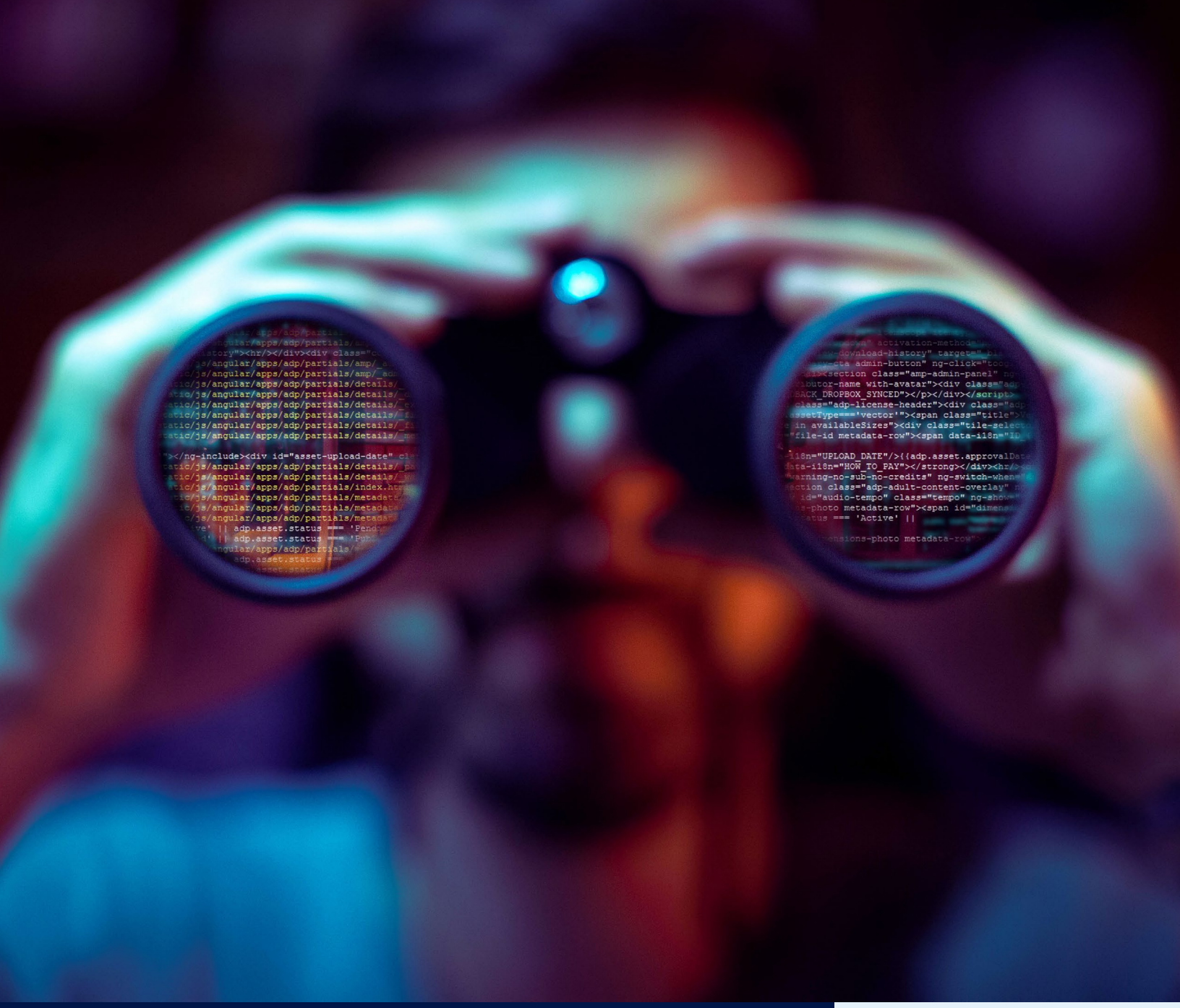


Zscaler Ransomware Kill Switch

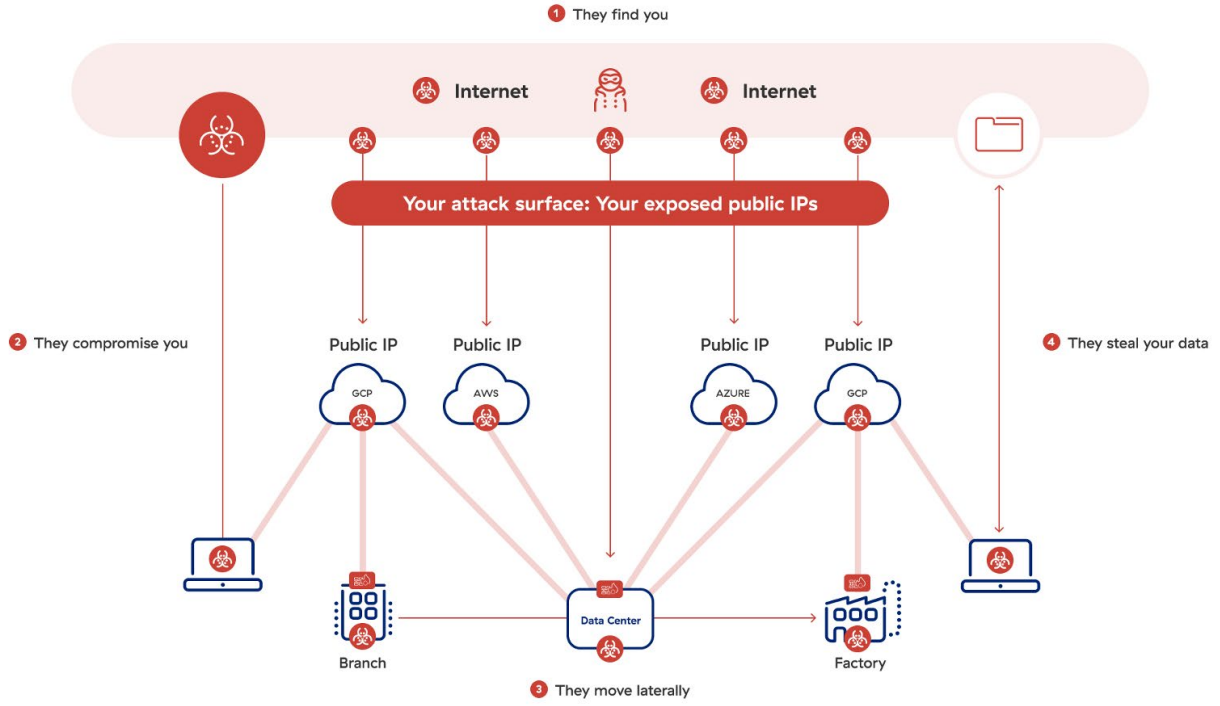
Automated Incident Response for OT/IoT Networks

Solution Brief

The Issue at Hand

Real-world critical infrastructure networks, filled with unprotected identities and vulnerable endpoints, remain a primary cyberattack target. The real threat isn't just initial breaches but attackers' lateral movement across networks, embedding ransomware and prepping malicious payloads. 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 targeted OT-connected organizations.

Unfortunately, breaches and ransomware can happen even in the most defended networks. Phishing attacks, stolen credentials, and bad actors can bypass perimeters. Many enterprises default to shutting down the entire compromised VLAN during an attack, disrupting essential traffic and halting operations. Random alerts aren't helping; in the chaos of incomplete information during an attack, how do you respond?



How Ransomware attacks happens

What Can You Do?

