7 Ways Financial Services Firms Can Conduct Cybersecurity at Business Speed

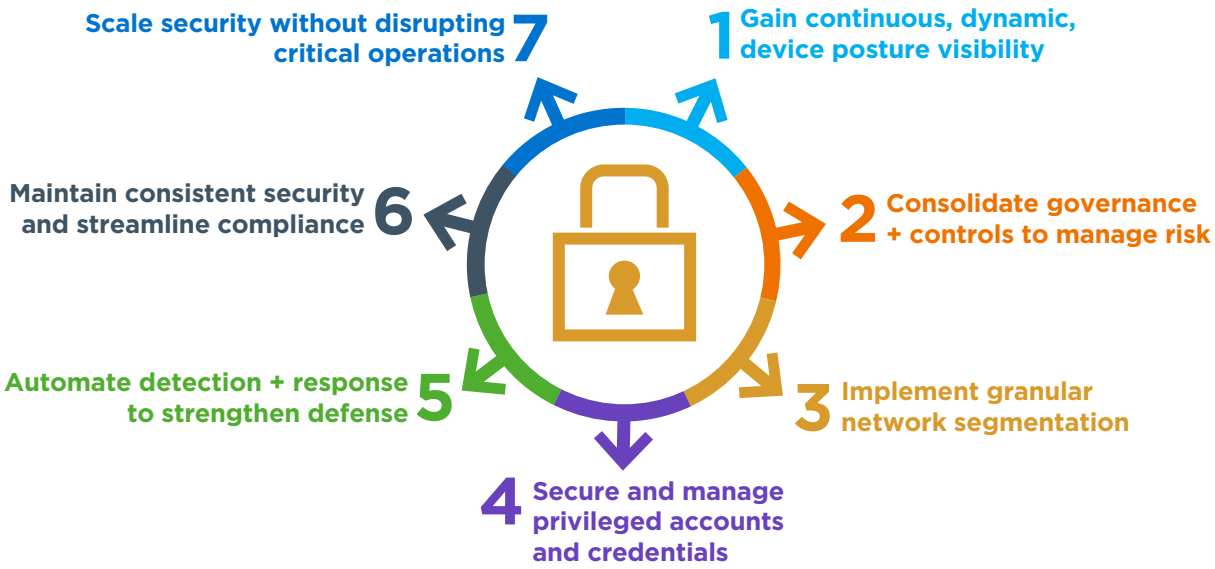
Financial services firms seeking competitive advantage and market success are under pressure to innovate as they develop cutting-edge algorithms and respond to customer demand for 24x7 access. From mobile and online banking to high-frequency trading and hedge fund management, millions and even billions of dollars are being invested in the infrastructure at every level. Maximum scalability and compute elasticity serve as tools to power the engine of financial services as workloads migrate from networks and the data center to the cloud.

In the midst of this technology transformation, security concerns – due to a barrage of cyberattacks targeting this sector – and mounting compliance regulations compete for attention. The big challenge financial services firms face is how to dynamically extend security and compliance to an ever-changing business architecture powered by massive compute capabilities and a web of technological complexity.

By implementing the right solution and best practices, security can scale and evolve with your changing business and technology needs. Security can safeguard vital data and transactions, minimize disruption and streamline compliance while supporting business agility and change.

Here are seven ways you can stay secure and compliant without interfering with mission-critical transactions and operations or disrupting the daily activities of employees, customers, partners and guests.

THE 7 WAYS TO CONDUCT CYBERSECURITY AT BUSINESS SPEED



1. GAIN STATUS CLARITY AND CONTINUOUSLY MONITOR SECURITY POSTURE ACROSS A CONSTANTLY CHANGING NETWORK ENVIRONMENT.

Accurate device visibility and context is paramount in knowing the status of and improving security posture. The dynamic nature of financial networks increases the threat landscape by adding compute, network, storage and mobility assets which can hinder visibility. By using a solution that gathers this asset intelligence without disrupting the business operations—upon connection and continuously—you can minimize blindspots in the physical and virtual network to build a robust security foundation.

An added benefit of this asset intelligence gathering is the ability to collect pertinent information about servers, devices, users, applications and operating systems to provide you with an accurate asset inventory, along with the current patching and configuration state. While this is typically the task of the CMDB system, they are highly dependent on what they can see or have seen. Having an accurate, single-source-of-truth asset inventory, requires verification using tools that can continuously see more of what's on the heterogeneous network.

2. CONSOLIDATE GOVERNANCE AND CONTROLS TO MANAGE RISK.

Adding elastic compute, network, storage and mobility technology to meet business needs typically requires using highly specific, point security solutions used in different places in the network—which fragments control and adds risk to the firm. By understanding and prioritizing the business processes, applications and infrastructure that are critical, you can develop a structure and related policies to stay vigilant about security and compliance in a unified manner.

How do you cohesively align these fragmented controls to ensure real-time mitigation of these risks? Reinforce this consolidated control throughout the firm with a solution that uses the same people and processes. Drive decisions with up-to-date asset intelligence to build context and reinforce actions, and implement governance and policies leveraging segmentation and access controls.

