Zero Trust: Defense Beyond Identity

REDSEAL

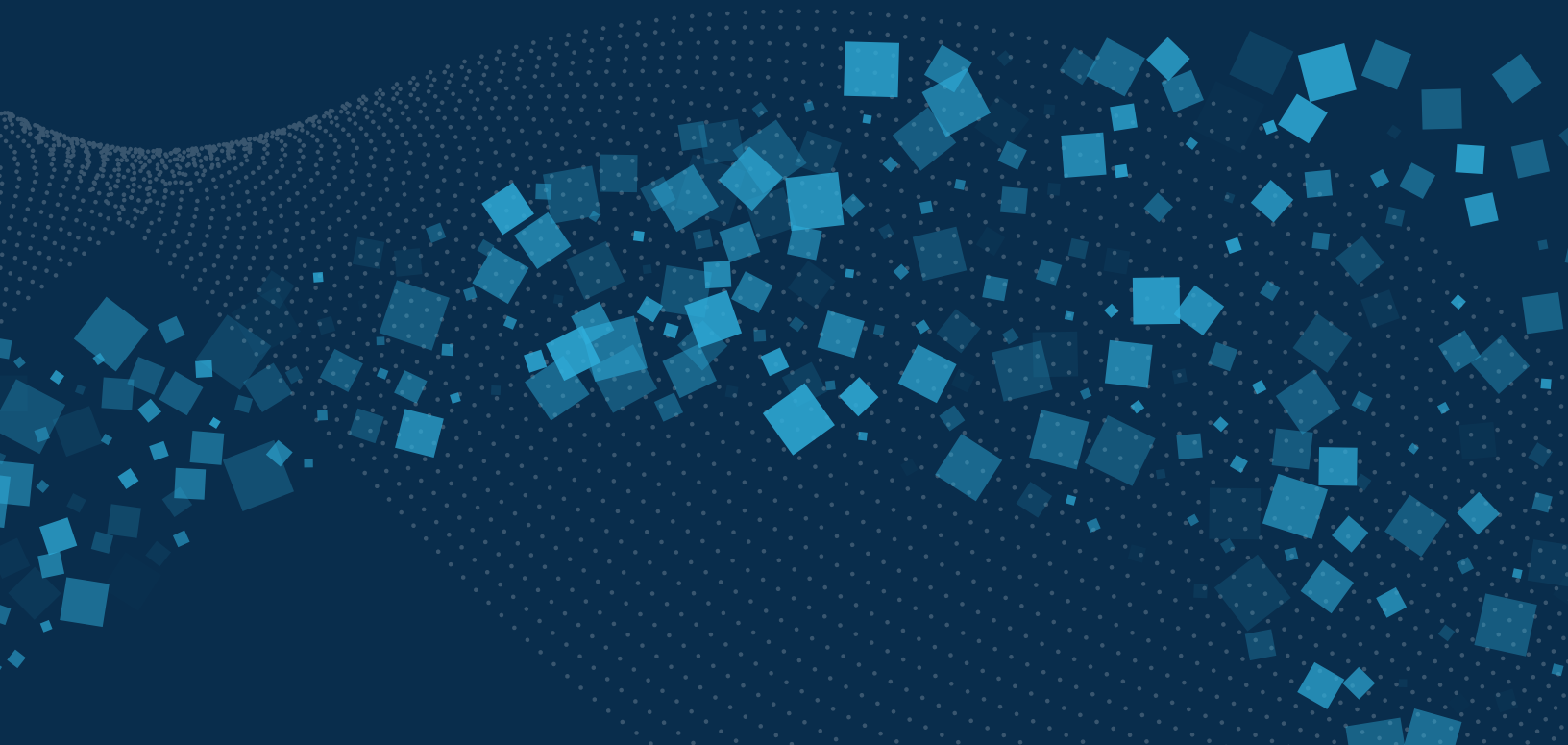
96%

of security decision-makers now say that zero trust frameworks are critical for organizational success

Zero trust adoption is on the rise. According to a recent survey from Microsoft, 96 percent of security decision-makers now say that zero trust frameworks are critical for organizational success, and 76 percent are in the process of implementation.

Often, zero trust activities start with identity: If companies ensure users are who they say they are, it's possible to reduce total risk significantly. As noted by the Federal News Network, however, "*achieving a secure zero trust environment is not complete with one item or action.*" Instead, it requires a shift in how organizations monitor and manage data security at scale.

In other words, effective defense in zero trust goes beyond identity to encompass network operations as a whole. It's essential to understand the basics of zero trust, consider the role of a comprehensive approach, and know some of the main components required to improve overall defense.



