FINANCIAL SERVICES IT SECURITY REFERENCE BLUEPRINT

IT security and network teams at financial institutions around the world must address demands to rapidly adopt new technology, protect intellectual property, secure myriad commercial and custom applications, and comply with regulations. Meanwhile, they must also securely enable access to personal and corporate financial data from a variety of access points – retail bank branches, campus sites, mobile devices, ATM networks and third-party business partner networks – despite the increasing volume and sophistication of threats. The Security Reference Blueprint for Financial Services IT empowers institutions to address all these concerns, augment the security of their existing infrastructure, enable new applications, provide secure access to data and prevent advanced threats without disrupting vital business operations.

Table of Contents

I. Executive Summary

The Security Reference Blueprint for Financial Services IT enables institutions to augment the security of their existing infrastructure, enable new applications, provide secure access to data and prevent advanced threats without disrupting business operations. This approach allows institutions to more effectively focus on today's evolving security threats, protect customer and corporate data from compromise, better address the expanding scope of compliance, improve resilience and availability, and meet technological and competitive challenges, such as networked mobile devices or the adoption of cloud-based computing. All this can be accomplished with the Palo Alto Networks® Security Operating Platform while complementing existing security capabilities as part of a layered defense approach.

II. Security Concerns for Financial Services

As the primary custodian of both personal and corporate financial assets and data, the financial services industry remains one of the largest targets for attack, sitting among the top five industries for security incidents and confirmed data loss.[1] Cyberattackers seek to steal funds from accounts; obtain personally identifiable information, or PII, for identity theft or credit card fraud; "jackpot" ATMs; or destabilize global financial markets to further political or other agendas. At the same time, changing end-user preferences for mobile computing, open banking, and the shift toward software, infrastructure and platform as a service – SaaS, IaaS and PaaS – cloud-based extensions can increase business, operational and reputational risks if not appropriately secured. The combination of these realities with the growth in demand from customers, business partners and investors for anytime, anywhere access to their financial information, as well as the considerable regulatory, business and technological changes in financial services environments today, has increased the need for secure networks that can seamlessly evolve in response.

Complex Environments

In addition to a steady diet of cyberattacks, the challenges financial institutions face include:

- Managing a mix of applications, such as internally developed software, commercial applications that are often highly customized, or those resulting from past mergers and acquisitions.
- Maintaining a multi-vendor philosophy for technology to address resiliency and vendor management concerns.
- Supporting IT infrastructure for multiple lines of business across diverse geographies that have disparate requirements and varying perspectives. For example, low-latency trading applications have distinct needs from those of other banking applications.
- Adhering to a combination of local, regional, national and industry regulations, increasing time and effort required for compliance, as well as causing dramatic operational and business model changes. Some of these call for a "defense-in-depth" approach, and other recommendations may not truly improve cybersecurity but are nonetheless required to achieve compliance.
- Shifting requirements for working capital, such as the Volcker Rule of the Dodd–Frank Act in the U.S., that affect investments in operations and businesses. Consequently, many institutions continue to operate in cost-optimization mode even though many years have passed since the global financial crisis of 2008.

Security Sprawl

The complexity of these challenges is exacerbated by many institutions having acquired multiple security products that are oblivious to one another and cannot function cohesively, reducing their effectiveness. Some of this security infrastructure sprawl was intentional in support of the belief that "defense in depth" – the notion that if one system misses an attack or instance of malware, another will catch it – equates to "vendor in depth." Regardless, the sophistication of attackers outpaces the capabilities of stand-alone point products, leading institutions to buy the next "best" security technology once more to defend themselves.

The Response

Unfortunately, large financial institutions can neither easily unwind nor consolidate their legacy security packages without potentially opening themselves up to significant operational and business risk. To prevent today's threats, existing security infrastructures must be complemented or replaced, where possible, by a new and effective approach to security that incorporates key security principles focused on the current threat environment.

Such an approach can address the types of exposure and damage cited above as well as reduce inefficiencies caused by unauthorized applications or misuse of network resources. This paper discusses using the Palo Alto Networks Security Operating Platform to implement these principles to detect and prevent threats to financial institutions' networks, improving network efficiency while reducing complexity and unnecessary overhead. It also provides a way to secure these environments and gather intelligence about incursions to mitigate or eliminate damage from future attacks. Native integration and automation between the components of the platform work to prevent successful cyberattacks and enable your team to focus on what matters.

