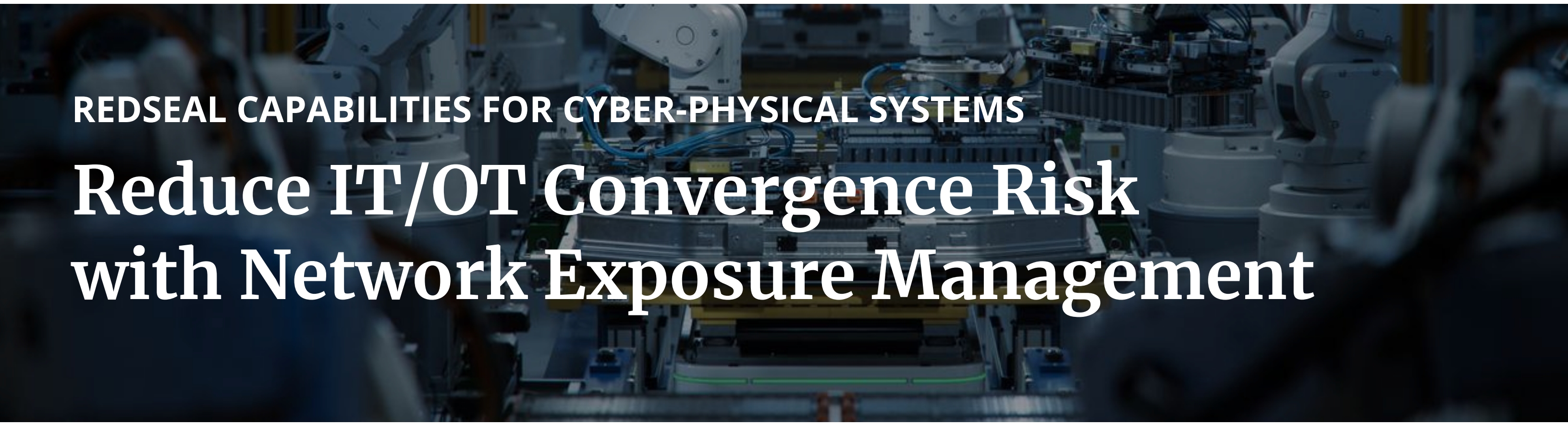


REDSEAL CAPABILITIES FOR CYBER-PHYSICAL SYSTEMS

Reduce IT/OT Convergence Risk with Network Exposure Management

Cyberattacks on cyber-physical systems (CPS), including operational technology (OT) and the Internet of Things (IoT), are on the rise. These systems connect digital technology with physical processes and critical infrastructure that humans rely on for their livelihood, health, and safety. Due to their strategic value and potential for widespread impact, they are prime targets for threat actors aiming to demand ransom, steal data, and disrupt operations.

IT/OT convergence adds to security challenges

Protecting cyber-physical systems is increasingly difficult as organizations demand greater IT/OT convergence to unlock digital transformation and operational efficiencies. IT security teams are now being asked to manage exposures of all types, enterprise-wide. In protecting CPS, they face some familiar and not-so-familiar challenges:

- **Legacy systems lacking security:** Many CPS components, especially in industries like manufacturing, utilities, and healthcare, have been in place for decades. Most of these legacy assets are unmanaged and cannot support modern cybersecurity controls.
- **Expanding attack surface with new threats:** The dual nature of converged IT/OT environments creates a broader and more complex attack surface that includes hardware, software, and on-premises and cloud infrastructure, all from different vendors. The increased use of unsecured IoT devices and remote OT access adds to the complexity.
- **Growing regulations:** Compliance requirements continue to increase, such as those related to the EU's NIS2 Directive and Cyber Resilience Act and the updated NIST Cybersecurity Framework in the US.
- **Complex decision-making:** Human error is especially problematic when organizations prioritize continuity over security. Patching vulnerabilities, while often low-impact in IT, is nearly impossible in CPS without disrupting critical operations. Creative mitigation strategies, rather than straightforward remediation, are often required.

Now more than ever, industrial organizations must be holistic, proactive, and continuous about closing defensive gaps and protecting critical infrastructure against threats.

