5 Reasons Why Financial Institutions Should Refresh Their Cisco Secure Firewall

The firewall. It's been a security workhorse – a trusted sentinel – for decades. It's a reliable partner in blocking threats. But hybrid environments, where remote users access your network and sensitive data from anywhere, have only made your firewall even more crucial. In this evolving world, you need a firewall that simplifies administration, brings clarity, and harmonizes network, workload, and application security across multicloud environments.

Here's why you should refresh your Cisco Secure Firewall:

1 Empower your hybrid workforce

The workplace has evolved significantly in recent years. More and more institutions are gravitating toward a hybrid work model, benefiting employers by saving operational costs while employees gain a better work- life balance. But this poses a new challenge to institutions: how to enable employees to work remotely – with access to critical resources – without increasing risk. Thanks to Secure Firewall Threat Defense Version 7.2, and the built-in crypto accelerator in the 3100 Series – which now boosts VPN performance up to 17x – you can confidently embrace remote work and gain secure, dedicated remote access without sacrificing productivity.

2 Regain visibility over encrypted traffic

It's a fact: Attackers love to innovate. With the proliferation of encryption, attackers are hiding within encrypted traffic designed to ensure data privacy. This challenge is exacerbated by modern protocols like TLS 1.3 and QUIC, making compliance difficult. Decrypting all this traffic is too resource-intensive and impractical. Secure Firewall Version 7.2 offers Encrypted Visibility Engine to deliver a significant advantage. Discover threats without decryption. Detect malicious applications like Tor browser and rogue VPN. Identify and address Shadow IT. Now you can gain superior visibility without compromising compliance, all without the hassle of decryption.

3 Speedy inspection with industry-leading technology

Attackers exploit vulnerabilities, routinely using cutting-edge technologies to run resource-draining attacks, triggering network latency and business interruption. With Cisco Secure Firewall's Snort 3 inspection engine, enjoy 3x faster inspection. Run more security rules and gain deeper visibility without slowing the network down and disrupting the user experience.

4 Real-time protection with automatic updates

Threat vectors are changing rapidly. Overwhelmed SecOps teams are in a constant battle against ransomware attacks, data exfiltration, and malware. Cisco Talos, the largest commercial threat intelligence team in the world, constantly analyzes the latest global threats and regularly releases new mitigation techniques. With Firewall Threat Defense and Talos, you can automate threat response and mitigate known vulnerabilities before they appear on your radar, protecting the integrity of your institution with superior visibility.

5 Increase efficiency with centralized management

In this dynamic multicloud world, you need a firewall manager that eliminates the need for teams to manage multiple environments and removes the silos of disparate security tools. With Cisco Secure Firewall Management Center (FMC), you can centrally manage hundreds of firewalls and gain in-depth visibility into security incidents from a single pane of glass. And now, with cloud-delivered FMC via Cisco Defense Orchestrator, reduce operational costs and increase your team's efficiency with centralized cloud-based management. Enhancements in Firewall Management Center were validated to reduce network operation workstreams by up to 95%, reduce the risk of a breach by up to 80%, and deliver a 195% ROI.

Update your Cisco Secure Firewall software now

We've made updating your Cisco Secure Firewall software easy. Get current with our LevelUp program.

Update my firewall software.

Save time and money during your next firewall refresh

Seamlessly convert your firewall configurations with the Secure Firewall Migration Tool.

Update my firewall hardware.

C22-4103681-00 01/24