1. The 2018 Verizon Data Breach Investigations Report

III. Reference Blueprint Goals and Security Principles

This Security Reference Blueprint for Financial Services IT describes a transparent, non-disruptive security framework that uses the capabilities of the Security Operating Platform to buttress and enhance the security of existing infrastructure. Using the blueprint enables IT security and networking professionals to:

- Reduce the overall exposed attack surface of a financial institution.
- Eliminate the ability of risky, unknown applications to access or embed themselves within the network.
- Prevent data breaches and the loss of confidential customer financial information and other sensitive records.
- Protect vital operational networks from compromise, unwanted downtime or service interruption caused by security breaches or data leakage. For example, any resources open to third parties, such as business process outsourcing, direct customer access and external business partners, warrant tighter controls.
- Comply with relevant global and regional government regulatory bodies, such as the Federal Reserve Bank, OCC, SEC, FCA, EBA, HKMA and MAS, as well as industry standards, such as PCI DSS, SWIFT and FINRA regulations.
- Stop corporate credential theft and exfiltration of PII or other sensitive data. Credential theft is a key element in many recent, successful attacks against the financial sector.
- Complement existing investments in security products through extensive technology partnerships Palo Alto Networks maintains with many leading companies, such as Proofpoint™, Tanium® and VMware®, to ensure an experience of seamless integration.

The reference blueprint allows financial institutions to detect and prevent today's network threats as well as extend that protection to endpoints. In addition, it will provide an opportunity to gather and correlate data about the intrusion from multiple, integrated data collection points to help the platform evolve and keep pace with the adversary. The reference blueprint incorporates core security principles to effectively and efficiently protect an institution whether traffic travels within or outside its network; whether threats come from the inside or outside, known or unknown; and whether exposure is intentional or accidental.

These core security principles include:

- Comprehensive visibility, effective control, and safe enablement of applications and activity to reduce the threat footprint as well as minimize needless bandwidth consumption.
- Segmentation to protect and defend systems at all portions of the network, preventing malware and cybercriminals from moving throughout the network.
- Defense of endpoints that may be temporarily off-network, such as mobile devices and laptops.
- Extensibility to safeguard data in cloud computing environments, including IaaS, PaaS and SaaS.
- Advanced malware detection to identify and prevent both known and zero-day attacks.
- Timely reporting to enable IT, cybersecurity and intelligence professionals to coordinate actions.
- Immediate, automatic sharing and distribution of threat intelligence between sensors and enforcement points.

The sections that follow address each of these principles in detail.

IV. Core Security Principles

Policy-Based Application Visibility and Enforcement

To effectively protect a financial institution, security and network teams must have visibility into applications, connected devices and individual users as well as their impact on security. Internal teams can make contextual, policy-based decisions about which applications to allow or block for specific user communities or groups. This provides much more flexibility when catering to the needs of specially designated network users or user groups while drastically reducing the volume of threats on the network.

Using a next-generation firewall to characterize applications, financial institutions can immediately reduce their threat exposure. Institutions can choose to block applications that carry the highest risk, such as peer-to-peer applications, immediately reducing the network's threat footprint, exposure to potentially malicious software and likelihood of data breaches.

Palo Alto Networks can provide a free Security Lifecycle Review, consisting of a one-week analysis of your environment with a complete report at the conclusion. For more information:

https://start.paloaltonetworks.com/cybersecurity-lifecycle-review-risk-assessment

To protect the network with this level of visibility, the Security Operating Platform can provide:

- Complete visibility and granular control over applications that attempt to evade detection by masquerading as legitimate traffic, hopping ports or sneaking into the network using SSL/SSH encryption.

- User identification that allows security teams to safely enable applications and content based on the employee and group identity information stored in enterprise directories. As an example, most employees do not require access to gambling-related websites, but analysts covering the gaming industry may. Such individuals could be allowed to access the gambling URL category by virtue of their User-IDs or group membership.
- Content identification that combines a real-time threat prevention engine with a comprehensive URL database and elements of application identification to limit unauthorized data and file transfers; prevent theft of corporate login credentials; and detect and block a wide range of exploits, malware, dangerous web surfing as well as both targeted and unknown threats.

As part of the application policy creation process, financial institutions can approve applications by user group in context – ensuring access to the applications they need. It is important to note here that using a port-based firewall or applying port-based policies on a firewall cannot distinguish the status of an application as risky; it can only identify applications as unauthorized or safe and of business value.

