Security Reference Blueprint for Financial Services

Information and network security teams at financial institutions must address business demands for digital transformation, tailored customer engagements, and expanded third-party partnerships while adopting new technology, protecting customer data, supporting legacy technologies, and complying with regulations. This entails securely enabling access to personal, financial, and corporate data found in private data centers or the cloud from a variety of locations—including retail bank branches, campus sites, mobile devices, standalone ATMs, and a growing business partner ecosystem—despite the increasing volume and sophistication of threats. The Security Reference Blueprint for Financial Services empowers institutions to protect customer and corporate data, rationalize the scope of compliance, improve cyber resilience, and prepare financial institutions to meet new and emerging information security and technological challenges stemming from digital transformation, cost containment, regulatory obligations, and an increased emphasis on improved customer experience.

Table of Contents

I. Executive Summary

The financial services industry remains a top target for malicious actors—unfortunately, a side effect of digital transformation is increased exposure to cyberthreats as more data is collected and shared with both traditional and new business partners. The Security Reference Blueprint for Financial Services can help institutions more effectively focus on today's evolving cyberattacks, protect customer and corporate data from compromise, better address the expanding scope of compliance, and improve both resilience and availability while meeting technological and competitive challenges. All this can be accomplished with the Palo Alto Networks portfolio of integrated security products, which can also complement existing security capabilities as part of a layered defense approach. Our objective is to help you simplify security for your enterprise, secure your journey to the cloud, and reimagine security operations with best-in-class prevention, detection, automation, and response capabilities.

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 cyberattacks, sitting among the top industries for both security incidents and confirmed data loss.[1] Malicious actors seek to steal funds from accounts, obtain personally identifiable information (PII) for identity theft or credit card fraud, "jackpot" ATMs, disrupt business operations, or destabilize global financial markets to further political or other agendas. At the same time, demand for mobile computing (work-from-anywhere), dependency on more third-party partners (e.g., FinTech, Big Tech), and the journey toward cloud computing can increase business, operational, and reputational risks if not appropriately secured. Combined with customer, partner, and investor expectations for anytime, anywhere frictionless access to their financial information and accounts—on top of the considerable regulatory, business, and technological changes in financial services environments today—all these factors have increased the need for security that can seamlessly evolve in response.

Complex Environments

In addition to a steady stream of cyberattacks, financial institutions face challenges that include:

- **Managing a mix of modern and legacy applications,** including internally developed software (cloud native and on-premises), commercial applications that may be highly customized, and those inherited from past mergers and acquisitions. Aging applications and associated infrastructure have been referred to as "technical debt."
- **Maintaining a multi-vendor philosophy across the technology infrastructure** to address concerns over resilience, vendor management, and diversity.
- **Supporting IT infrastructure for multiple lines of business** across diverse geographies with disparate requirements and varying perspectives. For example, low-latency trading applications have needs distinct from those of consumer banking applications.
- **Sharing data with multiple third parties,** such as service providers, business partners, and even competitors (e.g., for open banking), in support of new business models and customer expectations for enhanced engagements.
- **Adhering to local, regional, national, and industry regulations**, increasing time and effort required for compliance. Some of these explicitly call for a "defense in depth" approach while more consumer data privacy regulations crop up.
- **Operating in cost-optimization mode** due to low or negative interest rate environments and other macroeconomic conditions.
- **Battling for primary ownership of customer relationships** with traditional financial institutions, FinTech, and Big Tech, which may be both competitors and partners.

1. "2021 Data Breach Investigations Report," Verizon, May 2021, https://enterprise.verizon.com/resources/reports/dbir.

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, making them less effective. Some of this security infrastructure sprawl was intentional in "defense in depth"—the notion that if one system misses an attack or instance of malware, another will catch it. As attack sophistication outpaces the capabilities of standalone point products, institutions buy the next "best" security technology to further defend themselves. As institutions adopt public cloud computing, they are also drawn to proprietary security offerings from cloud service providers (CSPs) that are specific to that one environment.

Security tools proliferate over time with each new threat vector or expanding attack surface. Some large financial institutions have accumulated many more than 100 such narrowly focused security tools. All of these must be monitored, managed, and administered by the institution's security operations center (SOC).