What is Zero Trust?

In many ways, zero trust is a call back to the principles of physical security that denied all access unless users can prove who they say they are. Consider the classic keycard model used to grant building access — without proper identification, entry was denied to individuals even if they had seemingly legitimate reasons for requesting access.

Zero trust operates in a similar fashion. Consider its core concept: Never trust, always verify. Instead of assuming that users have good intentions or relying on security monitoring tools to catch concerning behavior and alert IT staff, zero trust frameworks require users to verify themselves before being granted access. Even after access is granted, permissions can be tailored based on users' roles to help limit risks if attackers slip through defenses.

As a result, zero trust is closely related to identity verification: If companies can reliably identify users, they can reduce total risk.

While identity is the first threshold, it's not enough in isolation — and relying on identity exclusively won't be enough to safeguard critical assets.

According to work from CISA, the DoD, and NIST, there are five pillars of effective zero trust:

- **Identity**
- **Device**
- **Network**
- **Application Workload**
- **Data**

The Fundamentals of Comprehensive Zero Trust: Identifying Your Data — and Where it's Located

So what does comprehensive zero trust look like? At a high level, it requires companies to both identify critical data sources and understand where they're located in the network. Given the cloud-based nature of many corporate networks, this is no easy task. Data may be stored across multiple on-site locations, cloud-based backups, and co-located data centers. What's more, the nature of this data is in constant flux. Emerging regulations around the collection, storage, and handling of data means that businesses can't adopt static security processes. What qualifies as sufficient security to meet due diligence requirements one day may no longer be enough as customer expectations evolve and government regulations look to limit the risk of personal or financial information being stolen or misused.

In practice, implementing comprehensive zero trust means moving beyond identity to address each pillar within the larger scope of operations.

Identity

Identity speaks to the user. Are they who they say they are, and can they prove it? Verifying identity often takes the form of solutions such as multi-factor authentication (MFA) that ask users to provide verification factors, such as something they have (like a USB token or SMS code) or something they are (such as a fingerprint scan) in addition to familiar usernames and passwords.

While identity is a critical step in the zero trust process, it's just the beginning. Simply confirming identity isn't enough to ensure security across networks.

Device

The device pillar focuses on understanding the type and number of devices used across enterprise networks and their impact on overall security. This includes a comprehensive inventory of all devices that connect to any corporate data source — such as desktops, laptops, tablets, and smartphones, both those owned by the company and those that belong to staff members. It also includes an analysis of the data types accessed by these devices. Where is it stored? How is it used? Who has permission to view or modify this data? Finally, effective device management requires real-time risk analysis to pinpoint potential problems as they occur.

Network

The zero trust network pillar looks to understand the movement of traffic across devices and data sources. Effective network security includes both macro and micro-segmentation to limit the impact of data compromise. For example, if critical functions are segmented within larger networks, administrators can provide targeted access that gives users just enough privilege to complete key tasks without accessing data they don't need.

