IDG Sponsored content

Network Security:

Multiple Challenges Underline Need for Increased Visibility and Verification

IT directors, VPs, and other executives believe they have good security practices in place but still recognize unanswered challenges and needs.

In a perfect world, CIOs, IT directors, and other IT executives could focus all of their attention on staying ahead of technology's rapid evolution while also ensuring that their organization has the optimal IT and network infrastructure to meet business and operational needs.

In the real world, however, an increasing portion of IT leaders' time is spent in fire-drill mode as they react to the rising deluge of cyberattacks. Today's digitally dependent organizations understand the damage that successful cyberbreaches can cause. Yet having a constantly distracted and reactive IT department also poses significant financial and reputational risks.

The rising sophistication and consequences of cyberattacks make clear the importance of implementing proactive security capabilities. A recent analysis by the Ponemon Institute and IBM found that the average total cost of a data breach worldwide has reached $4.24 million, up from $3.86 million a year earlier. One key driver of this escalating cost is that it took organizations, on average, more than nine months to identify and contain a breach.

To minimize the risk of breaches and rapidly identify successful intrusions and contain their damage, managers and security teams need full visibility across their entire IT and network estates. That includes having detailed information on device topology, state, and configuration. It also means getting prompt notification of any security policies that are broken — unintentionally or otherwise — by misconfigurations or by risky actions taken by employees.

FORWARD NETWORKS

To get a better sense of the state of network security, IDG surveyed 101 IT directors, VPs, and other executives as well as 98 frontline IT managers. Most expressed high levels of confidence in their organization's existing network security capabilities. However, most also expressed a desire for many additional capabilities, which suggests that some of that confidence may be misplaced.

Network Security Landscape: A Mixture of Confidence and Challenges

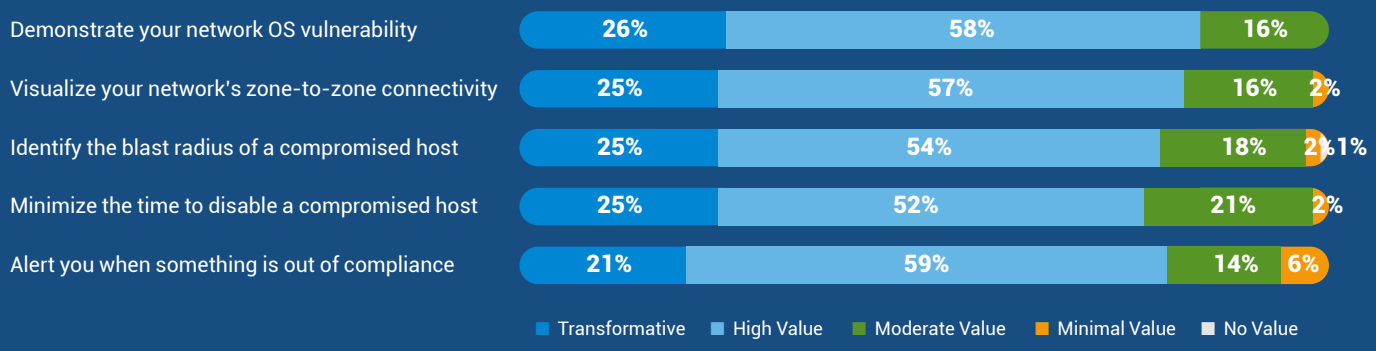
Among the "director+" executive respondents, 58% rated their overall network security as ahead of the curve compared to their competitors'. Another 37% said that it was on par with others, and — contrary to the reality of averages — just 5% said they were lagging their competitors.

Despite their high confidence levels, IT leaders identified improvements related to network security that they're seeking, such as:

- **89%** A better understanding of the blast radius of a compromised host
- **88%** Validation that their network architecture follows a zero-trust approach
- **85%** Improvement in network breach response times

There were also indications that IT directors and executives sometimes have perspectives different from those of frontline IT managers with regard to the status of their network security initiatives and capabilities. For example, whereas 59% of the directors+ cohort said their organization was building or already employing a zero-trust architecture, just 39% of IT managers said the same.

Figure 1: **IT Directors Place Value on a Single Solution That Solves Multiple Issues**



Source: IDG

Likewise, 70% of the IT directors+ strongly agreed with the statement "I am confident that I can prove/validate that my network architecture follows a zero-trust approach," compared to just 53% of the IT managers.

These disparities in perception are cause for concern. Executives who believe that their network is more secure than it is may ignore or underfund critical initiatives necessary to protect their organization's digital assets.

At a minimum, the different assessments suggest a lack of communication between IT executives and managers. There must be continual engagement and coordination with each other on network security objectives, progress, and outstanding needs.

Providing a Single Source of Truth for Network Security

It isn't only IT executives and managers who sometimes have difficulty communicating. Many of the specialized security systems and tools that organizations have deployed to monitor, assess, and counter cyberthreats don't "talk" to each other.

Software-driven security solutions have proliferated almost as rapidly as cyberthreats themselves, and attack volumes and complexities have exceeded the capabilities of humans to analyze and respond to them. Making the situation more challenging: Poorly integrated, discrete solutions can result in security silos and gaps. IT professionals need a single source of security truth and visibility to defend their end-to-end networks.

IDG survey respondents understand the value of a multifunction solution that can accurately and rapidly provide a range of security information, visibility, and functionality. As shown in Figure 1, a single solution was seen by most IT leaders as delivering high-value benefits.

Network Security Through Better Math

To handle the escalating demands and threats IT managers face in securing their organization's complex digital estate, Forward Networks has developed a mathematical process to precisely model an organization's end-to-end network. This constantly updated, always accurate digital twin shows network topology, device configurations, and behavior and presents information in easy-to-understand, vendor-agnostic visualizations.

For security operations teams, Forward Enterprise makes it easy to monitor security policy adherence through an always-current zone-to-zone connectivity matrix and to remediate network OS vulnerabilities through a Common Vulnerabilities and Exposures (CVE) matrix. They can also prove the network security posture with always-on monitoring and reduce the time to find and remediate compromised devices, using the solution's blast radius feature. Deployed on-premises or as a hosted cloud service, Forward Enterprise integrates easily with existing network management systems and tools.

Learn more about how your IT team can quickly and easily identify and address network security risks by visiting Forward Networks.