III. Security Reference Blueprint for Financial Services

This Security Reference Blueprint for Financial Services describes a transparent, nondisruptive security framework that uses the capabilities of the Palo Alto Networks product portfolio to enhance the security of existing infrastructure. The blueprint incorporates core security principles to effectively and efficiently protect a financial institution whether traffic travels inside or outside its network; whether threats come from the inside or outside, known or unknown; and whether exposure is intentional or accidental. However, to realize this, you must be able to:

- Obtain consistent visibility and granular control across data center, branch, mobile, and cloud environments.
- Segment the network to protect the environment, preventing malware and cybercriminals from moving laterally (i.e., create a Zero Trust network).
- Manage cloud security posture across multi-cloud architectures by continuously monitoring and enforcing governance policies.
- Shift left to secure cloud native applications before deployment with full software lifecycle vulnerability management, infrastructure-as-code (IaC) scanning, and runtime defense.
- Leverage enterprise-scale prevention, detection, and response based on integrated endpoint, network, and cloud data for a holistic view of threats and attacks.
- Implement security orchestration and automation to speed up incident investigations and standardize responses.

The Strata™ network security suite secures your enterprise against tomorrow's threats. Protect users, applications and data anywhere with intelligent network security.

The Prisma® cloud security suite delivers full lifecycle security and full stack protection for hybrid and multi-cloud environments.

The Cortex® security operations suite empowers security operations with AI-powered detection, prevention, and automation.

The elements of the Palo Alto Networks product portfolio detect and prevent threats to financial institutions' networks while reducing complexity and unnecessary overhead. These solutions provide a way to secure these environments and gather intelligence about incursions to mitigate or eliminate damage from future attacks. Native integration and automation among the components of the portfolio work to prevent successful cyberattacks and provide a holistic view of threats across your network, endpoints, and clouds. Furthermore, to alleviate SOC analyst workloads, security orchestration, automation, and response (SOAR) technology provides rapid machine execution with human oversight.

IV. Core Security Principles

Although your unique network requirements will guide your architecture decisions, including appropriate network segmentation, the environment in this example is segmented with a demilitarized zone (DMZ), a number of business-dedicated zones within the data center, campus sites, retail branches, remote employees, public cloud, and an external zone for third-party partners.

Palo Alto Networks Next-Generation Firewalls (NGFWs), in physical or virtual form factors, can scan all traffic entering and leaving different zones to guard against malicious payloads or data leakage. They can also enforce policies that make use of application, user, content, and device identification for better context.