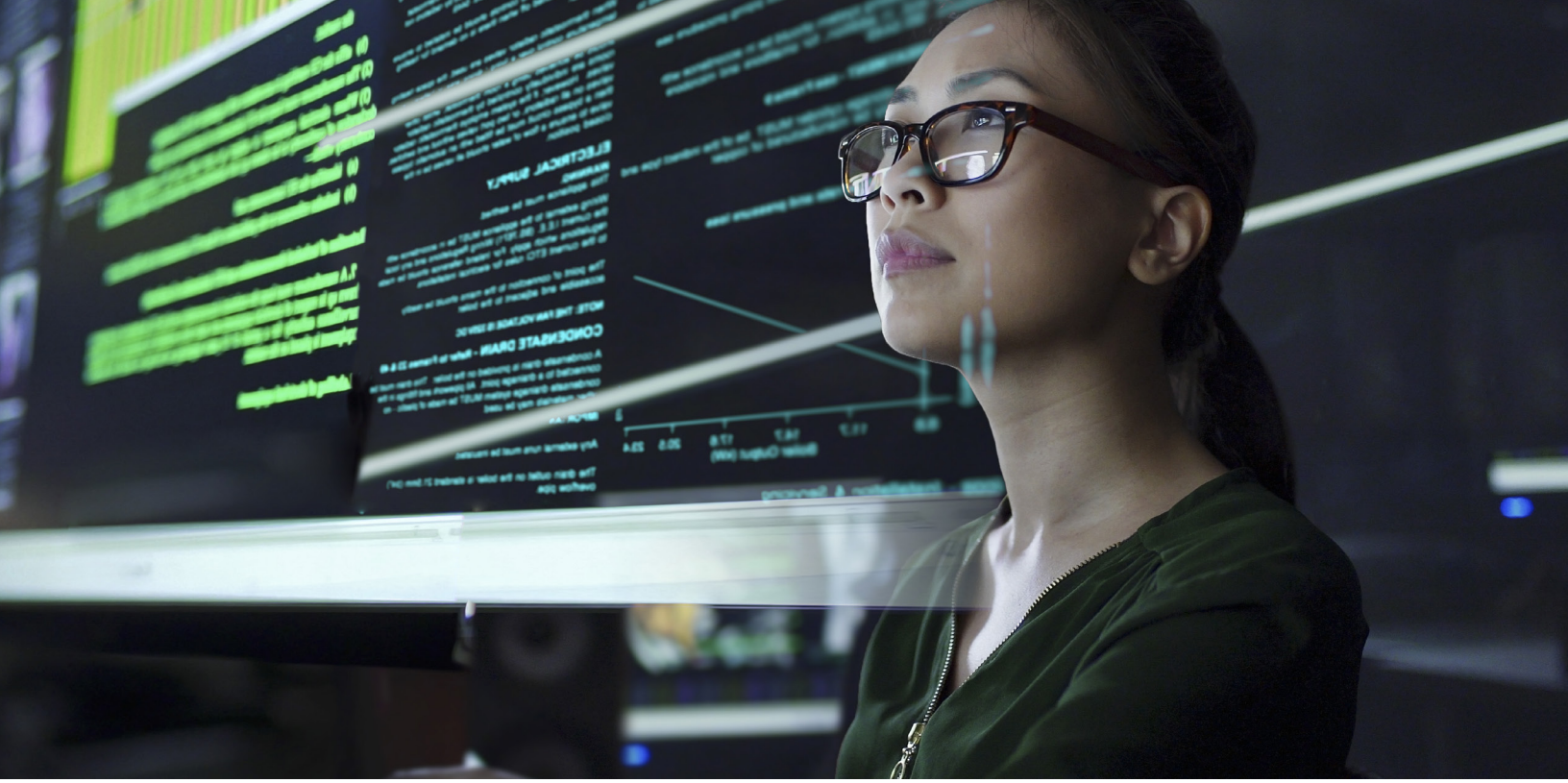
Zero trust network security also examines the movement of traffic: How much traffic is moving north/south or in and out of enterprise networks? How much is moving east/west or across the network components? Are these traffic volumes consistent, or are they experiencing significant spikes? If so, are these spikes tied to specific users or actions?

Application Workload

Application workload looks at how workloads are handled within applications themselves and how access to these applications is granted. Are companies using a local, single-sign-on (SSO) approach, opting for a more centralized methodology, or implementing solutions capable of continuously analyzing and assessing workflows across disparate network connections?

Data

Data also benefits from the implementation of zero trust controls. These include robust encryption that protects data at rest and in transit, along with dynamic controls capable of handling requests in both local and cloud environments. In addition, a complete inventory of data — including where it's stored, how it's used, and the privilege level required for access — is critical to ensure security at scale.



Understanding How it's All Connected

While creating a map of where data is located and what data requires the most protection is a great starting point for zero trust, the next step is understanding how IT environments are interconnected — and what impact this has on security.

This allows organizations to effectively implement the principle of least privilege, which states that "a subject should only be given those privileges needed for it to complete its task." In other words, users should only be given as much access as required to fulfill specific functions. What's more, privilege itself should be purpose rather than people-oriented — this means that if a user has a certain privilege to complete a task, this permission should be removed as soon as the task is complete. This principle should extend across the organization, from front-line staff to C-suite members. By enforcing least privilege wherever possible, companies can limit the risk of compromise.

To effectively implement and enforce least privilege, companies need the answers to three questions:

What connections exist?

What connections exist across your network, and how do they interact? For example, if you have a local data source connected to a public cloud for regular backups, how often is data transferred? What data is sent? How is it secured? Understanding these connections paves the way for improved protection.

Where do these connections lead?

It's also important to map out all of the pathways through your network that can access specific data. Consider a cloud instance with several geographically-disparate duplicates to help increase reliability. Each instance may have multiple paths to the same data, meaning it's worthwhile to map all routes and understand how data gets from point A to point B, or C, or D.

How are functions across these connections authorized?

