SOLUTION BRIEF

# 5 Reasons to Secure Firmware in Financial Services Organizations

Financial services firms are used to dealing with challenging IT and security environments. Teams must simultaneously enable highly-tailored omni-channel customer experiences, protect corporate and customer assets from highly sophisticated adversaries, and comply with the most extensive regulatory requirements of any industry. But as attackers have shifted their focus to firmware – the most fundamental and privileged code on a device – what was once a security oversight has become a critical consideration.

A firmware security platform identifies, verifies, and fortifies firmware – through automated tools – wherever it is in the enterprise, from endpoints and servers to network and IoT devices. Firmware security solutions give financial services firms a way to easily and consistently secure the hidden firmware the organization and its customers depend on. Here are 5 of the most common reasons financial services organizations invest in a firmware security programs, how they benefit, and what teams need to know to ensure firmware stays protected.

## OVERVIEW

**WHO SHOULD READ THIS:**
Cybersecurity teams, solution architects and infosec managers in finance organizations who are tasked with securing firmware in endpoints, servers and network devices.

**WHAT THEY WILL LEARN:**
The key requirements for securing firmware across mid-size and large financial services organizations.

**FURTHER READING:**
- An Auditor's Guide to Evaluating Firmware Security

# 1 Secure the Customer Experience

Modern consumers expect to easily access their accounts and services at any time and from any device they choose. To stay competitive, financial services firms must deliver seamless, consistent, and highly tailored user experiences across mobile, web, and in-person interactions.

Security teams understand that all of these new experiences and applications are ultimately dependent on hardware. Applications will depend upon servers either locally or in the cloud, and customers will rely on their laptops and other mobile devices. A loss of integrity to any of these devices can not only disrupt the customer experience but can lead to severe security issues and reputation damage.

As firmware updates are shipped from manufacturers more frequently, security teams will need to ensure that all servers and cloud assets are properly updated, secured, and free from threats at the firmware level. Organizations may also want to consider validating the integrity of the customer devices: for over a year, the Trickbot banking trojan has been targeting the firmware of infected machines, giving the malware incredible control and persistence on an end-user's device.

# 2 Defend Against Ransomware & Malware

Financial services organizations have always faced an array of highly sophisticated attackers. Many of the most advanced forms of malware such as Trickbot, Emotet, and countless others got their start as banking trojans before they expanded into other industries. Many of these same trojans have become key enablers for ransomware and targeted threat actors. These attackers can target both customer financial data as well as the internal systems of intellectual property.

And while financial organizations are accustomed to being on the front lines of the latest threats, today those lines have shifted to firmware. Through firmware, attackers now have access to a new codebase that is often full of vulnerabilities, rarely updated, yet some of the most privileged code on a device. Once compromised, attackers can control virtually anything on the host including subverting the operating system, reporting false information to applications, stealing data, or permanently disabling the device. Firmware within network devices such as VPNs, routers, and application controllers has become **some of the most popular initial infection vectors both for ransomware groups and APTs**.

A firmware security platform is not intended to provide end-to-end ransomware or malware prevention. But it does provide the crucial ability to proactively discover and mitigate the vulnerabilities and threats hidden in firmware that many ransomware and malware strains are now exploiting. In addition, a true firmware security platform also brings a wealth of unique **threat detection capabilities** not found in traditional tools, including the ability to detect unknown firmware threats.

# 3 Independently Verify the Integrity of the Technology Supply Chain



Every device within an organization is an amalgamation of components and code, often supplied by scores of vendors, suppliers, and sub-suppliers. Any link in this complex technology supply chain can introduce threats or vulnerabilities that can undermine the security of the asset and the entire acquiring organization.

The firmware layer of the technology supply chain is arguably the most complex and potentially challenging to protect. Every component or system within a device may have its own supplier and require its own custom firmware, suppliers can be spread across many countries of origin, and each of these entities can introduce opportunities for mistakes or compromises. Firmware packages are often reused by multiple suppliers, allowing vulnerabilities to be passed on to downstream products.