Application-based security policies can help control access in the following ways:

- Identify frequently used applications so you can more easily highlight unknown or potentially risky applications. You can first monitor traffic across your next-generation firewall to learn what's legitimate or not and put a traffic classification strategy in place.
- Identify applications that involve risks, such as:
  - Cloud-based file sharing, such as Dropbox®
  - Data transfer and exfiltration
  - Suspicious DNS, such as new, uncategorized domain names
  - Peer-to-peer networking
- Look for other dynamics within your environment, such as:
  - Port scanners and/or vulnerability scanners
  - Unapproved third-party networks
- Build groups for traffic types to always block:
  - Applications such as Tor®, BitTorrent® and Dropbox
  - IP ranges based on geographic location – your data center may have no need to talk to internet addresses in China, for instance
- Identify, monitor and analyze all SSL/TLS-encrypted traffic involving external websites. Though many applications and websites use encryption for privacy, malware authors are increasingly delivering encrypted malware payloads. All encrypted network traffic should be examined for the presence of malware, exfiltration attempts or other inappropriate usage.

By implementing granular application identification instead of only port-based filtering, administrators can gain greater visibility and precise control, reducing risk significantly.

Network Segmentation and Zero Trust

In some more recent targeted attacks, attackers have used spear phishing and social engineering techniques to gain initial access through unwitting victims. Many attackers can penetrate a target network, successfully establish a beachhead and remain undetected for a significant period while performing damaging actions.

The Zero Trust approach to enterprise network architecture, coined by Forrester Research, makes it very difficult for such adversaries to succeed and for everyday malware, or even malicious insiders, to move across the network. Based on verification of all users, devices and applications traversing your network, establishing Zero Trust boundaries[2] effectively compartmentalizes your user groups, devices and/or data types, such as PCI and banking-regulated data.

Segmenting your network into discrete zones based on data criticality carries three major benefits:

- Limit the scope of vulnerability. Separate vulnerable parts of the network, or older legacy servers that cannot be patched, from others.
- Limit the data that may be exposed and compromised in a breach. Protect critical portions of the network from the rest of the general-purpose IT environment.
- Limit the scope of compliance. Smaller portions of the network and fewer systems are subject to compliance audits.

Network segmentation can focus on isolating and protecting systems based primarily on the sensitivity of the data in the zone and the level of risk if that data is exposed. Next-generation firewalls can inspect all traffic entering a zone and use whitelisting to allow only known, trusted traffic, which is then continuously monitored for security vulnerabilities and malicious activity.

2. Many organizations use virtual local area networks, or VLANs, to segment their networks, but VLANs simply isolate traffic at Layer 2. They are unable to enforce the control of privileged information. Furthermore, by itself, a VLAN cannot inspect traffic for threats.

This tactic stops unknown, malicious traffic from entering a zone. Next-generation firewalls can also be configured to control which users have access to data or applications within a zone. Additionally, segmentation reduces the effort required to demonstrate compliance by limiting reviews to only the zone or zones in which data of interest resides.

There are two separate but complementary segmentation strategies:

- Control "north-south" traffic entering a network perimeter zone or private, public, or hybrid cloud.
- Control "east-west" traffic entering and exiting virtual machines within a zone.

Zero Trust boundaries, zones or virtual segments in a network enable you to defend each zone from any malicious traffic entering or exiting that zone. To prevent malware activity and lateral movement of advanced attackers through a financial services network, it is necessary to apply the controls at all key entry and exit points. Examples of segmentation zones include:

- Applications and databases that contain personal financial information belonging to one line of business, such as consumer banking.
- Administrative or corporate data and applications, such as for HR, payroll and legal departments.
- Networked or mobile devices used by tellers, financial advisers that access personal financial information.
- Specific organizational or geographic zones that are considered high-risk due to, for instance, pending acquisition, divestiture or geopolitical conditions.
- Access to third-party business partners, such as market data providers, stock exchanges, payment networks and ATM networks.
- Customer-accessible applications and resources, either via the internet or direct WAN connections.

Each zone in the network should be protected by a next-generation firewall, which brings several benefits. Beyond validating the whitelisted applications and their intended users, the Security Operating Platform performs several other important security functions on traffic entering and exiting a zone:

- Threat Prevention blocks malicious files with signatures for known threats.
- WildFire® threat analysis service detects and blocks zero-day threats, and is available as an on-premise or cloud-based deployment. The on-site appliance includes options for resiliency and controlled exchange of threat intelligence with the cloud-based environment for improved efficacy.
- URL Filtering blocks access to malicious websites and URLs, and shares newly discovered malicious domains and IP addresses internally or with the broader subscriber community as they're discovered.