Finally, companies need to know how operations across these pathways are authorized. What checks and balances are required to grant access? What does this access provide to users, and what happens if unauthorized use is detected?

Understanding what, where, and how connections work across the network puts organizations in the position to enforce least privilege by providing a complete picture of access and authorization.

Why Automation is Essential

It's one thing to prioritize the process of understanding connections across an enterprise network — it's another to complete this task both quickly and accurately. Put simply, the sheer size and scope of modern networks makes this an impossible task for IT teams, no matter how many staff they have or how experienced they may be. What's more, this data is constantly changing. New access requests are constantly being made, and new threats are always emerging, even as the landscape of data connections shifts. A new cloud service or a redesigned application could introduce a new potential point of compromise that must be addressed to ensure effective security.

As a result, businesses are best served by the adoption of advanced automation solutions that can help map network connections accurately and efficiently. Automation brings organizations several distinct advantages.

Understanding Network Interconnections

Automated mapping of network topology can provide a clear and detailed map of operational interconnections, making it possible for teams to identify potential blind spots or weak points quickly. What's more, automation makes it possible to regularly update this map, so companies don't fall behind the security curve.

Completing Device Inventories

The sheer number of personal and business devices now used to access corporate networks makes complete and accurate inventories a must. But the increasing volume of attached devices makes it impossible for staff to conduct this inventory manually. However, automation is up to the task.

Validating Network Configurations

The right network configuration can safeguard data. The wrong configuration can open a hole for attackers. Automation makes it easy to quickly test network configurations to ensure they align with best practices and limit overall access.

Enforcing Segmentation

Segmentation of functions and services reduces risk. Automation supports macro and micro-segmentation at scale and speed, in turn supporting "need-to-know" frameworks that give users exactly the right amount of access.

Identifying Application Interactions

Thanks to the growing use of open source technologies and customizable application programming interfaces (APIs), the volume of interaction between apps is steadily growing. Automation helps identify which apps can '"talk" to each other, what data is exchanged, and how this data is used.

The Importance of Integration

Visibility is the foundation of effective security. Without the ability for companies to understand what's happening, when, and why across their network, achieving zero trust becomes almost impossible.

As a result, visibility always comes first: Services and solutions that make it possible to discover what's happening across both local and cloud networks form the foundation of security operations. Without this visibility, businesses are shooting in the dark. They may be spending on security measures that may or may not provide the right protection at the right time. While tools such as next-generation firewalls (NGFWs) and runtime application self-protection (RASP) can help deflect generalized attack vectors, more specific security threats may go unnoticed.

Armed with visibility, however, businesses can pick and choose solutions that best meet their needs and reduce risk. The caveat? It's worth prioritizing integration when it comes to implementation. Consider a security tool capable of rapidly ingesting data and predicting likely threats. While this offers a significant advantage in zero trust frameworks, its efficacy drops off if it doesn't play well with tools from other vendors. For example, if solutions insist on the use of proprietary tools for data collection and analysis, they naturally limit the efficacy of security efforts by reducing the total amount of data available. This gives companies only part of the picture when it comes to protection, in turn, opening potential security gaps.

As a result, it's worth prioritizing tools and technologies that are naturally interoperable to help provide the most comprehensive network view possible.

Seeing is Securing

Zero trust defense starts with identity, but this isn't enough to safeguard networks at scale. Instead, effective security depends on sight — the ability to see and understand network connections at scale to make informed decisions about user access and stay ahead of emerging security threats.

Solutions such as RedSeal Stratus make it possible to reduce the risk of threats, vulnerabilities, and ransomware in both AWS and Azure. By visualizing your entire cloud inventory — including Kubernetes — in a single view, your teams can identify overly permissive configurations, make key changes to stay in compliance, and gain the end-to-end insight needed for a comprehensive zero trust approach. And if your network is also on-premise, RedSeal can provide solutions for that as well.

Ready? See what RedSeal can do for your zero trust security.

ABOUT REDSEAL (redseal.net)

RedSeal — a security solutions and professional services company – helps government agencies and Global 2000 companies see and secure their on-premise networks and cloud environments. RedSeal Stratus, the company's SaaS CSPM solution, gives an integrated view of cloud security posture through visualization of cloud-native and Kubernetes controls, and shows which resources are unintentionally exposed to the Internet. RedSeal's Classic product brings in all network environments – public and private clouds as well as on-premises. This award-winning security solution verifies that networks align with security best practices, validates network segmentation policies, and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk. The company is based in San Jose, California.

REDSEAL

+1 408 641 2200 | 888 845 8169 | redseal.net | info@redseal.net