Supply chain risk can be particularly challenging as the risks are inherited from outside organizations, which the acquiring organization typically can't directly control. A firmware security platform can enable organizations to independently verify the posture and integrity of all the acquired devices throughout their lifecycle. For example, security teams can assess the firmware of devices during the evaluation and selection process in order to identify if prospective vendors and devices contain important vulnerabilities. After a vendor is selected, a firmware security platform allows staff to quickly verify that each device is authentic, was not tampered with before delivery, and remains free of vulnerabilities. These same scans can be applied even after deployment to identify weak update processes, verify the integrity of firmware updates, and to monitor the behavior of new firmware updates to identify signs of malicious activity even within properly signed and validated firmware. Read more on firmware security for supply chains.

# 4 Incorporate Firmware Security In Compliance Programs



Being one of the most valuable and heavily attacked industries unfortunately means that financial organizations are also the most heavily regulated. Most organizations must comply with a complex web of overlapping standards and laws including PCI-DSS, SOX, GLBA, and the BSA. Organizations will then also need to comply with a variety of regional regulations based on where they do business including GDPR, CCPA, LGDP, NYDFS, and PSD2. One of the only saving graces is that the vast majority of these regulations can be mapped to a few all-encompassing security frameworks, such as NIST's Cybersecurity Framework (CSF) and SP 800-53 rev 5.

These core documents specifically call out the importance of firmware security, and these requirements have likewise been mapped to the aforementioned financial regulations. In fact, SP 800-53 rev 5 consistently refers to the combination of "hardware, software, and firmware" when discussing risks as well as specific controls. This foundational document calls out firmware 149 times mapping to many of the families of security controls including SI—System and Information Integrity, SA—System and Services Acquisition, CM—Configuration Management, AC—Access Control, RA—Risk Assessment, IR—Incident Response, and MA—Maintenance. Additional details on specific 800-83 controls and firmware security recommendations can be found here.

All of this means that firmware is definitely "in scope" for financial regulatory requirements, and that auditors are increasingly requiring organizations to provide insight into firmware inventories, update and patch management programs, as well as into their firmware-level threat detection and prevention processes.

# 5 Verify Firmware Integrity in Cloud Providers and Platforms

The shift to the cloud introduces a variety of new security issues and concerns that security teams need to address. However, while the "cloud" can often seem like yet another layer of abstraction, it is important to remember that all clouds, whether private, public, or hybrid ultimately rely on server hardware. The cloud may make more efficient and economical use of hardware, but it is still reliant on that underlying hardware.

As a result, an organization's cloud strategy can include a sizable amount of risk tied to the firmware in the underlying servers and infrastructure. Servers in particular heavily rely on out-of-band management capabilities built into components known as baseboard management controllers (BMCs). These BMCs allow staff to administer all the most critical aspects of the server including updating firmware, operating systems, and other critical settings even when the server itself is completely powered off. The recent **iLOBleed** attacks provided a real-world example of how attackers exploited server BMCs in order to wipe the data from infected servers.

A firmware security platform helps security teams take a proactive approach to ensure the integrity and security posture of their cloud infrastructure. For hardware in an organization's private cloud or bare-metal cloud services, security teams can directly scan devices for firmware vulnerabilities, verifying that all running firmware matches known-good samples and is free from threats.

# Conclusions

Firmware is the bedrock of computing, and rapidly becoming one of the most active attack surfaces as adversaries probe "below the waterline" of traditional security tools. A consistent, coordinated, and efficient approach to firmware security is essential in order to stay ahead of these threats, and ensures the firm and its customers' data remains safe. A firmware security platform is an invaluable asset in this regard and gives teams the automated tools and expertise they need to Identify, Verify, and Fortify firmware, wherever it exists in their extended networks — from endpoints and laptops to network devices and servers.

To learn more about the Eclypsium solution and how it can help deliver better, more secure experiences for financial services customers, please contact us **info@eclypsium.com**.