zscaler™

DATA SHEET

Zero Trust Device Segmentation

Simplified lateral threat protection for branch, factory and campus networks

Integral to Zscaler Zero Trust Networking, Zscaler Device Segmentation helps IT teams reduce risk, gain compliance, and improve business uptime by eliminating sources of lateral threat movement in enterprise networks.

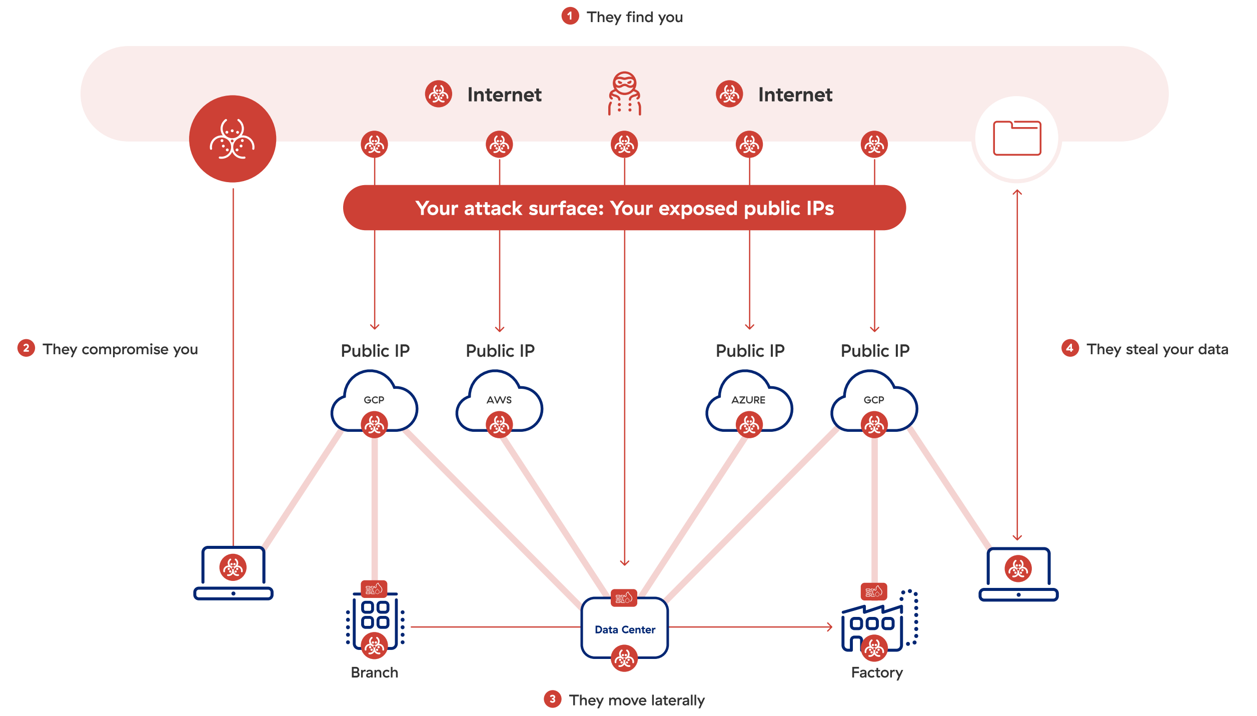
The Evolving Threat and Compliance Landscape

Recently, there has been a surge in alerts and warnings about cyberattacks from state-sponsored threat actors on US critical infrastructure. On February 7, 2024, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), along with the National Security Agency, issued an advisory warning to government organizations regarding cyber actors poised to disrupt critical infrastructure, such as transportation systems, oil and natural gas pipelines, water treatment plants, and electric grids. This complements similar actions taken by TSA for securing airports, aircraft operators, and railways, the recent DOE cybersecurity baseline, and the near final NERC update to CIP-015-1.

OT/IoT technologies were designed to deliver speed and transaction efficiency first, with security as a secondary goal. Unfortunately, OT/IoT is now a favorite cybercriminal target, with a 400% year-over-year increase in attacks, according to Zscaler ThreatLabz research. Ransomware is the most popular attack strategy, and 61% of all breaches in the last year targeted OT-connected organizations.