Reduce risk with the RedSeal platform

RedSeal's network exposure management platform plays an invaluable role in securing converged IT/CPS environments. It uniquely offers four foundational capabilities for powering an enterprise-wide, proactive cybersecurity program from a single platform:

- **Network visualization,** for building an accurate model (digital twin) of the entire attack surface and discovering all connected resources across public cloud, private cloud, and on-premises environments
- **Attack path analysis,** for uncovering all vulnerabilities and other exposures from direct, indirect, external, and internal sources, including segmentation violations
- **Exposure assessment and prioritization,** for focusing teams on addressing high-impact/high-risk exploitable exposures first
- **Validation and compliance checks,** for managing adherence to regulations, best practices, and policies, and pushing detailed telemetry data to mobilize teams

With RedSeal, organizations can finally get off the reactive treadmill of security firefighting. Exposures are discovered and assessed—constantly and without human effort—so teams can focus on preemptively closing the critical security gaps that allow attackers a toehold from which to leapfrog deeper into the network.

RedSeal gives security teams the evidence they need for frictionless resolution. This includes hop-by-hop proof that the identified exposure really exists, what downstream consequences occur if it's not addressed, and the exact control creating the unwanted exposure. The result is more efficient collaboration, decision-making, and risk reduction.

RedSeal benefits at-a-glance

Get a complete and shared understanding of your entire hybrid IT/OT environment, including all assets, connectivity, and potential exposures.

Proactively and efficiently close defensive gaps and harden your network against threats with actionable exposure intelligence.

Measurably reduce risk and build resilience as you accelerate IT/OT convergence while meeting new compliance mandates.

Key capabilities for CPS protection

Maintain a complete asset inventory

RedSeal automatically discovers all resources in integrated IT/CPS environments. It collects and stores detailed technical information about each asset, along with its business value and additional context—the "tribal knowledge" of associations with locations, organizations, and business systems. This allows technical queries using business language. RedSeal serves not only as a reference inventory for the state of the as-built network, but also as a common reference point of operational metadata about the network.

Model the entire hybrid IT/CPS network

RedSeal analyzes the configuration of every asset to deliver a detailed model of the entire, interconnected environment—a network digital twin. This shows connectivity among physical and virtual elements, managed and unmanaged assets, as well as internet-facing systems. The map is customizable to reflect topology groups, subnets, segmentation, physical locations, and more. With RedSeal, organizations understand how different components, devices, and systems are connected, ensuring that no part of the network is overlooked.

Discover all possible attack paths

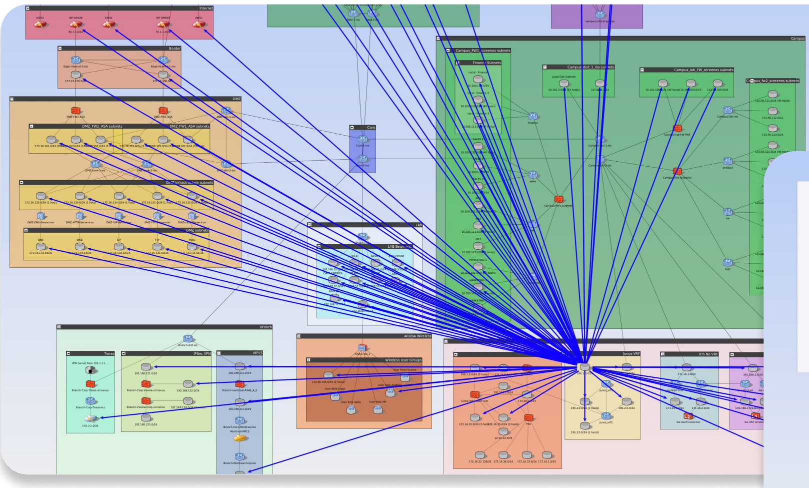
RedSeal explores every aspect of the network and network security controls to discover all access and traffic paths. It can simulate potential attacks, showing how a threat actor might move laterally from an entry point (like an IoT device) to more critical OT systems. This analysis includes hop-by-hop mapping from sources to destinations as well as the blast radius from any asset. It doesn't just look at a sample of the network and make assumptions. RedSeal evaluates every possible way in, out, and through the entire network—effectively, passive red teaming, but without the breach.

