IDG Sponsored content

Siloed and Poorly Integrated Systems Continue to Undermine Network Security

Evidence of multiple challenges suggests there is misplaced confidence among frontline IT managers that their network security practices are ahead of the curve.

Constrained by tight budgets and staffing shortages, IT managers are constantly striving to do more with less. This mandate is especially pressing when it comes to identifying and countering network security threats or when assessing and mitigating the effects of cyberbreaches.

In our digitally dependent world, the successes and failures of IT managers rest heavily on their ability to protect their organization's data and systems. However, defending against cyberthreats has grown continually more challenging, and not only because the threats themselves have increased in number, diversity, and sophistication.

The digital estate that IT managers must police has also become much more complex. Today IT environments typically encompass on-premises data centers, multicloud environments, network-edge facilities, a large variety of end user devices, and a broad collection of different networks.

To manage and secure these diverse environments, organizations have deployed a growing variety of systems and tools. However, these discrete systems often create additional layers of complexity as well as information silos. For many IT managers, there is no single source of truth for network security information or any simple way to gain end-to-end visibility across their IT infrastructure and operations.

No wonder that IT managers are sometimes overwhelmed with simply managing and maintaining all the IT elements under their charge as well as protecting them against cyberattacks. IT managers need easy and immediate access to accurate information — everything from validation of zero-trust architecture deployments to the number and scope of systems compromised by any successful cyberbreach.

Interestingly, a large majority of IT managers recently surveyed by IDG said their existing network security capabilities equaled or surpassed those of their competitors. Clearly, not every organization can be "average or above" in this regard. Managers who overestimate the strength and sophistication of their security operations may unintentionally expose their organization to significant financial, legal, and reputational risk.

Network Security Landscape: A Mixture of Confidence and Challenges

To gain insights into the current state of network security, IDG surveyed 98 IT managers along with 101 IT directors, VPs, and executives at large enterprises.

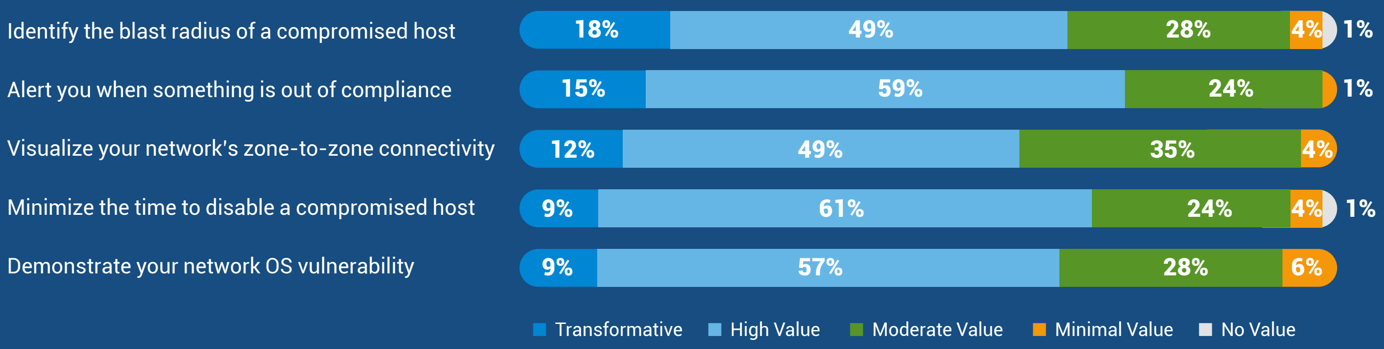
Nearly half (48%) of the IT managers surveyed said their overall network security was "ahead of the curve" compared to competitive organizations'. In one sign of a disconnect between the frontline IT managers and their bosses, the IT director+ respondents were more likely than IT managers to believe that their organization's network security was ahead of the curve.

In contrast to the directors' confidence, IT managers identified a wide range of network security challenges and pain points:

- 94% Establishing strong firewall rules
- 92% Minimizing the time required to disable a compromised host
- 83% Ability to know when something is out of compliance
- 82% Lack of a matrix to verify firewall security connectivity

FORWARD NETWORKS

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



Source: IDG

It's commonly accepted that success relies on shared vision and goals. Yet the IDG survey showed misalignment between the two respondent groups with regard to network security. For example, 39% of the frontline IT managers said their organization was building or already employing a zero-trust architecture, compared to 59% of the director+ respondents saying the same.

A 20% gap in perception is worrisome. It could be that IT managers are so consumed with reacting to cyberthreats and other pressing demands that they have little time to focus on proactive measures such as zero trust. However, this finding, along with other disparities, highlights the importance of continual engagement and coordination among all levels of IT when it comes to network security objectives, progress, and outstanding needs.

The Value of a Single Source of Truth for Network Security

Although IDG found several differences between IT managers and IT executives, the two groups mostly agreed on the challenges they face and the importance of addressing them. That agreement included the need for and benefits of a single highly integrated network operations security solution.

As IT managers know, many important security tasks are largely or partially performed manually. As shown in Figure 1, respondents said that a single solution able to automatically address five critical security functions would bring significant value.

Mathematically Verified Network Security

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.