Securing Modern Networks: Navigating the Complexities of Cloud and On-Premise Environments

Protecting on-premise devices and data centers has always been complicated, but expansion to the cloud, as well as the recent growth in distributed workforces and remote employees, has increased the problem's complexity significantly.

Achieving complete visibility of a network is a challenge for many organizations. According to a recent Ponemon Institute study:

- The average enterprise is now managing about 135,000 endpoint devices.
- 63 percent of companies say they lack the network visibility necessary to achieve a strong security posture.
- 48 percent of devices (64,800) are at risk because they have outdated operating systems or are not known by the organization.

While network complexity grows at breakneck pace, large enterprises will continue to seek complete visibility of what's attached to their networks, how to secure those networks properly, and how to react when their networks are infiltrated.

63%

of companies say they lack the network visibility necessary to achieve a strong security posture.

The Challenges of Complex Networks

Over the past three years, the complexity of networks has grown significantly due to the ever increasing number of access points. The average endpoint now has as many as seven agents installed for remote management, and the pandemic and rapid shift to remote work have only added to the number of endpoints that need to be managed.

In the event of an infiltration, IT leaders feel that they could only address a little over half of the attacks with their current expertise and technologies. As networks become more and more complex, the challenges of managing them also grow, whether these challenges are rooted in visualization, language barriers, or expertise.

REDSEAL

Constant Evolution

Networks are never static. New instances and resources are being added all the time. Configurations are being changed by multiple users. Devices are connecting and disconnecting. This ever-changing nature of the modern network makes it increasingly difficult to keep track of every access point, leaving them vulnerable to bad actors. It can be difficult to inventory everything on the network because things change quickly.

If you're in charge of security at a major train station, you will likely take a picture of the station to examine for any potential security threats. By the time you've identified a suspicious person, the person you're looking for is long gone and new threats could be coming up anywhere, out of your current sight. When things are in motion, the picture is constantly changing so a snapshot doesn't work. What was secure last month, last week, or even this morning may not be secure this afternoon.

It's the same with modern networks in constant motion. Conducting a static analysis can give you a sense of your security posture as it was at that one specific moment in time, but while you're resolving the problems from the moment you've analyzed, any number of things could have changed the situation entirely. Someone may have spun up an instance in the wrong location or changed a configuration, or maybe a third-party vendor was added or was given temporary access to troubleshoot an issue. There's now new vulnerabilities that didn't exist seconds before, and you may not find them before a bad actor does.

> When it comes to security, keeping track of a dynamic environment in near real time requires a dynamic approach.

Language Barriers

The language barrier between on-premise, physical devices and cloud resources present another major challenge. With traditional on-premises networking using certain systems, your team members would get training and certification to handle that system, so everybody would have a similar knowledge base and use a common technology. That doesn't work in the cloud.

In the cloud, you often deal with a whole host of cloud service providers (CSPs) doing things their own ways independent of each other. You could be dealing with Amazon Web Service (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Oracle Cloud all at once, with all their different processes and terminologies. Some things work roughly the same across providers but have different names, while others might have the same name but mean different things.

Lack of Expertise

Security and DevOps teams are being asked to be experts in multiple cloud systems. Even if they can rise above the technology barriers, not everyone has the training and background to work across multiple clouds. This is especially true for security teams.

An organization may have one DevOps team working in Azure with Azure specialists that know it inside and out, while another team may prefer to manage workloads in AWS. Security teams, on the other hand, have to understand all clouds, acting as universal security translators within organizations. For example, AWS availability zones within a region are geographically separate in different data centers, while in Azure, some regions have only a single availability zone. Meanwhile, Google has regions, but when you make a virtual network, it's not limited to just one of them; it's global.

The complexities and nuances of various clouds require deep knowledge and specialized skills, making it difficult for individuals or teams to be well-versed in all aspects. It also requires security teams strive to be the universal security translators within their organizations. Organizations need to prioritize ongoing training and development, leveraging specialized expertise where needed to ensure effective and comprehensive security across on-premise and multi-cloud environments.

Employee Turnover

While government and public agencies typically do not see significant turnover in IT and security teams, it plagues the private sector. Forty percent of senior IT and development decision-makers said they are dealing with employee turnover challenges. Even one or two team members with tribal knowledge of the infrastructure leaving can cause knowledge gaps in your security plan. It takes time to replace team members and even more time to get those new members up to speed and understanding your network and the underlying security posture.

