to-date, and seamless handover between M500 bases means you don't need to worry about dropped calls as you roam around the office, warehouse or into the break room.

## Call Handling Features

- Wireless DECT technology, providing better reliability and security than WiFi
- Intuitive, programmable keys for both phone and base station
- Eight phones can connect to eight calls simultaneously
- Unique paging system allows for broadcast paging to entire team
- Long range inside and around the facility with no dead zones or dropped calls





# M55 DECT Cordless Handset

Powered by  
**snom**

The M55 handset is one of two devices that pair to the M500 Pro DECT Multicell Base Station. This family of devices has Wireless DECT technology, providing better reliability and security than WIFI. The M55 is wireless and allows you the freedom to roam freely within your space without being tied down to one location.

## Call Handling Features

- 2.4" (240 x 320) color LCD
- 6 backlit dual-color LED programmable keys
- Integrated Bluetooth
- HD audio support
- Integrated belt clip
- HAC compliant
- Up to 19 hours of talk time
- Supports Key System Emulation



Programmable  
Keys



Integrated  
Bluetooth®



DECT 6.0



OTA Updates



Belt Clip



Long Stand-by  
Time

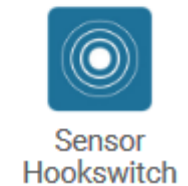
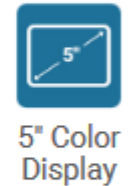
# M58 DECT Desk Phone

Powered by  
**snom**

The M58 Desk Phone is one of two devices that pair to the M500 Pro DECT Multicell Base Station. This family of devices will streamline your internal and external communications. The M58 does not need an ethernet connection. This gives you the flexibility to place the desk phone anywhere within your workplace.

## Call Handling Features

- 5" (480 x 272) color LCD
- 8 Line Keys
- Integrated Bluetooth
- HD audio support
- HAC compliant
- Supports Key System Emulation





# WP810 Cordless Phone



## Basic Cordless Wi-Fi IP Phone with Integrated Dual-Band 802.11a/b/g/n/ac and 6-hour talk time

The WP810 includes advanced antenna design and roaming support. By adding 6-hour talk time and HD voice with dual-MICs, the WP810 offers an affordable option and comes equipped with a combination of features, mobility and durability to suit all portable telephony needs.

### Call Handling Features

- 2 lines
- Dual-band Wi-Fi with efficient antenna design and advanced roaming support
- HD voice & dual MIC design with AEC and Noise Shield Technology
- Rechargeable 1500mAh battery, 6 hour talk time, 120-hour standby
- Configurable button for push-to-talk
- Micro USB port and 3.5mm headset jack







# GRP2612W IP Phone



## Call Handling Features:

- 4-line Support
- 5 navigation/menu keys
- 9 dedicated function keys for: MESSAGE(with LED indicator), TRANSFER, HOLD, HEADSET, MUTE, SEND/REDIAL, SPEAKERPHONE, VOL+, VOL-
- 2.4 Inch (320x240) TFT color LCD
- Built-in dual-band Wi-Fi support
- HD Voice
- Up to 16 digital BLF Key
- Dual switched auto-sensing 10/100 Mbps Ethernet ports
- RJ9 headset jack
- PoE Support
- Wall Mountable





# Edge 220 VoIP Phone



## User Interface Features

- 2.8" color LCD (320x240 pixel resolution) screen
- 1 USB 2.0 Type-C® (for media and storage applications)

## Call Handling Features

- 4-line keys supporting up to 16 SIP lines with pagination
- Enhanced Feature Keys make powerful feature shortcuts on line key appearances or soft keys
- Shared call/bridged line appearance
- Busy Lamp Field (BLF)
- Call transfer, hold, divert (forward), park, pickup
- Called, calling, connected party information
- Local three-way audio conferencing
- One-touch speed dial, redial
- Remote missed call notification
- Bluetooth® 5.0
- 2 RJ-45 (10/100/1000BASE-TX Mbps)



**Entry Point IP Phone for Hosted Voice use**





# Edge 350 VoIP Phone



## User Interface Features

- 2.8" color LCD (320x240 pixel resolution) screen
- 1 USB 2.0 Type-C® (for media and storage applications)

## Call Handling Features

- 8 programmable line keys supporting up to 32-line key assignments
- 4 context-sensitive soft keys
- 4-way navigation key cluster with center Select key
- Shared call/bridged line appearance
- Busy Lamp Field (BLF)
- Call transfer, hold, divert (forward), park, pickup
- Called, calling, connected party information
- Local three-way audio conferencing
- One-touch speed dial, redial
- Remote missed call notification
- Bluetooth® 5.0
- 2 RJ-45 (10/100/1000BASE-TX Mbps)
- Wi-Fi network connectivity



## Entry Point IP Phone for Hosted Voice use



# Edge 450 VoIP Phone



## User Interface Features

- Color IPS LCD 320 x 240 (primary); 240 x 320 (secondary) screens
- 1 USB 2.0 Type-C® (for media and storage applications)

## Call Handling Features

- 14 line keys supporting up to 44 line key assignments
- 4 context-sensitive soft keys
- 4-way navigation key cluster with center Select key
- Shared call/bridged line appearance
- Busy Lamp Field (BLF)
- Call transfer, hold, divert (forward), park, pickup
- Called, calling, connected party information
- Local three-way audio conferencing
- One-touch speed dial, redial
- Remote missed call notification
- Bluetooth® 5.0
- 2 RJ-45 (10/100/1000BASE-TX Mbps)
- Wi-Fi network connectivity