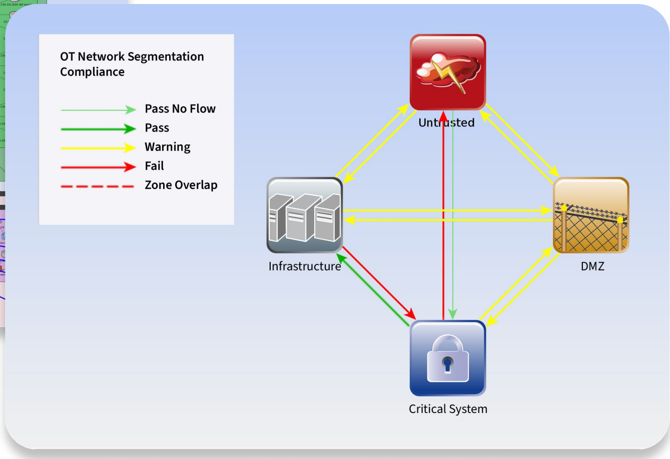
Uncover every exposure

RedSeal works with vulnerability scanners and other tools to continually assess the network for exposures, including vulnerabilities, misconfigurations, and other security gaps that could be exploited by attackers. To ensure full scan coverage, RedSeal consolidates vulnerability data from multiple scanners and vendors. It reports any assets and subnets that scanners miss, pinpoints any devices and rules preventing scanner access, and visualizes all reachable assets for optimal scanner placement.

Validate macro- and micro-segmentation

RedSeal provides insights into how the network is segmented and discovers any weaknesses or misconfigurations that could allow unauthorized access across segments. It can validate pre-defined segmentation policy sets required by laws, industry standards, and best practices, such as PCI DSS, HIPAA, and Cisco SAFE. It also validates custom segmentation against internal policies such as IT/IoT/OT and IPv4/IPv6. With automated re-validation of security segmentation requirements, RedSeal provides oversight over both intentional and unintentional segmentation compliance.





Reduce risk by uncovering unintended connections that lead to critical systems.

Quantify and prioritize every risk

RedSeal assigns a calculated risk score to every vulnerability and exposure, helping security teams prioritize efforts based on the impact to the organization. The score considers business, technical, internal, and external factors to focus security resources on the most critical systems and risks—a must when resources are limited.

Monitor and simplify compliance

RedSeal automates the process of checking the network against best practices, industry standards, and regulatory mandates (e.g., NERC CIP for energy or NIST for various sectors). It identifies non-compliant configurations, alerts stakeholders, and pinpoints the controls that need to change to meet requirements. RedSeal also generates pre-defined and custom reports on all aspects of cybersecurity and compliance to assist with internal and external audits.

Accelerate incident response

When a security incident occurs, RedSeal provides detailed network topology information to help security teams quickly assess the impact, understand how the incident spread, and identify the systems at risk. In CPS environments where downtime or physical consequences can be severe, this rapid insight and level of detail are critical for effective incident response.

Streamline change management

RedSeal allows organizations to model and simulate different network configurations, security policies, and potential threats. This proactive approach helps CPS operators understand the security impact of changes before they are implemented, ensuring that they don’t inadvertently introduce new vulnerabilities, exposures, and risk.

RedSeal works with your existing infrastructure

RedSeal leverages your existing networking and security investments—in on-premises and private/public cloud environments, and across IT, OT, and IoT. The RedSeal platform integrates with **125+** third-party products, including those from:

- Cisco
- Claroty
- Fortinet
- Hirschmann
- Microsoft
- Palo Alto Networks
- Siemens RUGGEDCOM
- Tenable

View the complete list of technology integrations on redseal.net.

Unify IT and CPS security with confidence

IT and CPS have different security requirements and protocols. RedSeal is designed to bridge this gap for security teams, providing insights into both the IT and OT sides of the network. This is particularly important because traditional IT security tools may not fully cover OT systems, leaving them vulnerable. RedSeal ensures that both IT and OT are visible and secured within a unified framework.

Contact RedSeal to learn more or request a demo today.

RedSeal, a leader in network exposure management, offers proactive insights to close security gaps in hybrid environments. It creates a network digital twin for comprehensive visibility and protection. Trusted by Fortune 1000 companies and U.S. military branches, RedSeal enhances operational efficiency, boosts productivity, and reduces business risk.
www.redseal.net | info@redseal.net | +1 408-641-2200 | 888-845-8169