POINT OF VIEW

Why Users Need Network and Security Convergence

Executive Summary

Security tools impact the network in many ways, yet traditionally, security and networking have operated as distinct, siloed functions. While the advantages of network and security convergence for IT and security teams are clear, the benefits to users may not be as obvious. A secure, reliable network is critical to ensuring employees can do their jobs, and this paper will explain how security and network convergence delivers a more robust and user-friendly network environment.

The Power of Convergence

Because security management can greatly affect network health, when security and networking operate as distinct siloed functions, there are significant challenges for network managers, ultimately affecting network users. When these challenges are resolved through security and networking convergence, the network operates more efficiently, making the network and connecting to it safer, faster, and more reliable. Users then get a significantly enhanced experience with consistent and dependable performance and rapid access to applications and data, helping them be more productive.

Key Advantages for Network Users

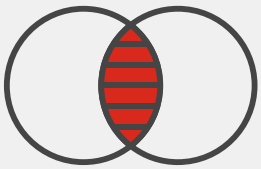
Combining security and networking functions enables unified management and reduces complexities and inefficiencies. It also makes full network visibility possible, which allows IT teams to anticipate and respond to issues, automate fixes, create and enforce policies, implement access control measures, and secure transactions end to end.

Enabling real-time insights and tracking network health, device performance, and security metrics from one source enables IT teams to reduce disruptions, improve performance and reliability, and offer superior connectivity.

Fewer disruptions with optimized security

Quite a few types of security breaches cause network slowdowns or can even take the network down completely, leaving users unable to access the resources they need to work. When security and network management is optimized, there is less chance of a security compromise, so there is less chance of a breach negatively impacting users.

EMA research found that successful NetSecOps collaboration resulted in a 45.1% increase in resolving network performance issues.[1]



Some 40% [of those polled] reported the benefit of [convergence] accelerated mean time to repair of network trouble...[2]

Centralized management of security and networking allows for a more streamlined and coordinated approach to network security, reducing the likelihood of vulnerabilities slipping through the cracks. It also provides the visibility needed to close security gaps and simplifies the process of implementing updates and patches. This ensures that all parts of the network are uniformly protected. The holistic view enabled by convergence is essential for maintaining robust security and optimal performance in increasingly complex network environments.

Better performance and reliability with faster time to resolution

Users expect the network to function at all times, and when it doesn't, they expect the problem to be resolved quickly. However, the cause of the issue is not always clear. For example, a security solution may be misconfigured to block legitimate traffic, which becomes a networking issue that negatively affects users. If security and networking are siloed, it is difficult to discover what is causing the problem. This leads to longer time to resolution, impacting user experience for longer periods of time.

Convergence allows for a single source of truth for information that feeds management tools. Tracking network performance and security metrics in real time facilitates swift detection and resolution of potential issues. Convergence drives proactively finding and addressing problems, helping IT and security teams to respond quickly, often resolving issues before users are aware of them.

When potential threats are detected and mitigated promptly, network disruptions are minimized. This is particularly beneficial for users engaged in activities requiring stable connections, such as videoconferencing and accessing cloud-based applications and other essential business tools. Maintaining consistent and uninterrupted connectivity is crucial for maintaining productivity and efficiency in these scenarios.

Network and security convergence also leads to improved network performance. By integrating security solutions into a cohesive system, network resources are used more efficiently. This reduces unnecessary traffic and frees up bandwidth, resulting in faster data transmission rates and lower latency. Enhanced network performance is especially important for end-users who rely on real-time communication and data processing, as it ensures a smoother and more responsive experience.

More reliable access with streamlined policy management

Without convergence, networking and security policies are typically configured by multiple people, multiple times, in multiple places, increasing the chance of human error. This can result in a variety of problems for users, including blocked access.

Configuration "drift" can occur when systems are separate, resulting in user policies being out of alignment. Key business resources may not be assigned the same permissions across different parts of the network, and users can be denied the access they need to get their jobs done.

Additionally, tracking down where the permissions are not correct to fix them is problematic because policies are spread across systems. With convergence, security mismatches are reduced, issues can be quickly rectified, and users are more likely to have the access they need when they need it.

Conclusion

The convergence of networking and security significantly improves user experience with fewer disruptions, better performance and reliability, and consistent access. Integrating security and networking tools accelerates issue detection and resolution, reducing downtime and maintaining productivity. By providing comprehensive monitoring and real-time insights, convergence enhances overall network reliability and security for the most important part of the network, the users.

[1] "ML-Driven Deep Packet Dynamics Can Solve Encryption Visibility Challenges," LIveAction, Accessed July 8, 2024.

[2] Denise Dubie, "Marrying network, security operations saves money, bolsters enterprise defenses," Network World, January 11, 2024.

July 17, 2024 2:18 PM / 2755549-0-0-EN