**Entry Point IP Phone for Hosted Voice use**



# Edge 550 VoIP Phone



## User Interface Features

- Color IPS LCD 800 x 480 screen
- 1 USB 2.0 Type-C® (for media and storage applications)

## Call Handling Features

- 12 line keys supporting up to 48 line key assignments
- 4 context-sensitive soft keys
- 4-way navigation key cluster with center Select key
- Shared call/bridged line appearance
- Busy Lamp Field (BLF)
- Call transfer, hold, divert (forward), park, pickup
- Called, calling, connected party information
- Local three-way audio conferencing
- One-touch speed dial, redial
- Remote missed call notification
- Bluetooth® 5.0
- 2 RJ-45 (10/100/1000BASE-TX Mbps)



**Entry Point IP Phone for Hosted Voice use**



# VWX 250 VoIP Phone



## User Interface Features

- 2.8" color LCD (320x240 pixel resolution)
- Adjustable base height
- Two USB ports (2.0 compliant) for media and storage applications

## Call Handling Features

- 4-lines (programmable line keys)
- Up to 34-line key assignments for lines, contacts, and features supported with pagination
- Enhanced Feature Keys make powerful feature shortcuts on line key appearances or soft keys
- Shared call/bridged line appearance
- Busy Lamp Field (BLF)
- Call transfer, hold, divert (forward), park, pickup
- Called, calling, connected party information
- Local three-way audio conferencing
- One-touch speed dial, redial
- Remote missed call notification



**Entry Point IP Phone for Hosted Voice use**



# Vox 350 VoIP Phone



## User Interface Features

- 3.5" color LCD (320x240 pixel resolution)
- Adjustable base height
- Two USB ports (2.0 compliant) for media and storage applications

## Call Handling Features

- 6-lines (programmable line keys)
- Up to 34-line key assignments for lines, contacts, and features supported with pagination
- Enhanced Feature Keys make powerful feature shortcuts on line key appearances or soft keys
- Shared call/bridged line appearance
- Busy Lamp Field (BLF)
- Call transfer, hold, divert (forward), park, pickup
- Called, calling, connected party information
- Local three-way audio conferencing
- One-touch speed dial, redial
- Remote missed call notification



## Mid-Point IP Phone for Hosted Voice use





# VVX 450 VoIP Phone



## User Interface Features

- 4.3" color LCD (480x272 pixel resolution)
- Adjustable base height
- Two USB ports (2.0 compliant) for media and storage applications

## Call Handling Features

- 12-lines (programmable line keys)
- Up to 34-line key assignments for lines, contacts, and features supported with pagination
- Enhanced Feature Keys make powerful feature shortcuts on line key appearances or soft keys
- Shared call/bridged line appearance
- Busy Lamp Field (BLF)
- Call transfer, hold, divert (forward), park, pickup
- Called, calling, connected party information
- Local three-way audio conferencing
- One-touch speed dial, redial
- Remote missed call notification



## Mid-Point IP Phone for Hosted Voice use



# EXP43 – Sidecar for VVX-450

Powered by  
**Yealink**

## Display

- 5 in LCD WVGA (480x800 pixel) resolution
- Color TFT graphical user interface

## Display Feature Keys

- 30 multifunctional line keys configurable as line registration, call appearance, speed dial, DSS or BLF
- Dual-color (red or green) illuminated LEDs for line status information
- 3-page keys for additional line appearances

## Compatible VVX Phone Models

- VVX 450
- Communication with host phone and/or other modules via USB port

## Expandability

- Up to two Expansion Modules can be attached to the VVX 450







# Trio 8300 – Conference Phone



The Polycom Trio 8300 Conference Phone offers a clear and rich audio experience to enhance conference collaboration. Its versatile, modular architecture ensures there is a solution just right for your space. Teams can connect and boost productivity with unparalleled audio clarity. It has a classic interface and future-proof flexibility for ease of use. Given its features, this conference phone is ideal for small rooms.



## Features:

- Voice Activity Detection
- Low-delay Audio Packet Transmission
- Packet Loss Concealment
- 3x Cardioid Microphones
- Poly NoiseBlock
- Adaptive Jitter Buffers
- Communications Protocol: SIP



W60B, W56H, W73H, T54W, T41S (w/ DD10K Dongle)

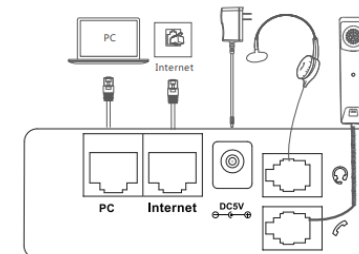
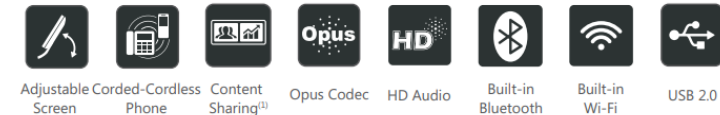
Powered by  
**Yealink**



**For Hosted Voice use**  
**\*\*\*Can over-subscribe HV seats\*\*\***

## Features:

- 10-line keys with LED
- 10-line keys can be programmed up to 21 various features (3 pages)
- 6 Navigation Keys
- 4 context-sensitive “soft” keys
- 7 Feature keys: message, headset, hold, mute, transfer, redial, hands-free speakerphone
- Volume control keys
- Illuminated mute/headset/hands-free speakerphone key
- 4.3" 480 x 272-pixel color display with backlight (16-bit depth color)
- Adjustable LCD screen
- Built-in Bluetooth 4.2
- Built-in dual band 2.4G/5G Wi-Fi (802.11a/b/g/n/ac)
- USB 2.0 port for USB recording, wired/wireless USB headsets and EXP50
- Dual-port Gigabit Ethernet
- PoE support
- HAC Handset
- Paperless label design
- Wall mountable