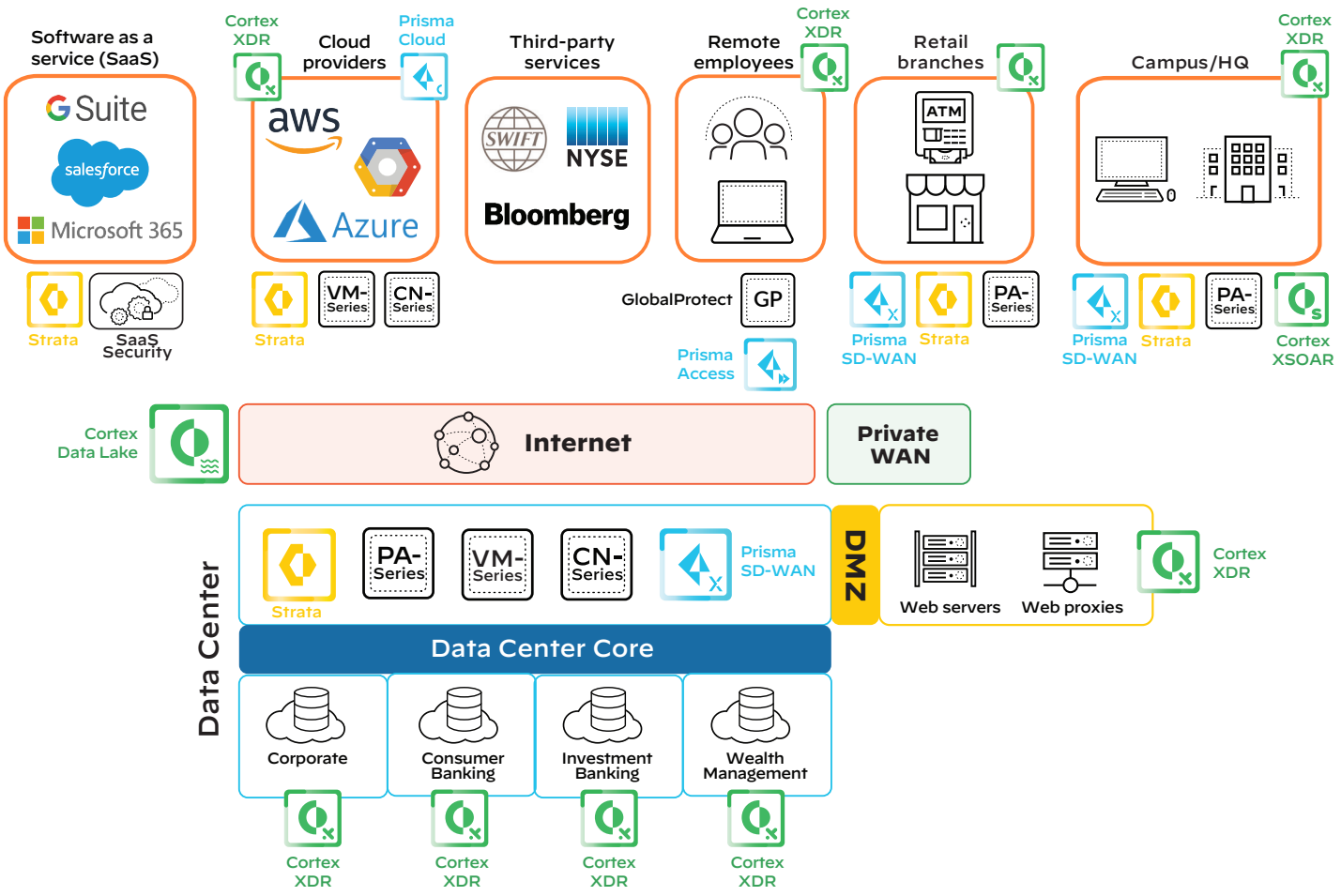

Figure 1: Security Reference Blueprint for Financial Services

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 specific network users or user groups while drastically reducing the volume of threats on the network.

Using a Palo Alto Networks NGFW to characterize applications, financial institutions can immediately reduce their threat exposure. Institutions can choose to block applications that carry the highest risk and even unexpected traffic. By implementing granular application identification instead of just port-based filtering, NGFW administrators can gain greater visibility and more precise control, reducing risk significantly.

Our NGFWs 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 encryption. Though many applications and websites use encryption for privacy, malicious actors are known to deliver encrypted malware payloads. All encrypted network traffic should be examined for the presence of malware, exfiltration attempts, or other inappropriate usage.

Additionally, security services natively integrated with our NGFWs will maximize your security posture with best-in-class prevention mechanisms. Your firewall protections are strengthened with cloud-delivered security services such as Threat Prevention, URL Filtering, WildFire® malware prevention, DNS Security, Enterprise DLP, and IoT Security, instead of requiring you to add disjointed point products to your network infrastructure, which would increase both your environment's complexity and the odds of a gap forming in coverage.

DMZ

Externally visible resources, such as web servers, web proxies, and VPN appliances reside in the DMZ and must be protected from outside threats by an NGFW at the perimeter. NGFWs also control traffic between the DMZ and the internal network, and they can additionally provide first-level URL and content filtering for outbound traffic.

The network perimeter may be designed with a separate NGFW for each external entry point or function. For example, distinct NGFWs may service inbound customer traffic from the internet while others handle outbound employee web-browsing traffic. This approach may be warranted to reduce the fault domain and suit business-specific availability requirements.

Our Next-Generation Firewalls stop cyberattacks while simplifying security. Innovations tightly integrated into the platform replace disconnected point products. This simplifies your security infrastructure and reduces the chances of human error—the leading cause of breaches.

Whether physical or software-based, our PA-Series, VM-Series, and CN-Series NGFWs provide consistent protection for your data center, campus, branch environments, and cloud workloads.

Natively integrated cloud-delivered security services give you the benefits of cloud scale, intelligence gathered from our entire customer base, and the agility to quickly adopt new capabilities.

Network Segmentation and Zero Trust

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

The Zero Trust approach to enterprise network architecture 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 effectively compartmentalizes your user groups, devices, and/or data types, such as PCI DSS and banking-regulated data.

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. Our NGFWs can inspect all traffic entering a zone and allow only known, trusted traffic, which is then also continuously monitored for security vulnerabilities and malicious content.

Zero Trust boundaries enable you to defend each zone from any malicious traffic entering or exiting that zone. Additionally, such segmentation reduces the effort required to demonstrate compliance by limiting reviews to only the zone(s) in which data of interest resides. 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 or financial advisers who access PII and customer financial information.
- Specific organizational or geographic areas that are considered high-risk (e.g., due to pending acquisition, divestiture, or geopolitical conditions).
- Access to third-party business partners, such as market data providers, payment networks, and ATM networks.
- Customer-accessible applications and resources, either via the internet or direct WAN connections.