Zscaler Zero Trust Networking

A simpler, safer and cost effective means for users, devices and workloads to communicate



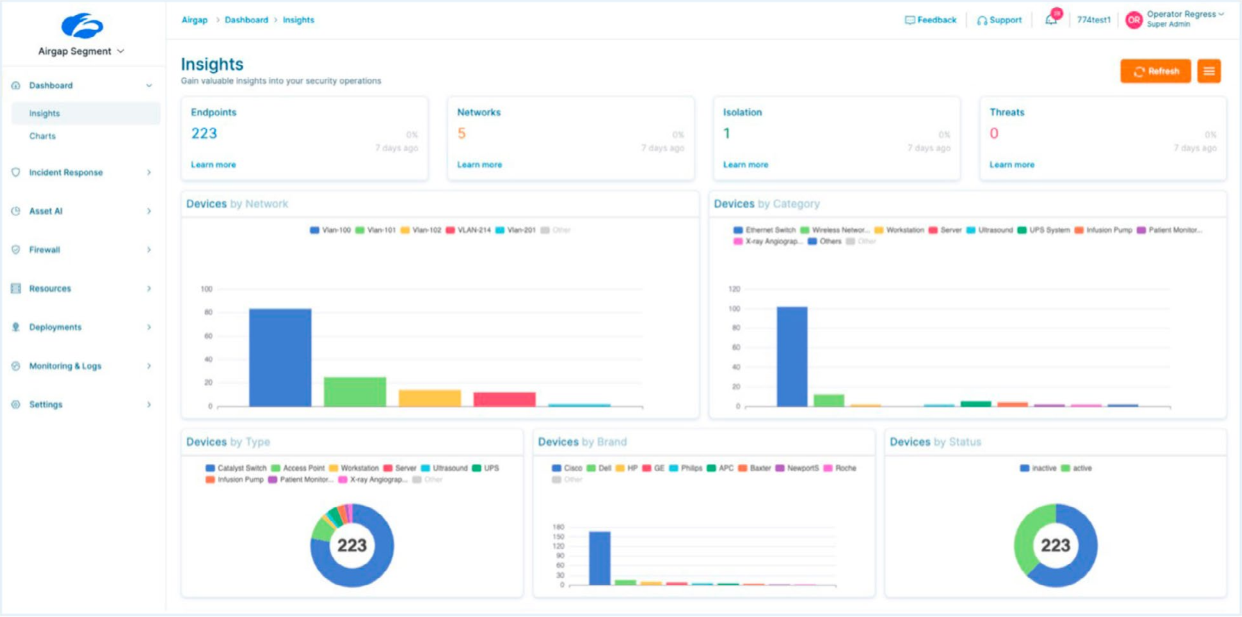
How ransomware attacks spread

The EPA, CISA, and the FBI strongly recommend system operators work toward the executive order from the Office of the President to use zero trust as a guideline toward better cybersecurity. The highlighted items are key areas in these recommendations where Zscaler can immediately help with our Zero Trust Device Segmentation solution:

- Reduce exposure to public-facing internet
- Reduce exposure to vulnerabilities
- Network segmentation
- Log collection
- Prohibit connection of unauthorized users
- No exploitable services on the internet
- Limit OT/IoT connections to the internet
- Detecting relevant threats
- Conduct an inventory of OT/IT assets

A More Secure Architecture for Device Segmentation

Segmentation has long been a staple in networking, with tools like access control lists (ACLs) and firewalls managing north-south (client-to-server) traffic. However, OT segmentation shifts the focus to the more vulnerable east-west traffic, which flows laterally between devices and workloads. On shared VLANs, due to legacy switching architecture, devices can see and communicate with all others, creating a rich environment for malware to spread. Unfortunately, agent-based solutions pioneered for cloud workloads cannot segment the legacy and headless machines so common in OT, and traditional ACL-based approaches remain overly complicated.