## Features:

- 12-line keys with LED
- 8-line keys can be programmed up to 21 various features (3 pages)
- 6 Navigation Keys
- 5 Feature keys: mute, headset, message, redial, hands-free speakerphone
- 2 Volume control keys
- Illuminated mute/headset/hands-free speakerphone key
- 2.8" 320x240-pixel color LCD with back
- Built-in Bluetooth 4.2
- Built-in dual band 2.4G/5G Wi-Fi (802.11a/b/g/n/ac)
- 2 USB 2.0 ports for USB recording, wired/wireless USB headsets and EXP50
- Dual-port Gigabit Ethernet
- PoE support
- HAC Handset
- Paperless label design
- Wall mountable



## Features:

- 4-line keys with LED
- 4-line keys can be programmed up to 12 DSS keys (4-page view)
- 6 Navigation Keys
- 5 Feature keys: mute, headset, message, redial, hands-free speakerphone
- 2 Volume control keys
- 2.4" 320x240-pixel color display with backlight
- Bluetooth via Yealink BT50/BT51A Bluetooth adapters
- Built-in dual band 2.4G/5G Wi-Fi (802.11a/b/g/n/ac)
- USB 2.0 port for USB recording, wired/wireless USB headsets
- Dual-port Gigabit Ethernet
- PoE support
- HAC Handset
- Paperless label design
- Wall mountable







# EXP50 – Sidecar for T5 Series Phones

Powered by  
**Yealink**

## Display Features

- 4.3" 272x480-pixel color display with backlight
- 16-bit depth color
- Three page views are possible
- Different color icons for each function shown on the LCD

## Features Keys & Indicators

- 20 physical keys each with a dual-color LED
- 40 additional keys through page switch
- 3 independent control keys with illuminated LED are used for fast switching pages
- Programmable for shared line, BLF List, call park, conference, forward, group pickup, group listening, LDAP, XML Browser...





# CP925 – Conference Phone

Powered by  
**Yealink**

The Yealink CP925 is a touch-sensitive HD conference phone designed for small to medium conference rooms.

CP925 adopts a business and introverted design that perfectly matches the calm style of the conference room, but also an acoustics fabric, which is impervious to any accidental liquid spills. Its fingerprint-proof LCD screen with a clear UI interaction page makes it easy for everyone to control the meeting.

CP925 has seven built-in microphones, providing you with a clear and natural conference call experience. In addition, you can connect CP925 to your mobile device (such as a smartphone) via Bluetooth to achieve a hybrid UC meeting. Its 20-foot and 360-degree Omni-direction sound pickup provide users with a clear and natural voice conference experience.



## Features:

- Conference VoIP phone
- IEEE 802.11a/b/g/n (Wi-Fi) / Bluetooth 4.2
- SIP
- SRTP
- with Bluetooth interface
- 5-way call capability
- SIP v2





# CP935W-Base – Conference Phone

Powered by  
**Yealink**

## General Features

- 4" capacitive touch screen
- Black acoustics fabric, resistant to water/oil/stain
- Battery capacity: 7800mAH, charging time: 4 hours
- Up to 167 hours standby time in DECT mode (in ideal conditions)
- Up to 15 hours talk time (in ideal conditions)

## Audio Features

- Optimal HD audio
- Yealink Noise Proof Technology, Smart Noise Filtering
- 20-foot (6-meter) microphone pickup range
- Built-in 6-microphone array for 360-degree voice pickup
- Full-duplex speakerphone with AEC

## Phone Features

- 5-way conference call

## Connectivity

- Built-in Bluetooth/Wi-Fi
- 1 x USB 2.0 Type-C port





# DIRECT ROUTING: Both Native & Valet Options

Voice, Video & Collaboration

## What are the Main Advantages of Direct Routing?

- Seamless calling from within MS Teams - desktop, mobile, endpoint
- Advanced calling features - voice mail, forwarding, hunt groups, auto-attendant
- Instant access to your contacts - uses MS Teams contact list
- One-click meeting creation
- Collaborate with both internal and external users at the same time

## Why Lingo for Your Direct Routing Needs?

Our MS Team's Direct Routing solution combines up-to-the-moment integration to the Microsoft Graph API, automated scripting of Microsoft PowerShell and marries it to the TeamMate Connector – a purpose-built interoperation layer that allows us to normalize communication with any SIP PBX, SIP Trunk or SMS gateway.