Although Zero Trust should be the ultimate goal, many financial institutions have essentially open internal networks and may still perceive it as a significant challenge. However, even taking a few steps toward Zero Trust network segmentation can help institutions better protect critical financial functions and sensitive information, reduce the exposure of vulnerable systems, and prevent movement of malware through their networks. As a recent example, after a series of successful attacks on its members, SWIFT imposed a set of mandatory security controls that includes the separation of local SWIFT-related infrastructure from the rest of a financial institution's IT environment.

Protection Across the Network

In addition to application visibility and network segmentation, there are a few other considerations for your network to ensure effective security across the cyberattack lifecycle.

Private, Public and Hybrid Clouds

Although network segmentation addresses the protection of "north-south" traffic entering and exiting data centers as well as that of "east-west" traffic between applications in their own segments within data centers, it's worth noting a few more considerations for these environments:

- **Reliability**: Consider active/active high availability for your "north-south" boundary appliances to synchronize their configuration and session information continuously, ensuring no lost traffic or degraded performance in the event of a hardware failure.
- **Orchestration and management**: Use centralized management to ensure policies can keep pace with the rate of change to your virtualized workloads. In VMware NSX® deployments, automate virtualized next-generation firewall provisioning through predefined APIs.

VMware and Palo Alto Networks have integrated security for software-defined networks to provide:

- Automated, transparent insertion of next-generation security services in software-defined data centers.
- Complete next-generation security capabilities for all traffic within a data center.
- Dynamic security policies that understand the context of the virtual machines in a data center.

https://www.paloaltonetworks.com/partners/vmware.html

- **Policy consistency**: Centrally define and consistently apply policies to all devices to reduce complexity, and use centralized management for a single point of control for all firewalls, physical and virtual. Otherwise, gaps in threat protection are possible.

The move from traditional data center architecture to hybrid cloud infrastructure is a growing trend in the financial services industry. Implementing virtualization for existing applications within a data center reduces costs, enhances business flexibility and may even improve security. Moreover, since Palo Alto Networks next-generation firewalls have the same features across physical and virtual form factors, virtualization lays a foundation that simplifies future cloud migration.

Although security concerns have made the financial services industry relatively slow to adopt the public cloud, many institutions are now taking steps to explore it, if not embrace it. In line with their multi-vendor approach, many financial institutions will likely adopt more than one public cloud provider for diversity and flexibility.

For more peace of mind, continuous monitoring of public clouds allows institutions to deploy applications with confidence, knowing that security is enabled. Moreover, financial institutions can achieve continuous compliance by analyzing the configurations of all cloud services and account settings against organization- or industry-defined controls.

Additionally, extending next-generation security capabilities to your SaaS environments and cloud storage services is important to protect data from accidental disclosure and from threats originating in the public cloud.

Endpoints

To effectively protect all endpoints on the network, IT teams should enforce the Zero Trust model everywhere, down to laptops, desktop PCs and servers.

Attention should be paid to endpoints vulnerable to external threats that could affect critical business processes. For example, endpoints dedicated for use by business process outsourcing or third-party software developers may warrant greater protection than employee desktop PCs. Even employee endpoints are not all created equal; desktop PCs for bank tellers or financial advisers may be more valuable targets than those of the procurement team.

Your endpoint security strategy should cover all endpoints, including virtual and physical desktops, laptops, servers, and ATMs, regardless of patch or software update level.[3]

The two main threats to endpoints are executable malware and exploits that target specific application vulnerabilities. It is critical to protect against both, but exploit prevention is particularly important, even within whitelisted applications, as zero-day threats can appear at any time.

To effectively protect the endpoint:

- Employ lightweight agents to monitor for exploit techniques and malicious executable files.
- Apply policy-based restrictions. You can easily set up policies to restrict specific execution scenarios. For example, you may want to prevent the execution of files in the Microsoft® Outlook® temporary directory or of a specific file type directly from a USB drive.
- Reconsider your antivirus strategy. Traditional antivirus products have proven ineffective as compromises continue.