Zero Trust Device Segmentation dashboard

Zscaler has introduced Zero Trust Networking as a simpler, safer, and more cost-effective way for users, devices and workloads to communicate. Device segmentation is central to this approach as foundation step in establishing granular visibility and control for the modern network.

Zscaler removes intra-VLAN segmentation friction with an agentless solution that stops all lateral threats by isolating every IP endpoint, including legacy and headless systems, into a "network segment of one." This removes the need for complex ACLs, and requires no changes to existing infrastructure, while providing the most granular and effective segmentation available.

Use Cases

Some of the most common use cases for agentless device segmentation include:

LAN Interior Segmentation

Extend zero trust to the LAN by enforcing segmentation on east-west traffic. This shrinks your internal attack surface and eliminates the threat of lateral movement in critical OT/IoT networks, with no need for NAC or firewall-based segmentation.

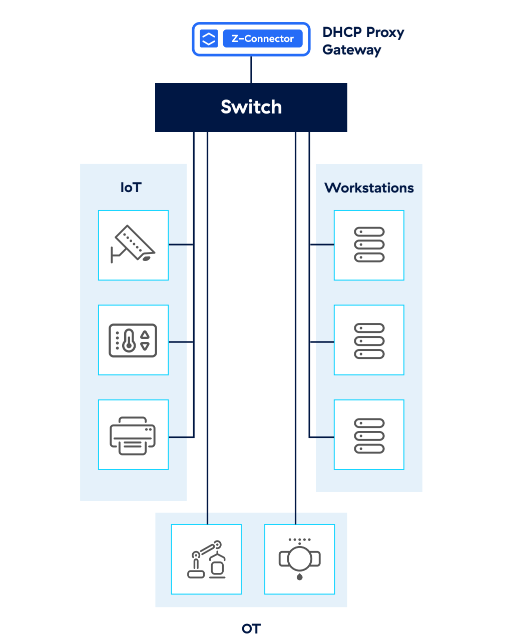
To enforce zero trust segmentation on your network, simply:

- Automatically provision every device into a segment of one (/32)
- Auto-group devices, users, and apps by analyzing their traffic patterns, preventing rogue devices from using MAC spoofing to get onto the network
- Dynamically enforce policies for east-west traffic based on the identity and context of users and devices.

IT/OT Segmentation

Zscaler Zero Trust Device Segmentation technology acts as a ransomware kill switch, disabling non-essential device communication to halt lateral threat movement without interrupting business operations. This solution neutralizes advanced threats such as ransomware on IoT devices, OT systems, and agent-incapable devices.

- Autonomously group and enforce policy for known MAC addresses on any device (e.g., RDP access to cameras denied except for admins)
- Automatically isolate unknown MAC addresses to limit blast radius in case of a compromised device
- Integrate with asset management systems for secure access control policies



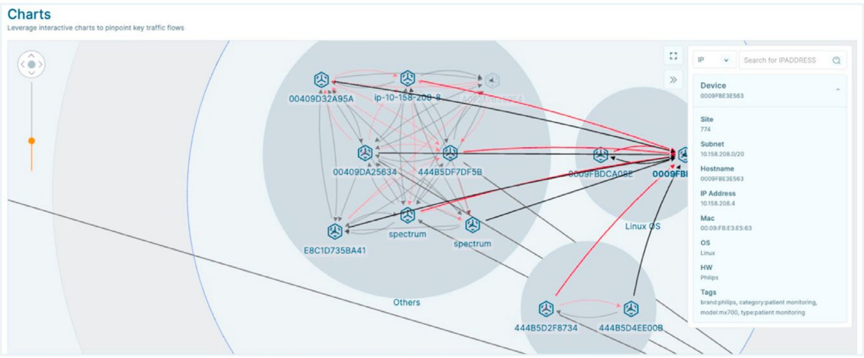
Automated IoT/OT Segmentation Segment of 'one' for every device

Automatic Device Discovery and Classification

Because a significant portion of OT/IoT traffic stays within the local network, it is important to have continuous visibility into east-west traffic. With automatic device discovery and classification, network administrators can better manage performance, uptime, and security for IoT/OT systems without complex inventory management.