UCaaS POWER OPTIONS



Lingo Voice Difference



# DIRECT ROUTING: Native Vs. Valet Option

Voice, Video & Collaboration

## Direct Routing that utilizes MS Native dialing application:

- Requires Microsoft Voice license (E3+Voice or E5 that includes Voice)
- Fully integrated and can seamlessly work with MS CoPilot & all MS approved 3<sup>rd</sup> Party integrations
- Seamless calling from within MS Teams - desktop, mobile, endpoint
- Advanced calling features - voice mail, forwarding, hunt groups, auto-attendant
- Instant access to your contacts - uses MS Teams contact list

## Direct Routing that utilizes Lingo's Valet dialing application:

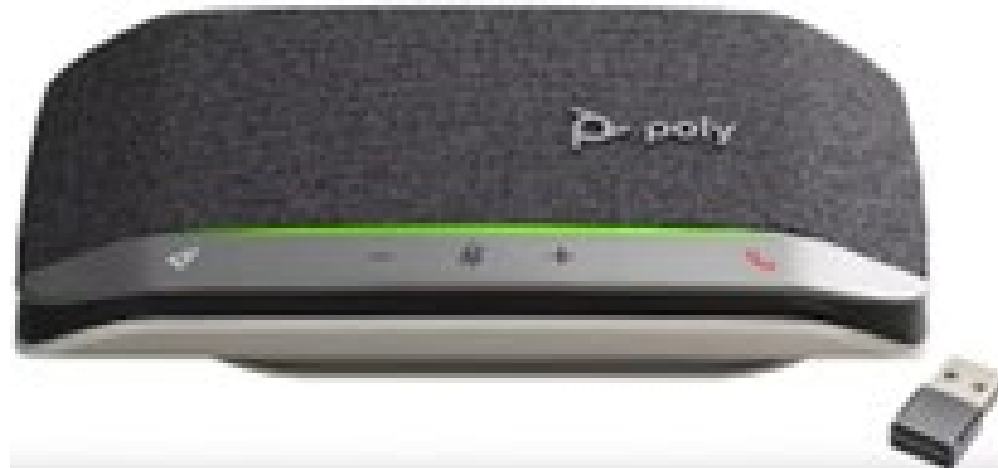
- Only requires a single free MS Teams Phone Resource Account licenses
- Fully integrated and can seamlessly work with MS CoPilot & all MS approved 3<sup>rd</sup> Party integrations
- Seamless calling from within MS Teams - desktop, mobile, endpoint
- Advanced calling features - voice mail, forwarding, hunt groups, auto-attendant
- Instant access to your contacts - uses MS Teams contact list



# CCX 400 MS Teams Phone



**Entry Level IP Phone for MS Teams**



## Speaker Phone for MS Teams



# SIP-MP56 MS Teams Phone

Powered by  
**Yealink**



## Mid-level IP Phone for MS Teams





# VP59 MS Teams Phone

Powered by  
**Yealink**



**Upper-end IP Phone for MS Teams**  
**\*\*\*Has built-in Camera\*\*\***



# CP900 MS Teams Speaker Phone



## Speaker Phone for MS Teams



# The Lingo Difference

- Voice Readiness Test with True Moss Score

Number of Concurrent VoIP Lines (1-50)

Apply

VoIP Lines Simulated: 4

Initiating Client Connection

Please wait while we establish the client connection.



- Traffic Shaping Edge Device (8:1 Ratio)



- Virtual Tech (BNA)





# HOSPITALITY VOICE

Easy-to-manage VoIP guest services phone system

**Deliver awesome guest and employee experiences with Lingo hospitality cloud solutions.**



Lingo helps hotels elevate how they interact with guests from the booking experience to check-in to check-out. We modernize your property to help you deliver a differentiated guest experience that builds long-term guest and brand loyalty.



# HOSPITALITY VOICE

Easy-to-manage VoIP guest services phone system

**Lingo helps hotels elevate how they interact with guests from the booking experience to check-in to check-out. We modernize your property to help you deliver a differentiated guest experience that builds long-term guest and brand loyalty.**

Reduce complexity by getting everything you need from one partner in a simple, turnkey package including:



Automated Guest Amenities



Cloud PBX Phone System



SIP Trunking



POTS Replacement



Reservation Center



Internet

## Why Hospitality Brands Love This Solution

- Easy-to-manage VoIP hotel phone systems.
- All-inclusive monthly pricing eliminates varying month-to-month costs.
- Full-feature integration with 70+ Property Management Systems.
- Enterprise-grade 99.999% availability, security and reliability.
- Concierge white glove discovery, deployment and support.
- Trusted solutions and services backed by telephony and hospitality experts.



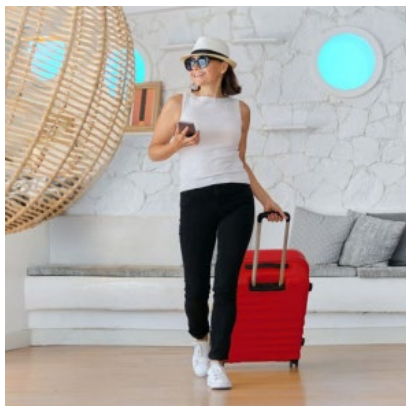
# HOSPITALITY VOICE

Easy-to-manage VoIP guest services phone system

## Cloud PBX Phone Systems

Enjoy crystal-clear voice with unlimited calling in the United States, Canada and Mexico.

- Cloud-based service with all inclusive pricing and support from a single vendor.
- Easy-to-use web portal to make changes to your phone system like call routing and greetings.
- Re-use your existing equipment and wiring.
- Never miss a call with the Ooma mobile app or portable handset.
- Keep improving the guest and employee experience with modern call analytics.



## SIP Trunking

Get internal, inbound, outbound, local and long distance calling with advanced voice capabilities using internet and premises-based telephony equipment.

