POINT OF VIEW

Simplify Network Operations

How to Improve Operational Efficiency and Ensure Productivity

Executive Summary

As organizations continue to rapidly adopt new technologies to support digital acceleration initiatives, they create complex, vulnerable network environments that are difficult to manage, secure, and monitor. Enterprises tend to adopt point products to protect their various digital acceleration tools, or plug a certain gap in security, without consideration for interoperability. As a result, enterprises have an average of more than 76 security tools to manage.[1]

While technologies and approaches such as software-defined WAN (SD-WAN), software-defined branch (SD-Branch), zero-trust network access (ZTNA), and multi-cloud network architectures enable organizations to stay competitive, action must be taken to avoid negative consequences brought on by complexity. Network operations teams must figure out how to ensure efficient operations and employee productivity, while quickly detecting and remediating incidents.

"The cacophony of noise generated from dozens of separate systems offers the perfect cover for threat actors, enabling them to remain undetected inside networks for months (and sometimes even years)."[2]

Simplification and Integration Are Key

For successful digital acceleration, network operations teams need to ensure the quality of user experience on any application accessed from any location. If teams do not have full visibility and cannot get through the overwhelming amount of data generated by disparate solutions, this is not possible. Simplifying network operations with consolidation, comprehensive monitoring, and automation is required.

The first step to eliminating complexity challenges is to adopt an integrated network and security infrastructure. When all deployed solutions are connected, critical capabilities are enabled that increase operational efficiency, reduce the impact of staffing shortages, ensure employee productivity, and reduce mean time to detection (MTTD) and mean time to remediation (MTTR).

Increase Operational Efficiency

Complex network configurations and security policies take a lot of time and resources, plus present the opportunity for configuration errors—a top cause of security breaches. Organizations will be more secure and improve visibility and efficiency with one unified console for management and analytics across the enterprise. With centralized management and analytics tools, teams can get a single pane of glass with consolidated dashboards, policy and posture management, and security analytics.

To be efficient, IT teams need to be able to go to one place to perform network configurations, set consistent policies, manage the entire network at scale, and gain visibility into the attack surface. Plus, zero-touch provisioning should be available to save deployment time.

"The Cybersecurity Workforce Estimate and Cybersecurity Workforce Gap suggest the global cybersecurity workforce needs to grow 65% to effectively defend organizations' critical assets."[3]

Mitigate the Impact of Staffing Shortages

The global cybersecurity staffing shortage is massive, meaning organizations must find ways to automate labor-intensive tasks. The longer it takes to identify and remediate a network issue that impacts users or a breach, the more damage will be done. Network automation, orchestration, and response are critical to mitigate the lack of human intervention, at the same time eliminating human error.

Security and network integration along with the right tools can tremendously decrease the time to remediate issues impacting users and cyber threats to the business. With incident detection combined with evidence and forensics, network administrators can determine a resolution effectively. At the same time, policies can be triggered that make device configuration changes automatically to close the loop on attack mitigation.

Ensure Employee Productivity/User Experience

Stitching together information from disjointed monitoring tools will not enable the required holistic view of the end-to-end digital experience. Coverage from the end user to the application over any network is the only way to identify performance issues and anomalies of user-to-application access.

Effective digital experience monitoring (DEM) solutions offer complete visibility of network performance and security posture, combined with automated remediation for applications in any deployment—whether container, cloud, on-premises, or hybrid.

With DEM, network operations teams can get insights into employee performance with baseline metrics and diagnostic data from every application, to every user, over every network. Information will be available across heterogeneous and distributed networks to ensure seamless user-to-application interactions and employee productivity.

Reduce MTTD and MTTR

It can take quite a while to identify the root cause of network traffic problems and anomalies that impact user experience, especially in a multi-layered, distributed network. AIOps with built-in network-security automation and orchestration addresses this by eliminating silos and reducing complexity. Today's network operations teams need to be able to ingest and act on absurdly high volumes of data, which is only possible with artificial intelligence (AI), machine learning (ML), and automation.

An effective AIOps solution will have:

- Broad coverage across LAN, WAN, and cloud deployments. Simplified monitoring across wireless, switches, firewalls, and SD-WAN should be available in one console.
- The ability to analyze the dependence of device, LAN, WAN, and cloud events while incorporating policies to identify the root causes of end-user performance issues. This enables teams to cut through the noise and surface the issues affecting the business.
- Integrated orchestration tools for network automation both proactively and through rules. Leveraging AI and ML automation prevents issues before they arise.

Rapid analysis of logs, dynamic insights, and event correlation enabled by ML reduces MTTD and MTTR to resolve network issues before users are impacted.

Conclusion

Today's highly distributed networks that span LAN, WAN, data center, and cloud edges require integrated visibility and control to ensure optimized performance across the network. An integrated networking and security architecture can help enable a high degree of operational efficiency and faster troubleshooting and remediation. Centralized management and security analytics, DEM, and AIOps can unburden network operations teams with simplification and automation.

[1] Paul Muncaster, "Organizations Now Have 76 Security Tools to Manage," Infosecurity Magazine, December 1, 2021.

[2] Martin Roesch, "Complexity vs. Capability: How to Bridge the Security Effectiveness Gap," Dark Reading, February 1, 2022.

[3] "2021 Cybersecurity Workforce Study: A Resilient Cybersecurity Profession Charts the Path Forward," (ISC)², 2021.

June 30, 2022 1:46 PM
1657040-0-0-EN