Managing Network Growth

As networks continue to grow and evolve, organizations must take proactive steps to secure them in real time. A firewall — even one with next-generation capabilities that integrates threat detection and mitigation — cannot fully protect your network. While it is an important layer in your security plan, it is limited to only detecting threats when they occur.

To secure your eternally growing and evolving network, you need a proactive strategy, not a reactive one. That strategy needs to address your cyber security systems, modern and dynamic policies and procedures, and team training and development. You need to build a collaborative strategy to effectively protect your organization's networks.

Overcoming a Lack of Visibility

While cloud security is a shared responsibility between cloud service providers and customers, Gartner says that more than 99 percent of cloud security failures are the fault of the customer and not the CSP. While CSPs protect the cloud infrastructure, their customers must also protect their own cloud networks. This also holds true for on-premises security. One major factor in these security failures is a lack of visibility across the entire network.

Organizations need a comprehensive visualization of the entire network beyond the details provided by the CSPs, consolidated reporting from multi-cloud and on-premise resources, and an analysis of every connection and pathway between every device, all forming one holistic view.

Proactive Vulnerability Identification

Attack path analysis is crucial to provide a comprehensive overview of every potential pathway within your network, including an analysis of your configurations and security policies at each step. To be effective, it needs to monitor and analyze your network for changes.

Organizations also need to be proactive in instituting rigorous policies and procedures. For example, you can prevent developers from spinning up new instances unless they go through a specific security process. While this may slow down DevOps teams and cause friction between developer and security teams in the short term, thoughtful changes to procedures will ultimately make your network more secure.

But policies alone are not a foolproof solution. Even if your team understands the goals and strategy, they may make mistakes or struggle to keep up. If setting up cloud resources involves checking a few boxes, overlooking just one of them can expose your network.

Once your network reaches a certain size, it becomes nearly impossible to manage every aspect manually. Automation is essential to apply consistent security policies and manage everything on your network.

Bridging the Language Barrier

Securing complex networks also requires bridging the technology barrier. InfoSec and NetOps/DevOps teams are tasked with different goals and have different priorities. Developers are under intense pressure to get products to market. That means moving fast and being agile and often pushing the envelope. Meanwhile, security teams are charged with protecting everything and tend to be more conservative. This disconnect in goals and approaches often creates friction within organizations. Security teams need to produce evidence of defensive shortcomings and communicate how to fix the problem in terms developers can understand.

From a security standpoint, organizations need a powerful, automated platform to understand on-premises and cloud networks, helping everyone communicate in a common technology language to understand where, how, and why security gaps exist. Network operations, cloud operations, and development teams all need a single source to prove problems and show what needs to happen in terms they all can understand.

Securing your networks

Effectively managing network growth requires a proactive approach that goes beyond traditional reactive firewall protection. Organizations need to focus on enhancing visibility, proactively identifying exposures, and bridging the language barrier between security teams and network administrators. By implementing modern and dynamic policies, investing in team training and development, and utilizing comprehensive cyber security systems, organizations can build a collaborative and robust defense that adapts to the evolving threat landscape. Embracing this proactive strategy will enable organizations to effectively manage and secure their growing networks and protect their valuable assets in real time.

Manage Network Complexity and Stop Unintended Exposure with RedSeal

RedSeal helps you answer critical security questions, such as:

- Where are our vulnerabilities and what are the attack paths?
- If a threat actor penetrates our defenses, what resources are at risk from lateral movement?
- Do we have effective network segmentation policies and are they in the right place?

RedSeal security software and professional services help government agencies and Global 500 companies measurably reduce risk. The RedSeal platform brings all network environments, public and private clouds and on-premises, into one dynamic visualization that provides the accurate data needed to keep your organization safe.

Contact us today to learn more

ABOUT REDSEAL (redseal.net)

RedSeal helps customers discover, assess, and reduce cybersecurity risk across hybrid enterprise networks. Uniquely, the RedSeal platform brings all network environments, including public clouds (AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud), private clouds, and on-premise into one comprehensive set of visualizations which identify cybersecurity risks across the entire enterprise network. Customers can assess and remediate prioritized risks to reduce the potential attack surface, support compliance initiatives, better defend the enterprise and deliver return on investment. RedSeal's customers include 100's of Fortune 1000 companies and over 75 government agencies, including all 4 branches of the U.S. military. To learn more about RedSeal, please visit www.redseal.net.

REDSEAL

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