For network and device visibility:

- Discover, classify, and inventory OT/IoT devices without the need for endpoint agents
- Get a baseline of traffic patterns and device behaviors to determine authorized and unauthorized access
- Gain accurate network insights for performance management and threat mapping



Device
0009FBE3E563

Site
774

Subnet
10.158.208.0/20

Hostname
0009FBE3E563

IP Address
10.158.208.4

Mac
00:09:FB:E3:E5:63

OS
Linux

HW
Philips

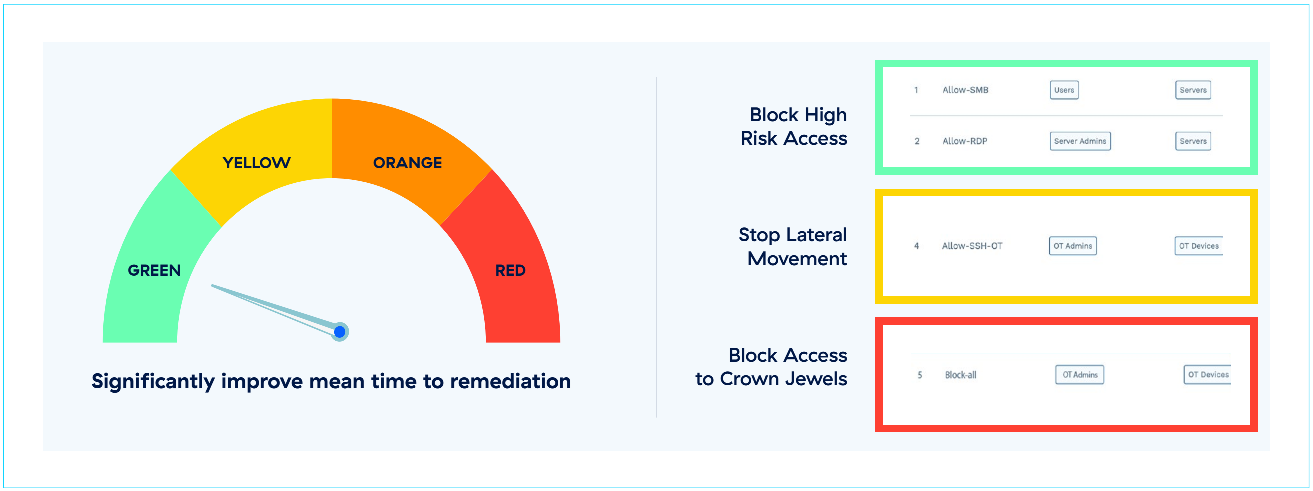
Tags
brand:philips, category:patient monitoring, model:mx700, type:patient monitoring

Device Discovery dashboard

Automated Incident Response

Introducing the Zscaler Ransomware Kill Switch, one-click attack surface reduction fully integrated into our Zero Trust Device Segmentation solution. Lock down known vulnerable protocols and ports, and even instantly disable access to critical networks like entire hospital or factory floors. All with preset severity levels to minimize business downtime.

The Ransomware Kill Switch acts as multi-layer policy enforcement point, allowing for tiered levels of incident response to an active compromise, and augmentation of existing security tool investment. Each level of the Ransomware Kill Switch has functionality akin to “virtual fuses” or Defcon levels, with predefined escalation paths to block all unnecessary network communications to or from any endpoint, denying lateral propagation, and dramatically reducing attack surface.



Block High Risk Access	1	Allow-SMB	Users	Servers
	2	Allow-RDP	Server Admins	Servers
Stop Lateral Movement	4	Allow-SSH-OT	OT Admins	OT Devices
Block Access to Crown Jewels	5	Block-all	OT Admins	OT Devices

This solution instantly disables nonessential device communication to halt lateral threat movement without interrupting business operations. This solution neutralizes advanced threats such as ransomware on IoT devices, OT systems, and agent-incapable devices.

Zscaler offers complete control of the Ransomware Kill Switch via APIs. Using these programmable interfaces, IT organizations can enable existing security orchestration tools such as security information and event management (SIEM), security orchestration and response (SOAR), or EDR/XDR solutions to automate incident response and immediately quarantine compromised endpoints and contain the blast radius of infection.

