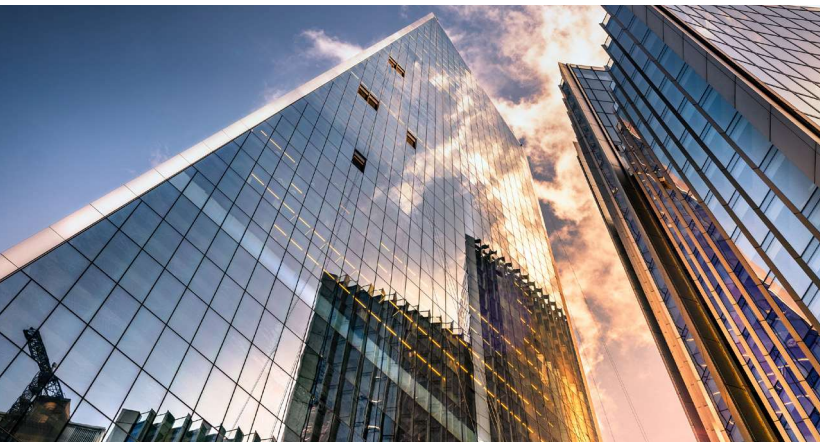




Securing the Modern Enterprise: Why Network and Email Security Must Work Together

As a CISO overseeing security for a large enterprise, you face an ever-evolving threat landscape. Attackers are becoming more sophisticated, leveraging AI and other advanced techniques to breach defenses. Meanwhile, your organization's attack surface continues to expand as applications and data move to the cloud, and employees work remotely from various locations.

In this complex environment, a siloed approach to security is no longer sufficient. Two of the most critical components of your security stack - network security and email security - must work in concert to provide true defense in depth.

The Power of Shared Intelligence

When network and email security solutions share threat intelligence, they become exponentially more effective at preventing attacks. As Mark Ostrowski of Check Point explains:

"When you learn about something that's an active attack or a known phishing site, or known phishing domain...it makes perfect sense to take that same collaboration, same sort of IoC, or the same indicator of that phishing attempt and collaborate across everywhere. So it just makes the phishing protection on the gateway better, and then vice versa."

This shared intelligence allows you to quickly propagate protections across your entire environment. For example, if a malicious file is detected by your network firewall, that intelligence can be instantly shared with your email security system to block similar threats. The reverse is also true - phishing attempts caught by email filters can inform network-level protections.

Interoperability for Seamless Protection

Beyond just sharing threat data, truly integrated network and email security should work together seamlessly. As Jeff Schwartz of Check Point notes: "Historically, if you had a separate email security solution, a separate network security solution, separate endpoint or cloud solution, the interaction and the velocity of being able to provide portability of controls across those different infrastructure types was very, very low."

Modern solutions built on a common platform can provide that crucial interoperability. This allows you to implement consistent policies and protections across network and email vectors. It also enables automated, coordinated responses to threats.

Prevention-First Security

While detection and response capabilities are important, preventing attacks from succeeding in the first place should be the priority. This is especially critical given the speed and scale of modern attacks.

As Jeff Schwartz explains: “Even if an organization has, let’s say, 100,000 connections a day, which I would say is a very small organization, a 1% difference in security efficacy translates to 1,000 false negatives. So 1,000 false negatives means a human being has to go find 1,000 malicious connections that were previously considered benign.”

By leveraging shared intelligence and interoperable controls, you can dramatically improve your prevention capabilities across both network and email vectors. This reduces strain on your security team and minimizes risk to the organization.

Adapting to the New Reality

The way we work has fundamentally changed, with employees accessing resources from diverse locations and devices. As Mark Ostrowski notes:

“Think about providing that prevention capability - the workforce has certainly changed as well over the last few years. We have people coming in through SASE solutions, people coming through traditional VPN, people coming in from the office, people coming in from mobile devices.”

Your security strategy must adapt to this new reality. Integrated network and email security allows you to provide consistent protection regardless of how and where employees connect. It also enables you to implement zero trust principles more effectively across your environment.

The Path Forward

As cyber threats continue to evolve in sophistication and scale, silos in your security stack become dangerous weak points. By bringing network and email security together through shared intelligence, seamless interoperability, and a prevention-first approach, you can significantly strengthen your overall security posture.

This integrated approach allows you to:

- Rapidly propagate threat intelligence across vectors
- Implement consistent policies and controls
- Automate coordinated responses to threats
- Improve prevention rates and reduce false negatives
- Adapt to modern, distributed work environments
- Enable true defense in depth

The threat landscape may be daunting, but with the right integrated strategy, you can stay ahead of attackers and keep your enterprise secure.