- We partner directly with multiple carriers as an Incumbent Local Exchange Carrier (ILEC), not as a reseller, so you always receive the best rates.
- Quickly add new phone lines or modify phone service without business disruptions or buying new hardware.
- Interoperability with all major native SIP trunk solutions and analog/digital PBX phone systems.
- Automatic failover protection helps ensure calls are never dropped due to natural disasters, power outages or ISP downtime.
- E911 dialing capabilities enhance compliance with regulations such as Kari's Law and RAY BAUM's Act.
- Sophisticated, easy-to-configure call flows empower administrators to route calls to the right employees and departments.

## Automated Guest Amenities

Increase revenue and brand loyalty by personalizing the guest experience.

- Welcome VIP guests and loyalty members with special messages and offers.
- Inform guests of checkout procedures before check-out.
- Promote property amenities and events.
- Enable guest-centric wake-up call service and voicemail management.
- Notify guests of anticipated service impacts, retract unread messages when issue is resolved.



# Voice Power Options

---



Option #2 – 8,16,24 & 48 PoE+ Switch







# INTEGRATED VOICE

*VoIP, Analog, IP-PRI & SIP Trunking*



Analog Handoff



IP-PRI Handoff



SIP Trunk Handoff



# Handy Tone 812 ATA



## Analog Telephone Adapter

- For use with Integrated Voice
- (1) LAN RJ-45 port
- (1) WAN RJ-45 port
- (2) RJ-11 ports



# Handy Tone 818 ATA



## Analog Telephone Adapter

- For use with Integrated Voice
- (1) LAN RJ-45 port
- (1) WAN RJ-45 port
- (8) RJ-11 ports



# Adtran 908 for ATA

Powered by  
**Adtran**



## Analog Telephone Adapter

- For use with Integrated Voice
- (1) WAN RJ-45 port
- (24) ports via Amphenol cable & 66-block



# Trunking

Powered by:  broadsoft &  netsapiens

## What is SIP Trunking?

**SIP Trunking** enables the end point's PBX to send and receive calls via an IP network, such as the Internet or private WAN. As SIP is applied for the signaling protocol for multiple real-time application, SIP trunk is able to control voice, video and messaging applications.

- Can be delivered over an existing broadband connection
- Empowers companies with significant productivity-enhancing benefits
- Reduced costs through convergence of voice and data
- Seamless integration with existing IP PBX system
- Scalable growth supported with the addition of new trunks
- Uses proprietary, BGP gateways to ensure maximum performance
- Eliminate waste when you pool and burst call paths across multiple locations
- Delivers voice and data traffic over a single dynamic broadband pipe
- Connects from Lingo digital voice platform to existing IP PBX
- Customized flexible calling plans to meet unique calling requirements

## What is IP-PRI?

PRI stands for **P**rietary **R**ate **I**nterface — a traditional means of communication able to carry 23 concurrent calls. IP-PRI is one of the latest evolutions of TDM-PRI.

## IP-PRI vs TDM-PRI

TDM-PRI is a copper-based voice solution that only carries 23 analog voice channels, while IP-PRI allows you to choose as many voice channels you want — similar to the functionality of SIP Trunking — and keep the network that you're on. For an IT specialist, IP-PRI makes it easier to monitor phone and internet service, since TDM-PRI is a standalone circuit.

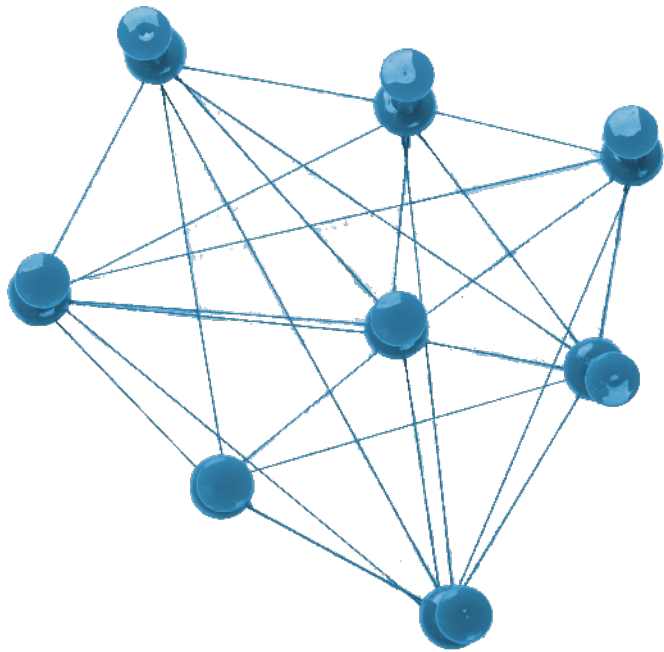
Lingo's IP-PRI has an IP to TDM gateway — a piece of networking equipment that is able to convert session initiation protocol (SIP) signaling into PRI.





## IP-PRI Adapter

- For use for IP-PRI
- (1) WAN RJ-45 port
- (1) IP-PRI port



# POTS ALTERNATIVE

# POTS ALTERNATIVE: Fire, Life & Safety + Voice

## Strategy

- For use with Integrated Voice
- Voice Service Alternative
- Supplemental to Lingo VoIP solution
- Lines that would have been left on the LEC: Fire, Life, Safety
- Secondary as Voice replacement

## Key Capabilities

- Comprehensive Technology.
- Redundancy: Wireless backup
- Fire, Security, Elevator, POS, Fax, etc.
- Simple POTS
- E911

## Components

- No Line Minimum
- Price Elements:
  - Box (Includes Warrantee)
  - Seat License (FXS, FLS)
  - Install