Security and IT teams should also enforce the Zero Trust model for mobile and specialized devices, of which there are three major categories to consider: Windows® or Mac® laptops; smartphones and tablets; and specialized devices, such as ATMs and point-of-sale terminals. Depending on the type of device, you should implement the following capabilities in your security program for mobile devices where possible:

- Secure connectivity via a VPN tunnel over the internet to the corporate network to protect communications.
- Regular security status checks for all managed devices to ensure they have updated protection.
- Identification and remediation of all mobile malware on devices that could affect your institution's network.
- Granular policies to determine which users and devices can access sensitive applications and data from mobile devices that are verified to be up-to-date and clean of malware. Policy criteria can be based on application, user, content, device and device state.

The natively integrated Palo Alto Networks Security Operating Platform brings network, cloud and endpoint security into a common architecture, with complete visibility and precise control. The platform approach enables your organization to detect and prevent successful attacks, streamline day-to-day operations, boost security efficacy, and stop threats at each stage of the attack lifecycle.

https://www.paloaltonetworks.com/products/platforms.html

Security subscriptions on the platform are seamlessly integrated to add protection from both known and unknown threats, classification and filtering of URLs, and the ability to build logical policies based on the specific security posture of a user's device.

https://www.paloaltonetworks.com/products/platforms/subscriptions.html

3. Laptops can be especially at risk if they contract malware on a public network, such as a Wi-Fi hot spot at a hotel or airport. If a returning user connects an infected laptop to the corporate network, the risk of infecting other systems undetected increases significantly.

- Ongoing scanning consistent with that conducted on your network: intrusion prevention system for vulnerabilities, malware protection for mobile threats and URL filtering for malicious websites.

Advanced or Zero-Day Attack Prevention

You must handle advanced attacks and zero-day malware quickly, using automation to ensure threat prevention immediately upon discovery. This is critical to prevent subsequent evasion and further attack attempts. When any unknown file attempts to enter a trusted perimeter or network zone, that file should be thoroughly inspected in an advanced malware execution environment for static and dynamic analysis, with multiple means to address evasion techniques. Finally, automatically generated protections against any newly discovered threats should be published to all subscribed next-generation firewalls. WildFire distributes new protections automatically in as few as five minutes, in addition to pushing information on newly discovered command-and-control domains and other malicious websites to URL filtering databases.

Timely Reporting, Threat Intelligence and Correlation

Cohesion between IT, cybersecurity and intelligence professionals reduces the danger threats pose to your network. Coordinating your endpoint, data center, networking and security teams will help your institution fully understand the potential threats to your network, ensure immediate access to priority events, and enable automatic sharing and distribution of intelligence.

WF

Palo Alto Networks WildFire cloud-based threat analysis service provides dynamic analysis of suspicious content in a "bare metal" environment to discover unknown threats and automatically create as well as enforce content-based protection. It also detects malicious links in email, proactively blocking access to malicious websites.

WildFire is also available as a resilient, scalable on-premise appliance able to query the WildFire cloud and make use of the threat intelligence found there.

With interoperability across all the security capabilities discussed here, the Security Operating Platform makes this coordination and collaboration easy. Individual next-generation firewall and management appliance views can be customized for each administrator or department while maintaining shared views into alerts and other activities of interest across your network. Refer to the next section for an overview of specific capabilities that improve reporting and threat intelligence correlation.

V. The Security Reference Blueprint for Financial Services IT

The key security principles outlined in this paper can be fully realized with the capabilities of the Palo Alto Networks Security Operating Platform to protect your institution from endpoint to network core to cloud. This section provides a high-level reference blueprint for financial services IT that incorporates the described principles using the Security Operating Platform.