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. In concert with zero trust segmentation of the OT/IoT environment, the following are recommended areas of focus for network and security leaders:

Granular containment to limit lateral spread

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

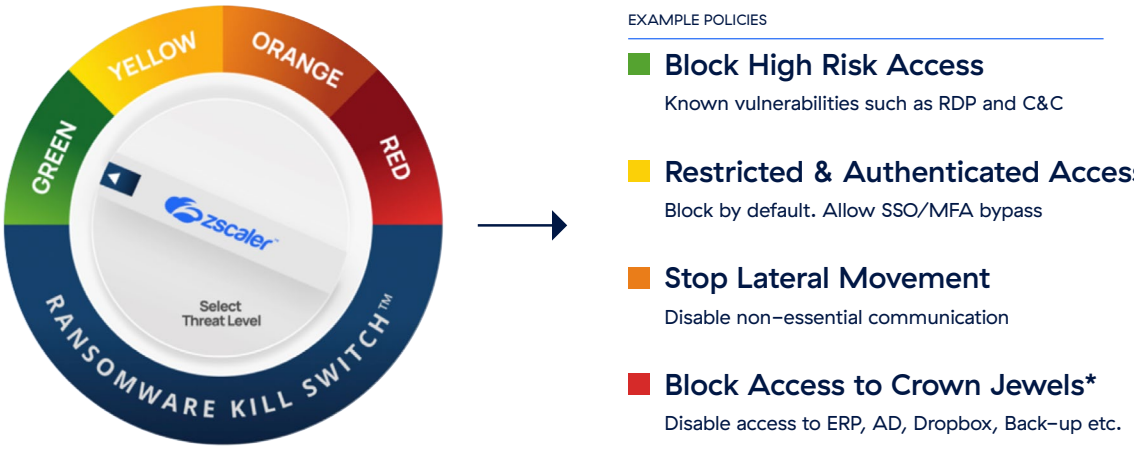
Hard containment at key boundary layers, such as between corporate IT and core networks

Graceful shutdown of suspect ports and protocols to maximize business uptime

How Can You Do It?

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 pre-set 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 RKS 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.



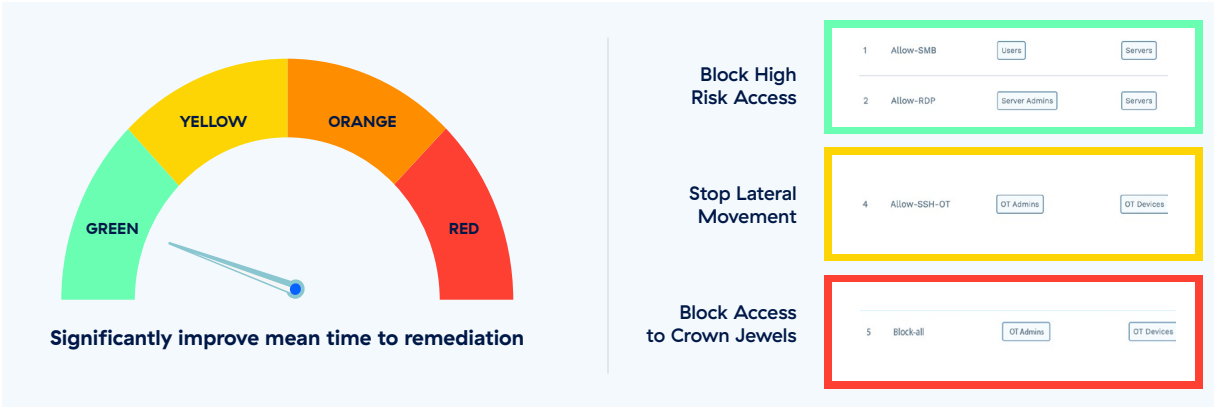
Zscaler Ransomware Kill Switch

Use Cases

Some of the most common use cases for the Ransomware Kill Switch include:

Automated Incident Response

Zscaler Ransomware Kill Switch provides user-selectable attack surface reduction. Just pick a pre-set severity level to progressively lock down known vulnerable protocols and ports, and even instantly disable access to entire networks like manufacturing lines and hospital floors. No guesswork in the chaos of a breach—just turn the dial to match the threat while maintaining business uptime.