This provides organizations investment protection for their existing network and security infrastructure while immediately improving enterprise security posture.

Benefits

Granular containment to limit lateral spread

Pre-planned, automated incident response in the chaos of a breach

Hard containment at key boundary layers, such as between corporate IT and core networks

Graceful shutdown of suspect ports and protocols to maximize business uptime

Eliminate lateral threat movement across the LAN

Shrink the attack surface by isolating every into its own “network of one”, eliminating attack surface and threat propagation risk. Even compromised devices can no longer infect devices belonging to their neighbors.

Reduce operational complexity and cost associated with legacy segmentation tools

Segment every IP endpoint without the complexity of aging, IP-centric networking technologies like NAC and east-west firewalls, or complex constructs like ACLs and manual VLAN segmentation.

Gain enhanced visibility into east-west traffic

Gain full lateral visibility with automatic device discovery and classification, network admins can better manage performance, uptime and security for any device, even those that can’t accept agents.

Deploy without network disruption

Agentless technology that deploys quickly without disrupting the customers current way of doing business and does not require changing of network architecture or re-IP addressing the devices.

Faster compliance

Federal cyber standards across industries now call out segmentation as a cornerstone of zero trust. The Zscaler agentless approach deploys quickly and instantly improves compliance posture.

Features

Airgap Isolation

- Agentless device Isolation
- Airgap Plus (micro-subnets)
- One-click device quarantine
- Airgap Isolation violation detection
- MAC address-based filtering

Zero Trust Segmentation

- Network-based segmentation

Device-based segmentation

- Autonomous grouping and policy
- IntraVLAN and InterVLAN policy control
- Dynamic tag-based policy
- Device- and user identity-based policy
- Time-based policy
- Hierarchal policy framework

Asset Discovery and Profiling

- Endpoint and network discovery
- Device fingerprinting
- Profile-based device categorization
- ICS/Medical protocol decoding

High Availability

- Two-node cluster with VRRP
- VRRP with session sync
- Config and state sync
- Link aggregation
- Interface liveliness monitoring
- Hitless software upgrades
- In-service hardware replacement

Routing and Network Services

- Dynamic routing—BGP, OSPF
- DHCP Server, Relay/Proxy
- VLAN trunking
- Network Address Translation
- Policy-based Routing
- Equal Cost Multi Path (ECMP)

Incident Response

- Ransomware killswitch

Visibility and Logging

- Traffic map with policy correlation
- Integrated elastic data lake
- Session-init logs for all intra and inter segment communications
- Log exporting to SIEM/Log collector

Flexible Deployment Models

- Zero-touch Airgap Gateway provisioning
- Site templates and profiles
- Standalone, high-availability cluster or multi-cluster deployment
- Physical or virtual machine-based Airgap Gateways

Monitoring and Troubleshooting

- Remote debug console
- Local CLI on Airgap Gateways
- SNMP support

Centralized cloud-based Management

- Single sign-on (SSO) and MFA
- Audit trails for login events, and configuration changes
- Role-based access control
- Multitenant cloud delivered platform
- API-based access

3-Party Integrations

- Microsoft Active Directory
- SIEM Integration
- EDR Vendors—Crowdstrike, SentinelOne
- Asset management—Armis, ServiceNOW, Ordr
- SSE—Zscaler ZIA

Zscaler Gateway Appliance Sizing

Hardware specifications for physical gateway deployments

	S	M	L
Availability	Now	Now	New
Hardware Model	ZT800	ZTS4000	ZTS8000
CPU	8C Atom	8C Xeon	16C Xeon
Memory	16GB	32GB	64GB
Storage	256GB	256GB	960GB
Ports	6x 1GbE 2x 1GbE (SFP)	4x 1GbE 2x 10 GbE	4x 1GbE 6x 10 GbE
Form Factor	Destop	1U	1U
Other Features		RPS	RPS
Throughput (64KB HTTP)	6 Gbps	20 Gbps	40 Gbps
Sessions	500K	1M	2M
# Endpoints	750	2,000	4,000

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.