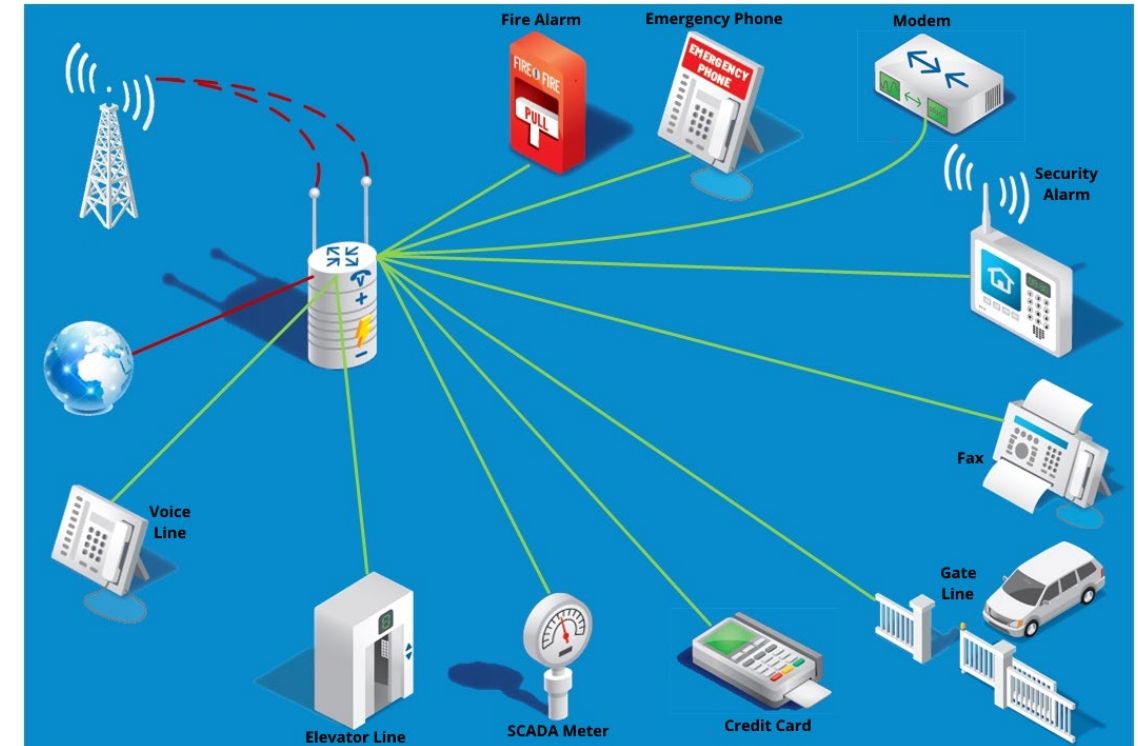
# ALERT+ :Fire, Life Safety + Voice

Fire, Life & Safety Lines

Walk Away From The HIGH Price of Old Copper POTS Lines and Move to Lingo's POTS Alternative Solutions

## The Advantage:

- Multiple Options: Comcast, Cox, Ooma, Spectrum, & Velocity
- See significant savings and improved repair SLAs
- Up to 24 hours of battery backup
- Future-proof against sun-setting POTS lines
- Single leg, Active / Active & Active / Standby Options
- Compliance with NFPA 72 (National Fire Alarm and Signaling Code)
- Compliance with UL-864 (Standard for Control Units and Accessories for Fire Alarm Systems)
- A Managed Facility Voice Network (MFVN) device ensures the service quality and reliability from your location to the PSTN or other MFVN peer network





# ALERT+:Hardware Options

Fire, Life & Safety Lines



	COMCAST	COX	OOMA	SPECTRUM	VELOCITY
Features					
Hardware Make / Model	Arris / eMTA	Arris / eMTA	Ooma Airdial	Arris / eMTA	DataRemote CDS-9010 / CDS-90X1
Max Lines	24 (8 ports x 3 eMTAs)	12 (4 ports x 3 eMTAs)	4 Lines per Unit No Cap	12 Lines per eMTA No Cap	2 or 8 Lines per Unit No Cap & Can Mix
Battery Backup	Up to 8 Hours of stand-by depending on use	Up to 8 Hours of stand-by depending on use	Up to 24 hours stand-by depending on use	Up to 8 Hours of stand-by depending on use	Up to 24 hours stand-by depending on use
E911 Form	Lingo Form	Lingo Form	Carrier Form	Carrier Form	Carrier Form
Porting Numbers	Customer Name BTN LOA CSR/Bill Copy (recent) Phone Numbers Porting Account number porting number from: Authorized Users on LEC Account *LEC (company) number is porting from *LEC Account Pin (if applicable) *LEC Account Passcode (if applicable) Full or Partial port If partial, disposition of remaining TN's (i.e., are we disconnecting remaining #'s)  *** Comcast & Spectrum utilize Carrier LOA Cox, Ooma & Velocity utilize Lingo's LOA ***				
Broadband	RG6 Coax	RG6 Coax	Any	RG6 Coax	Any
LTE	N/A	N/A	VZ, AT&T, T-Mobile	N/A	VZ, AT&T, T-Mobile
LTE Only	N/A	N/A	Yes	N/A	Yes
Multi-Path	N/A	N/A	Yes	N/A	No