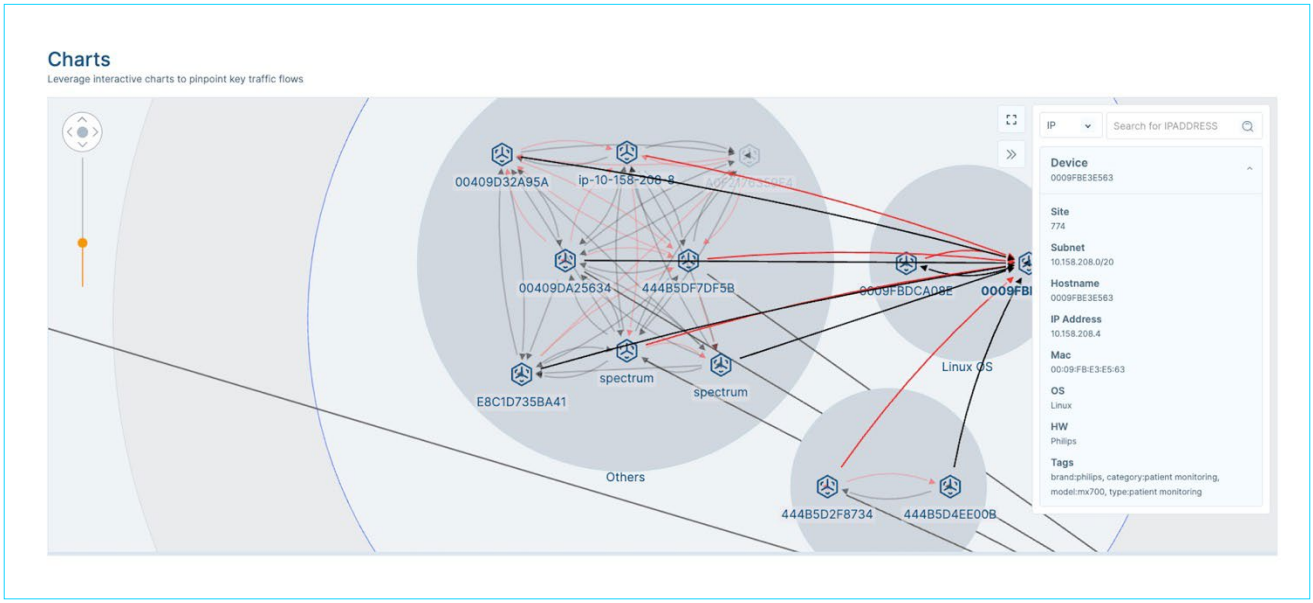
This solution instantly disables nonessential device communication to halt lateral threat movement without interrupting business operations. This solution neutralizes advanced threats such as ransomware on IoT devices, OT systems, and agent-incapable devices.

Enhanced Visibility and Control

Challenges:

- **Visibility:** Network device inventory is in constant flux. Organizations cannot secure communications between devices if all the devices are not identified and are constantly changing.
- **Control:** Given this complicated and ever-changing environment, controlling which devices can and should communicate makes enforcing even basic security practices a monumental task.

You can't protect what you can't see. Most IT organizations can't visualize lateral traffic since it is not feasible to capture E/W traffic from all access switches. The Zscaler solution provides complete visibility into all transactions in and out of every protected endpoint, allowing for real-time business/ security policy creation and enforcement.



Critical Infrastructure Protection

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.

In the chaos of a breach, you can now instantly lock down vulnerable protocols and ports with pre-set severity levels to maintain business uptime.

Zscaler Zero Trust Device Segmentation Dashboard

Speak with a technical expert

Want to learn more about how Zscaler can help protect your critical infrastructure organization? Schedule a time to speak with one of our technical experts.

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 SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com