REDSEAL

# Fortifying Your Network Security within the Zero Trust Framework

## The zero trust imperative

As cyber threats grow more sophisticated, organizations increasingly recognize the need for a zero trust framework to secure their networks. Unlike traditional perimeter-based security, zero trust assumes no entity inside or outside the network is trusted by default—everything and everyone must be continuously verified before access is granted. In this environment, visibility, context, and a deep understanding of your network are crucial. RedSeal's network exposure management platform and sophisticated modeling and risk scoring capabilities provide the critical insight needed to accelerate your zero trust journey.

## How RedSeal supports the journey

Zero trust frameworks continue to provide vital guidance and emphasize the need for comprehensive visibility and control—organizations must continuously monitor and understand all devices, applications, and services operating both on-premises and across cloud environments.

This inventory is crucial for enforcing the continuous validation of access to sensitive IT assets. RedSeal's network exposure management platform with dynamic network modeling provides the visibility and insight necessary to support this critical zero trust approach.

### Implementing a zero trust framework

- ✓ Inventory creation
- ✓ Inventory mapping
- ✓ Identity and information
- ✓ Consideration of how and where
- ✓ Standardized terminology
- ✓ Segmentation policies
- ✓ Identify what damage might occur

| | Zero trust requirement | RedSeal's crucial role |
|---|---|---|
| **Granular network visualization** | The foundation of zero trust Access is knowing your network—its assets, connections, and potential vulnerabilities. With a clear visual of the network's topology, organizations can understand their current landscape, plan for segmented architectures, and monitor network changes that may impact security. | RedSeal delivers a detailed and accurate representation of complex hybrid networks. It provides a comprehensive model of the entire network topology, allowing organizations to see all network devices, host connections, and potential access paths. |
| **Contextualizing vulnerabilities** | In a zero trust environment, it's essential to prioritize vulnerabilities that pose the greatest threat based on their context within the network. Understanding the context of network access helps teams identify the potential impact and exploitability of each vulnerability. | With RedSeal's insights, organizations effectively prioritize remediation efforts, focusing on vulnerabilities that can be potentially exploited due to current network configurations. |
| **Attack path analysis** | A crucial aspect of zero trust is ensuring that only authorized entities can access specific network resources. By comprehending potential access paths and how how data flows through networks, organizations can validate that their access controls and segmentation policies comply with regulations and best practices. | RedSeal identifies how adversaries can access the network but also uniquely shows lateral movement and risks within the network. A comprehensive device inventory is crucial because zero trust allows only certain authorized individuals to perform specific actions on certain devices. RedSeal gathers data on the configuration state of all network and cloud-based assets, presenting a complete picture to security teams and detecting misconfigurations that could pose risks. |
| **Policy compliance and continuous monitoring** | Constantly evolving networks can lead to configurations that deviate from the intended security policies, potentially undermining zero trust access principles. With continuous monitoring, organizations can maintain consistent policy enforcement and quickly rectify any deviations. | Through continuous monitoring, RedSeal ensures that network device configurations align with an organization's security policies, alerting administrators to any deviations. Further, RedSeal integrates with a variety of governance and orchestration tools, enhancing their insights with its detailed network models. |

## Additional considerations for zero trust adherence

Industry experts advocate for not only recognizing the network as a foundational component of zero trust, but also actively engaging in strategies like data flow mapping, macro- and micro-segmentation, as well as leveraging software-defined networking (SDN) for enhanced security measures. This balanced focus ensures a comprehensive and resilient zero trust model, and RedSeal can address those network-related challenges effectively.

**Data Flow Mapping:**

RedSeal's capabilities in mapping the network and understanding how data moves across it align with the document's emphasis on understanding data flow to identify and secure unprotected data flows. RedSeal enables organizations to visualize their network paths and flows, which is foundational for recommended effective segmentation and isolation strategies.

**Macro segmentation:**

RedSeal's Zones and Policies feature uniquely supports the concept of macro-segmentation, which the segmentation of the network into different security zones to control access and movement between them. By defining and enforcing network policies, RedSeal prevents unauthorized access between different parts of the network, such as between departments or between the IT environment and operational technology systems.

**Microsegmentation:**

Further reducing the attack surface within network segments, RedSeal's detailed network models and policy management assist in the detailed enforcement of policies that control access to resources within these segments. RedSeal's analytical capabilities identify where micro-segmentation is most effectively applied to manage the policies that enforce this segmentation.

**Software-Defined Networking (SDN):**

RedSeal's network modeling and risk assessment capabilities are complementary to SDN's dynamic and adaptable network management. RedSeal enhances SDN implementations by providing a detailed understanding of the network structure and potential vulnerabilities, thereby aiding in the creation of more effective SDN policies.

For more than 20 years, RedSeal has partnered with federal agencies and F500 companies to strengthen their cybersecurity posture.

Contact RedSeal today to discuss how we can support your zero trust journey.