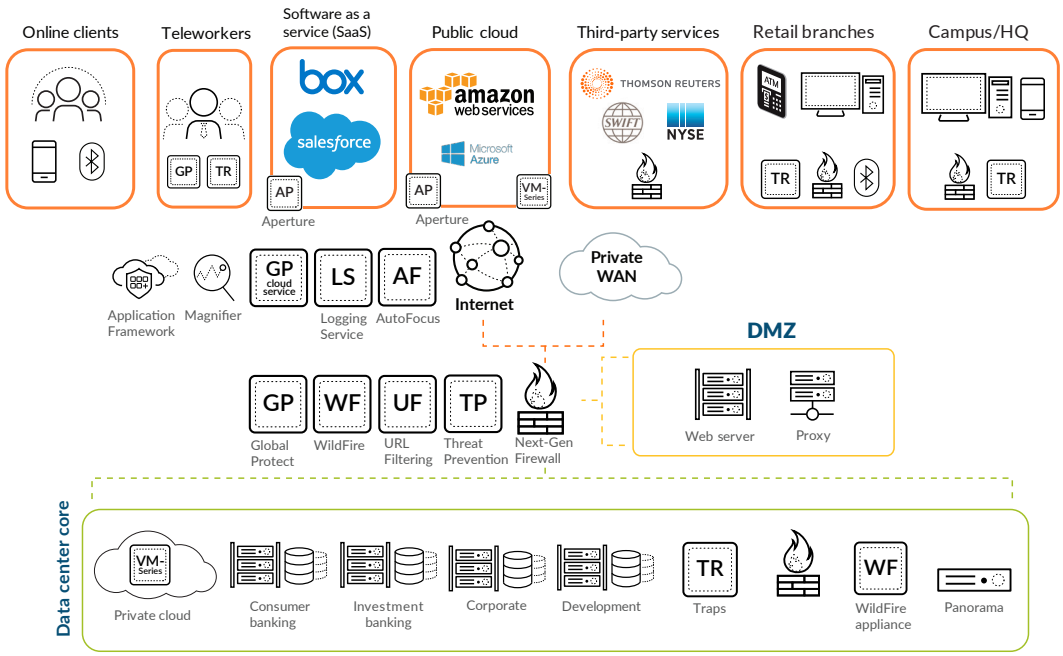

Figure 1: Security Reference Blueprint for Financial Services IT

Although your unique network requirements will guide your architecture decisions, including appropriate network segmentation, the financial institution network in this example is segmented into a "demilitarized zone," or DMZ; a data center zone; private and hybrid clouds; internal corporate access points for campus and remote offices; and external zones for third parties, such as partners, vendors and customers. Within the data center, further segmentation by line of business, such as consumer banking, institutional banking and corporate services, is also depicted.

Palo Alto Networks next-generation firewalls, physical or virtual, can scan all traffic entering and leaving different zones to guard against malicious payloads or inappropriate data leakage, and enforce policies that make use of application, user and content identification.

- URL Filtering enables access to all whitelisted sites, with bandwidth control for designated categories and more. The URL Filtering service identifies categories of malicious sites so that appropriate policy control or investigation can be enacted.
- Known threat prevention covers detection and blocking of common or known malware on the network. Command-and-control signatures flag requests to and from malicious domains, protecting your data from being stolen, while DNS sinkhole technology allows administrators to redirect outbound requests to malicious domains or IP addresses to an internal IP address, preventing those requests from ever leaving the network. Automatically compiled reports of compromised machines provide actionable data for incident response teams.
- Advanced and zero-day attack prevention makes use of a malware execution environment that automatically creates signatures for all next-generation firewalls. All unidentified files should be sent to WildFire – available as a cloud-based subscription service or an on-premise appliance – for static and dynamic analysis of potential threats. WildFire automatically distributes data on zero-day threats it identifies to all subscribed WildFire customers in as few as five minutes.
- Credential theft prevention builds upon user and content visibility, with the next-generation firewall blocking the transmission of corporate login credentials to websites with phishing characteristics. Phishing attacks have become more sophisticated over the years, and many individuals have been duped by well-crafted emails from widely distributed as well as targeted spear-phishing campaigns.

DMZ

The DMZ, which is externally facing, as shown in Figure 1, has several functions. The outer portion of the DMZ provides the primary line of defense, including protection against DDoS attacks. The DMZ proper contains externally visible resources such as web servers and web proxies. Finally, the inner portion controls traffic headed for the internal network and can provide first-level URL and content filtering for outbound traffic. Credential theft prevention – blocking the submission of corporate credentials to external phishing websites – can also be performed at the perimeter firewall.

Although Figure 1 depicts a single NGFW for the network perimeter, it can also easily be designed with a separate security appliance for each external entry point or function. For example, separate NGFWs may service inbound customer traffic via the internet and traffic from third-party partners, respectively. This separation may be warranted to reduce the fault domain and suit business-specific change control windows.

Corporate Data Center

A separate NGFW controls north-south traffic into and out of the data center zone. Using the Zero Trust model, the NGFW rejects all but whitelisted traffic to ensure only authorized applications, users or content can traverse the network. Network segmentation of resources by function, such as development, test or production, is another option in the data center.