# Voice Features



lingo.com






	COMCAST	COX	OOMA	SPECTRUM	VELOCITY
<b>Features</b>					
Caller ID	*	*	*	*	
Recent Call Logs			*		
Call Forwarding	*	*	*	*	
Call Transfer	*	*		*	*
3-Way Calling		*	*	*	*
Speed Dial		*		*	
Call Return		*	*		
Call Waiting		*			
Do Not Disturb		*			
Call Hold	*	*			
Last Number Redial		*			
Anonymous Call Rejection		*	*		
Directed Call Pickup		*			
Priority Alert		*			
Selective Call Acceptance		*			
Selective Call Rejection (Call Block)		*	*		
Simultaneous Ring Personal		*			
Speed Dial 100		*			
Speed Dial 8		*			
Call Park	*	*			
Call Pickup		*			
Incoming Call Plan		*			
Series Completion		*			
Feature Access Codes (star codes)		*			
Conference Calling	*				
Extension Dialing	*				
Hunt Groups	*		*		
Customized Caller ID	*				
Call Forward Unreachable	*				
Ring Down			*		*
Ring No Answer			*		
International Call Blocking	*	*	*	*	
Call Conference			*		
Backup Number			*		
SMS / Texting & Email Alerts			*		
Voicemail via Email / SMS			*		

[Return to Main Menu](#)

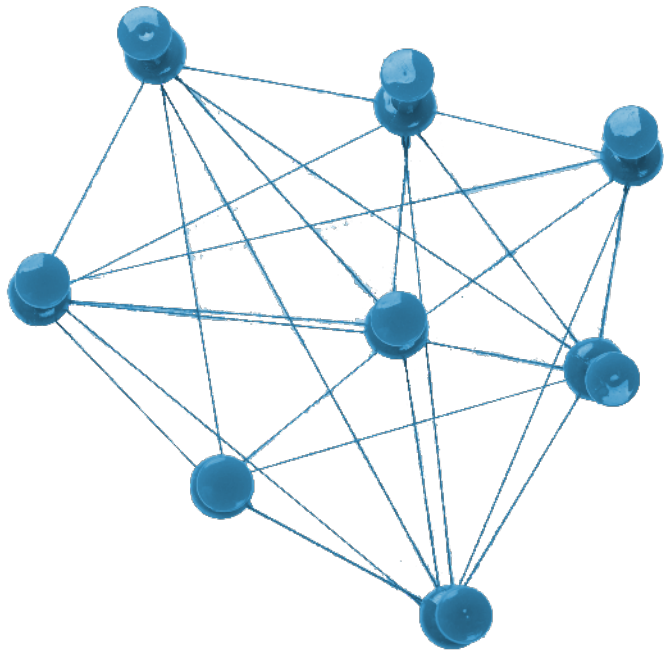


# SD-WAN POTS (Software Defined Plain Old Telephone Service)

**SD-WAN POTS** is a POTS Alternative offering that is delivered as VoIP calls through an encrypted managed IP voice network tunnel to ensure top call quality. It utilizes the tried-and-true tested SD-WAN technology to ensure that not only is the call quality the best possible outcome, but also ensures those calls are securely encrypted covering any concerns with HIPAA, PCI and your secure voice communications needs. This offering also comes with a battery backup that can last up to 24 hours depending on use,

-  Delivered as VoIP calls through an encrypted managed IP voice network tunnel to ensure top call quality
-  Each line comes with unlimited domestic outbound calling
-  Dual Leg Connection – Primary Broadband with LTE Standby
-  Inbound & Outbound calling is fully integrated to the Public Switched Telephone Network (PSTN)
-  Built-in 24-Hour Battery backup





# MISCELLANEOUS SERVICES



# Miscellaneous Services

---



## FAX SOLUTIONS

*Cloud, UCaaS, VoIP & POTS*



## TSaaS

*Site Assessment, Cabling & Hardware Installation*



## Virtual Tech



## E-Rate – Universal Service Programs



## Lingo Rebilling - Invoice Integration



# FAX SOLUTIONS

Cloud, UCaaS, VoIP & POTS



## Secure Cloud Fax



## Lingo UCaaS Fax



## Lingo VoIP Fax



## Traditional POTS Fax



# Secure Cloud Fax

---

Tired of replacing toner and buying paper for faxes? Want to better protect your data, reduce your eco-footprint, and lower faxing costs? Lingo's Secure Cloud Fax, powered by eFax Corporate®, lets you send and receive faxes anywhere using cloud faxing.

**Secure Cloud Fax** is a simple, reliable fax solution that allows you to enjoy significant cost savings. With Secure Cloud Fax, your faxes are sent straight to your email, keeping them private, confidential, and secure. Choose from multiple cloud-based plan options that are scalable and flexible to meet your exact needs.

- Our easy-to-use web portal is accessible via PC, Mac, and mobile
- Email
- Multi-function printers
- Online web portal
- Desktop, smartphone, or tablet apps



# UCaaS Fax

---

The **Fax to E-Mail** Upgrade option allows Fax (T.38) messages are converted to TIFF e-mail documents and delivered to the user's mail server via SMTP. From there they may be viewed, printed, or forwarded to another user.

Blending fax messaging with the voice messaging service, broadens the Unified Messaging capabilities of Lingo's VoIP offerings to provide end-users with the flexibility to use and manage their messages from any location that can access their e-mail system.

With the **Fax to E-Mail** messaging service, users can send faxes to group distribution lists in a manner similar to the use of e-mail distribution lists. Because fax messaging are routed as e-mail attachments, users minimize the need for physical fax machines and phone lines dedicated to fax use.

The fax capability also leverages VoIP globalization, enabling end-users with distributed locations-such as frequent business travelers or businesses with multiple offices-to maintain a fax number in one country and receive faxes in other parts of the world as they travel.