3. IMPLEMENT GRANULAR NETWORK SEGMENTATION.

A well-formulated network segmentation strategy enables you to separate highly sensitive financial data and mission-critical applications. By leveraging real-time asset intelligence, you can create security policies and determine the optimal network segmentation zones within physical and virtual environments—regardless of where they are located. For example, you can choose to segregate device types across the campus, data center servers and the cloud. That way, you'll ensure that rogue devices are not allowed and that only authorized devices can connect in certain environments. Likewise, you can ensure that critical applications are segmented from lab, development and general IT environments.

4. SECURE AND MANAGE PRIVILEGED ACCOUNTS AND CREDENTIALS.

Exploitation of privileged account credentials is one of the most common ways for attackers to access sensitive financial data and applications. To reduce your attack surface and risk, it's a good idea to limit the number of administrative and user privileges overall. To start, you need to gain visibility into privileged accounts on all types of managed and unmanaged devices, including IoT devices, that connect to the network. Employ an agentless solution that can automate policy-based access control and enforcement of these devices based on their security posture and behavior.

5. AUTOMATE DETECTION AND RESPONSE FOR A STRONGER DEFENSE AND IMPROVED OPERATIONAL EFFICIENCY.

Avoiding breaches is a top priority for the financial services sector. For the second straight year, financial services tops the charts as the most targeted industry with the highest volume of security incidents and the third highest volume of cyberattacks.[2] All too often, it's a challenge to keep up with threats because security teams don't know where to focus their attention. They get bogged down by an overabundance of data from disparate multi-vendor security tools that don't communicate with one another.

By orchestrating security information sharing across your current tools, you can get the most out of your investments. For example, correlation and analysis of automated feeds of high-value endpoint information by your security information and event management (SIEM) solution can help your team more quickly identify, prioritize and mitigate incidents. By sharing context and by controlling intelligence across systems, you're better able to enforce consistent network security policies. A unified and integrated approach to security will not only contain the spread of malware across the network, it will also result in enhanced efficiency through automated workflows and processes and will yield a higher return on investment.

6. MAINTAIN CONSISTENT SECURITY ACROSS YOUR ENTERPRISE AND STREAMLINE COMPLIANCE.

The Financial Services Sector Coordinating Council (FSSCC) estimates that financial institutions are impacted by up to 24 federal and state regulatory, oversight and examination agencies and self-regulatory organizations,[3] such as MiFID II, EU GDPR , SWIFT CSP, FFIEC, NYDFS, to name a few.[4] Most of these compliance regulations require broad and deep technology controls. Extending continuous monitoring and security controls across your entire environment—from campus to data center to cloud—helps you close security gaps, simplify processes, provide policy-based security throughout all your infrastructure touch points and ease compliance. Advanced network visibility solutions can discover corporate-issued devices that lack required security software or have out-of-date security software and trigger antivirus programs to install or update the software on noncompliant endpoints so that they regain compliance. Some solutions also supply easy access to reports, along with compliance validation through built-in templates that align with stringent security frameworks and regulations. These capabilities save time and effort and provided added reassurance at audit time.

7. SCALE SECURITY WITHOUT DISRUPTING CRITICAL OPERATIONS.

Large-scale, global financial services firms often have hundreds of thousands of endpoints to secure—and this can be a monumental task. Flexibility and centralized management are key. Ideally, your solution should work across a heterogeneous environment—from data center to cloud—and allow you manage up a large number of endpoints with a single console for greater control and efficiency. This level of scalability is especially important in banking environments with geographically distributed branches. In an industry that is frequently subject to mergers and acquisitions, a scalable security solution can address the sprawling heterogeneous network environments that emerge as a result of growth and consolidation.

CONCLUSION

In the highly demanding and highly regulated financial services sector, security needs to support both the rapid pace of technology infrastructure transformation and the compute elasticity required for day-to-day operations. By deploying the right network visibility solution and by implementing best practices, you can successfully achieve your business goals and build a stronger and more cohesive security and compliance framework.

Find out how ForeScout can help your financial services firm gain visibility, exercise control and enable continual monitoring of managed, unmanaged and IoT devices while demonstrating compliance. https://www.forescout.com/solutions/industries/financial-services/

Learn more at
www.ForeScout.com

ForeScout

ForeScout Technologies, Inc.
190 W Tasman Dr
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

[1] https://www.bankinfosecurity.com/blogs/3-steps-to-asset-management-software-auditing-p-2611
[2] https://www.scmagazine.com/top-five-most-frequently-targeted-industries-of-2017-are-financial-services-information-and-communications-technology-manufacturing-retail-and-professional-services/article/758556/
[3] https://www.nist.gov/sites/default/files/documents/2017/02/14/20160219_financial_services_sector_coordinating_council.pdf
[4] Markets in Financial Instruments Directive (2004/39/EC) (MiFID II), General Data Protection Regulation (GDPR), SWIFT Customer Security Programme (CSP), Federal Financial Institutions Examination Council (FFIEC), New York Department of Financial Services (NYDFS)