The use of private and public clouds is growing, and both can benefit from the protection of next-generation firewalls – physical or virtual in the private cloud, virtual in the public cloud. Palo Alto Networks VM-Series virtualized next-generation firewalls support the same security features as their physical counterparts to safely enable applications flowing into and across your private, public and hybrid cloud computing environments. VM-Series firewalls work with many popular hypervisors and public cloud service providers.

For orchestration, Palo Alto Networks offers an XML management API that enables external cloud orchestration software to connect over an encrypted SSL link to manage and configure next-generation firewalls. The exhaustive and fully documented REST-based API allows configuration parameters to be viewed, set and modified as needed. Turnkey service templating can be defined for cloud orchestration software so that the security features within the next-generation firewall become part of the data center workflow. Palo Alto Networks Panorama™ network security management can ensure policies keep pace with the rate of change to your virtualized workloads.

AP **Did You Know?**

Palo Alto Networks Security Operating Platform provides complete visibility and granular control over SaaS applications in your network. Then, among your sanctioned SaaS applications, Palo Alto Networks Aperture SaaS security service provides protection of your data in those SaaS environments, with full visibility across user, folder and file activity to prevent exposure.

Public Cloud: IaaS, PaaS and SaaS

To address the IaaS use case, Palo Alto Networks virtual next-generation firewall is supported by the three most prominent public cloud service providers. Adoption of cloud-delivered services, such as Salesforce® and Office 365®, continues to grow among financial institutions as well. Additionally, applications may make use of object storage, caching and database platforms in the cloud. Securing access to such SaaS and PaaS offerings is accomplished by a combination of the next-generation firewall, Aperture™ SaaS security service and Evident. The NGFW provides inline protection of the cloud workload through application visibility at the network level.

EV Palo Alto Networks Evident provides continuous security of public cloud infrastructure services and one-button compliance reports, enabling you to deploy applications confidently, knowing the cloud is configured to meet your organization's security requirements.

Aperture offers data classification, data leakage protection and threat prevention for data in SaaS environments. Evident monitors public cloud resources and storage services, and generates compliance reporting on cloud security. Both Aperture and Evident utilize APIs from public cloud service providers to obtain visibility into those environments.

Remote Office Locations

Traffic from retail branch offices or campus sites access the corporate data center zone via wide area networks – including software-defined wide area networks – or internet connections. Desktop computers, mobile devices and servers in these locations may be protected by a local NGFW. Different departments at these remote locations may also be segmented from one another to limit exposure in the event of a compromise.

Endpoints – Laptops, PCs and Servers

Whether in the data center or in a remote office, current software levels on endpoints are difficult to maintain due to challenges with patch management. Palo Alto Networks Traps™ advanced endpoint protection, with its multi-method prevention techniques for malware and exploits, can serve as a compensating control as well as a suitable replacement for antivirus.

Traps can protect Windows, macOS® and Linux endpoints to ensure that any exploits on vulnerable systems, regardless of patch status, are immediately thwarted. The Traps agent will automatically prevent attacks with blocking techniques, such as thread injection. When it discovers unknown executable files, the Traps agent will automatically engage WildFire threat analysis to assess potential malicious behavior. Traps can protect physical endpoints as well as virtual desktops and servers.

Traps advanced endpoint protection is designed to identify exploits as they attempt to execute, and to block the execution of malicious code. Traditional antivirus software depends on malware signatures, which may not always be up to date. Rather than running as a separate process scanning for malware, the Traps agent automatically injects itself into individual processes as they execute, and then monitors all application activity for patterns of behavior that are unusual or associated with previously documented exploits. When it identifies such behavior, Traps automatically triggers and blocks the attack.

Palo Alto Networks GlobalProtect™ network security for endpoints can protect remote and/or mobile devices, including PCs and handheld devices. To create logical network segmentation, GlobalProtect uses an IPsec tunnel and enforces security policy within the internal network, where partitioning with a physical NGFW is not feasible.

Centralized Monitoring and Management

Panorama network security management enables you to control your distributed network of next-generation firewalls from a central location via a physical or virtual machine in your private or public cloud. You can view NGFW activity, manage all aspects of device configuration, push global policies, and generate reports on traffic patterns or security incidents, all from a single console. Panorama reduces network complexity with logical, functional device groups, simplifies network management with global policy control, and reduces the time threats linger on your network with actionable data highlighting critical information for response prioritization. Leading automated threat correlation connects the dots between indicators of compromise across your entire network, enabling you to detect advanced threats that would otherwise go unnoticed.