# VoIP Fax

---

You don't have to change your phone system to improve the way your business communicates. Get the best of both worlds with **Lingo VoIP Fax**. Better value, more flexibility, robust features, and real-time failover. That's how Lingo does phone service! Installed by Lingo's white glove technicians across the U.S., Integrated Voice & Fax brings new life to existing phone systems by adding cutting-edge VoIP features and central management.

- Our easy-to-use web portal is accessible via PC, Mac, and mobile
- Lingo's voice network is powered by BroadSoft, the industry leader in cloud unified communications
- Noninvasive troubleshooting and VoIP-readiness testing
- Inside wiring services available
- Industry-leading technology, deployed by expert Lingo technicians
- 24x7 support and advice when you need it most, provided by Lingo's Expert Network Center



# Traditional POTS Fax

---

Traditional Fax Lines are POTS phone lines that are attached only to a fax machine.

- Check for availability...less & less true POTS (Copper) options. Should be looking at migrating to VoIP options, such as hosted voice, integrated voice, or POTS-in-a-Box replacement (EPIK)





# TSaaS - Technical Support as a Service

Site Assessment, Cabling & Hardware Installation

## Are you Facing These Challenges?

- Employees on-site that lack the skill set to perform this work
- Budget or time to send employees to other sites
- A way to contract qualified technicians in the areas where you operate
- Knowledge to write a scope of work to get the work completed
- Time to research local talent
- Onboarding newly acquired locations

## Applications for TSaaS

- Site Surveys
- Wiring new buildings for Ethernet
- Replacing UPS batteries
- Fiber Optic Extensions
- Installing Home Theater/Audio Visual
- PC replacement
- Printer installation
- Mounting Webcams
- Electrical work
- Replacing automatic door
- Alarm system installation
- Kiosk installation
- Onboarding newly acquired locations
- Point of Sale (POS) installation



# E-Rate: Universal Service Program for Schools and Libraries

Lingo's The Federal Communications Commission (FCC) offers an E-Rate program designed to make telecommunications and information services more affordable for public K-12 schools, private non-profit schools, public libraries, school libraries, non-instructional facilities, and selected non-traditional educational facilities. Specific eligibility is determined by the FCC.

The FCC, Universal Service Administrative Company (USAC), and USF work together to provide the assistance to schools and libraries. USAC manages the program with funding from the Universal Service Fund (USF) ([fcc.gov/general/universal-service-fund](https://fcc.gov/general/universal-service-fund)).

The E-Rate program provides discounts to eligible schools, libraries, and selected educational facilities ranging from 20 to 90 percent on qualifying telecommunications services and Internet access as well as certain connectivity management/maintenance costs.

If demand for E-Rate money is greater than the available funds, funding is allocated first to the highest poverty schools and libraries, then the next-highest poverty applicants, and so on.



# Lingo's Rebilling - Invoice Integration

**Lingo's Rebilling/Invoice Integration** gives you greater control of all your business communication services and delivers total visibility and accountability for each location on your Lingo invoice.

- Include your other business communications services in your Lingo account hierarchy
- We take over payment, management and bills on our consolidated billing platform
- Combine all your business communications services onto your Lingo invoice
- Implement Moves, Adds, Changes and Deletions (MACDs) to all locations
- Redeploy your employee resources to revenue-generating functions
- Write one check for all of your business communications services
- Reduce risk of disconnection from late payment or lost invoices
- Onboarding newly acquired locations
- Track and trend you're invoicing to maximize savings
- Identify any unused services or disparate charges
- Report, manage and resolve issues
- Reduce invoice processing fees



# Lingo Odds & Ends

---



E-Rate – Universal Service Programs



Lingo Rebilling - Invoice Integration



# E-Rate: Universal Service Program for Schools and Libraries

---

The Federal Communications Commission (FCC) offers an E-Rate program designed to make telecommunications and information services more affordable for public K-12 schools, private non-profit schools, public libraries, school libraries, non-instructional facilities, and selected non-traditional educational facilities. Specific eligibility is determined by the FCC.

The FCC, Universal Service Administrative Company (USAC), and USF work together to provide the assistance to schools and libraries. USAC manages the program with funding from the Universal Service Fund (USF) ([fcc.gov/general/universal-service-fund](https://fcc.gov/general/universal-service-fund)).

The E-Rate program provides discounts to eligible schools, libraries, and selected educational facilities ranging from 20 to 90 percent on qualifying telecommunications services and Internet access as well as certain connectivity management/maintenance costs.

If demand for E-Rate money is greater than the available funds, funding is allocated first to the highest poverty schools and libraries, then the next-highest poverty applicants, and so on.



# Lingo's Rebilling - Invoice Integration

**Lingo's Rebilling/Invoice Integration** gives you greater control of all your business communication services and delivers total visibility and accountability for each location on your Lingo invoice.

- Include your other business communications services in your Lingo account hierarchy
- We take over payment, management and bills on our consolidated billing platform
- Combine all your business communications services onto your Lingo invoice
- Implement Moves, Adds, Changes and Deletions (MACDs) to all locations
- Redeploy your employee resources to revenue generating functions
- Write one check for all of your business communications services
- Reduce risk of disconnection from late payment or lost invoices
- Onboarding newly acquired locations
- Track and trend you're invoicing to maximize savings
- Identify any unused services or disparate charges
- Report, manage and resolve issues
- Reduce invoice processing fees