Threat Intelligence, Correlation and Behavioral Analytics

Within your financial services network, Palo Alto Networks AutoFocus™ contextual threat intelligence service provides prioritized, actionable security intelligence on attacks that merit immediate attention. AutoFocus builds on billions of threat artifacts from more than 24,000 WildFire subscribers and applies unique, large-scale statistical analysis, human intelligence from the Palo Alto Networks Unit 42 threat intelligence team, and tagged indicators from your organization as well as a global community of cybersecurity experts. AutoFocus provides full context on attacks, such as the perpetrators, their tactics and any indicators of compromise present on the network. Moreover, AutoFocus can filter security intelligence explicitly for the financial services industry.

Specific industries often face multiple attacks by the same adversary, highlighting the need to share intelligence within the community. Palo Alto Networks cloud-delivered threat intelligence enables rapid sharing of threat signatures so that all parties can benefit from threats discovered across all organizations and within your industry. AutoFocus enables organizations within a given industry to understand what others have already seen on their networks.

GlobalProtect Components

GlobalProtect portal provides management functions for your GlobalProtect infrastructure. Every client system in the GlobalProtect network receives policy and configuration information from the portal.

GlobalProtect gateway provides security enforcement for traffic from GlobalProtect agents/apps based on applications, users, content, device and device state; extends a VPN tunnel to mobile or remote devices with GlobalProtect application; and integrates with WildFire to prevent new malware.

GlobalProtect client software runs on end-user systems and enables access to your network resources via the GlobalProtect portals and gateways you have deployed. The GlobalProtect agent runs on Windows and macOS systems, whereas the GlobalProtect app runs on mobile devices.

You can also integrate public, private and commercial intelligence feeds with MineMeld™ threat intelligence syndication engine, available as an open source tool or as part of AutoFocus. Additionally, MineMeld can automatically create new prevention controls for Palo Alto Networks next-generation firewalls based on aggregated intelligence.

For even greater visibility into malicious activities within your environment, Magnifier™ behavioral analytics profiles user and device behavior and generates alerts on anomalies indicative of attacks. By applying machine learning and cloud-delivered behavioral analytics on rich network, endpoint and cloud data, Magnifier can quickly find and stop targeted attacks, insider abuse and compromised endpoints.

Migration to Palo Alto Networks Security Operating Platform

When you're ready to realize the threat prevention benefits of the Security Operating Platform, the Expedition migration tool makes it easy to migrate from IP/port-based firewall rules in legacy firewalls[4] to application-based rules in Palo Alto Networks next-generation firewalls while minimizing the risks of the change. Beyond converting your firewall rules into a PAN-OS® security policy, Expedition uses machine learning to generate additional security policies based on actual traffic flows and compares your configuration against recommended best practices.

Even with Expedition, a phased approach via documented change control is recommended. Successful deployments typically first involve a like-for-like migration of firewall rules to the Palo Alto Networks next-generation firewalls. After about 15 days, your deployment team will use the Expedition tool to begin the iterative process of defining application-based policies to replace your legacy port-based rules. After the last migration phase, port-based rules are removed, and only the application-based policies remain.

In future phases, your deployment team can work with your institution's different lines of business to restrict access to individual applications based on User-ID™ technology, either via Active Directory® security groups or location-based user IP address ranges.

VI. Conclusion

Financial institutions that implement effective security controls with a network segmentation focus can protect critical operational environments and data against compromise. In an environment characterized by legacy platforms, multiple point products and diverse content sources, the great challenge is to implement new security controls that reduce the attack surface and improve protection without causing disruption and outages. Properly deployed as outlined above, the Security Reference Blueprint for Financial Services IT can improve legacy network efficiency and defeat advanced attacks by positively controlling applications, users and content everywhere across the network, all while enabling even the most demanding business users. Notably, your financial institution can start its journey with the Palo Alto Networks Security Operating Platform at the network perimeter, on endpoints, in the cloud or anywhere in between to complement your existing security investments. Adopting additional elements of the platform will further improve your cybersecurity posture.

For more information, visit us at www.paloaltonetworks.com.

4. The Palo Alto Networks Expedition migration tool is compatible with Juniper, Cisco, Check Point, Fortinet and McAfee configuration files.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

financial-services-it-security-reference-blueprint-wp-072318