Although Zero Trust should be the ultimate goal, many financial institutions may have essentially open internal networks and perceive implementation as a significant challenge. However, even taking a few steps toward Zero Trust network segmentation can help better protect critical financial functions and sensitive information, reduce the exposure of vulnerable systems, and prevent movement of malware through their networks. As an example of this, the Society for Worldwide Interbank Financial Telecommunications (SWIFT) mandated the separation of local SWIFT-related infrastructure from the rest of a financial institution's IT environment after a series of successful attacks on its members starting in 2016.

Corporate Data Center

NGFWs also control north-south traffic into and out of the data center zones. Using the Zero Trust model, NGFWs reject all but expected traffic to ensure only authorized applications, users, or content can traverse the network. Network segmentation of data center resources by lines of business may be appropriate to limit data exposure in the event of a compromise. Another option is to segment data center resources based on function, such as development, test, or production. The key is to identify the critical data and protect access accordingly.

Virtualized portions of the data center can also benefit from the protection of NGFWs. VM-Series Virtual NGFWs augment your security posture with the same deep visibility and precise control as a physical NGFW, but in a virtual form factor, making it automatable, scalable, and easily deployed across your private cloud. VM-Series firewalls integrate security provisioning directly into your DevOps workflows and CI/CD pipeline, ensuring effective security and simplified compliance without slowing down your business, even in the most dynamic environments.

For private cloud environments with Kubernetes®, CN-Series Container NGFWs may be deployed on each cluster node to obtain visibility into container traffic and to enforce advanced security services too. This protection can be enforced on allowed traffic traversing namespace boundaries—whether outbound, inbound, or east-west—between pods, and even between containerized applications and legacy workloads, such as virtual machines (VMs) and custom hypervisor servers.

Prisma Cloud is a comprehensive Cloud Native Security Platform (CNSP) with the industry's broadest security and compliance coverage—for applications, data, and the entire cloud native technology stack—throughout the development lifecycle and across both hybrid and multi-cloud environments. Prisma Cloud offers an integrated approach that enables SecOps and DevOps teams to stay agile, collaborate effectively, and accelerate cloud native application development and deployment securely.

Public Cloud

Many financial institutions are now well into their cloud journeys, partly fueled by their digital transformation efforts. In line with their multi-vendor philosophy, financial institutions are adopting more than one public CSP for diversity and flexibility. Maintaining consistent security policies across multi-cloud environments will be key. Supported by the most prominent CSPs—Google Cloud, Amazon Web Services, and Microsoft Azure, among others—VM-Series firewalls can provide inline protection for cloud workloads through application visibility and control at the network level. CN-Series Container NGFWs provide visibility and control over CSP-hosted Kubernetes environments, protecting traffic to and from pods.

For even more peace of mind, continuous monitoring of public cloud workloads allows institutions to deploy applications with confidence that security is enabled as part of their CI/CD pipeline. Moreover, financial institutions can achieve continuous compliance by analyzing the configurations of all cloud services and account settings against organization- or industry-defined controls. Prisma Cloud is a comprehensive CNSP that delivers full lifecycle security and full stack protection for hybrid and multi-cloud environments.

Another element of public cloud is the growth in use of both sanctioned and unsanctioned software as a service (SaaS) applications (e.g., Microsoft 365™, Salesforce®, Box) among financial institutions. It's critical to protect any sensitive data that is uploaded, created, or shared against loss, theft, or data leakage from SaaS. Additionally, cloud-based threats have increased in both volume and sophistication, and they pose a real risk for SaaS applications. Traditional security for SaaS relies on manual signature-based approaches to discover new SaaS applications, delaying visibility and control. Palo Alto Networks SaaS Security is the first integrated cloud access security broker (CASB) that keeps pace with the SaaS explosion. Natively integrated with Palo Alto Networks NGFWs (cloud-based, virtual, and hardware form factors), it delivers proactive visibility, best-in-class protection, and the fastest time to value for all SaaS applications, along with simple deployment and low total cost of ownership (TCO).

Remote Office Locations

Traffic from retail branch offices or campus sites reach the corporate data center zone via wide area networks and/or internet connections. With initiatives such as software-defined wide area networking (SD-WAN) and growing dependence upon SaaS applications, it can be difficult for organizations to provide secure connectivity and maintain an optimal end user experience.

Prisma SD-WAN Instant-On Network (ION) appliances can be used as edge devices with security built in, making it easy to deploy both networking and security with a single branch device. Direct

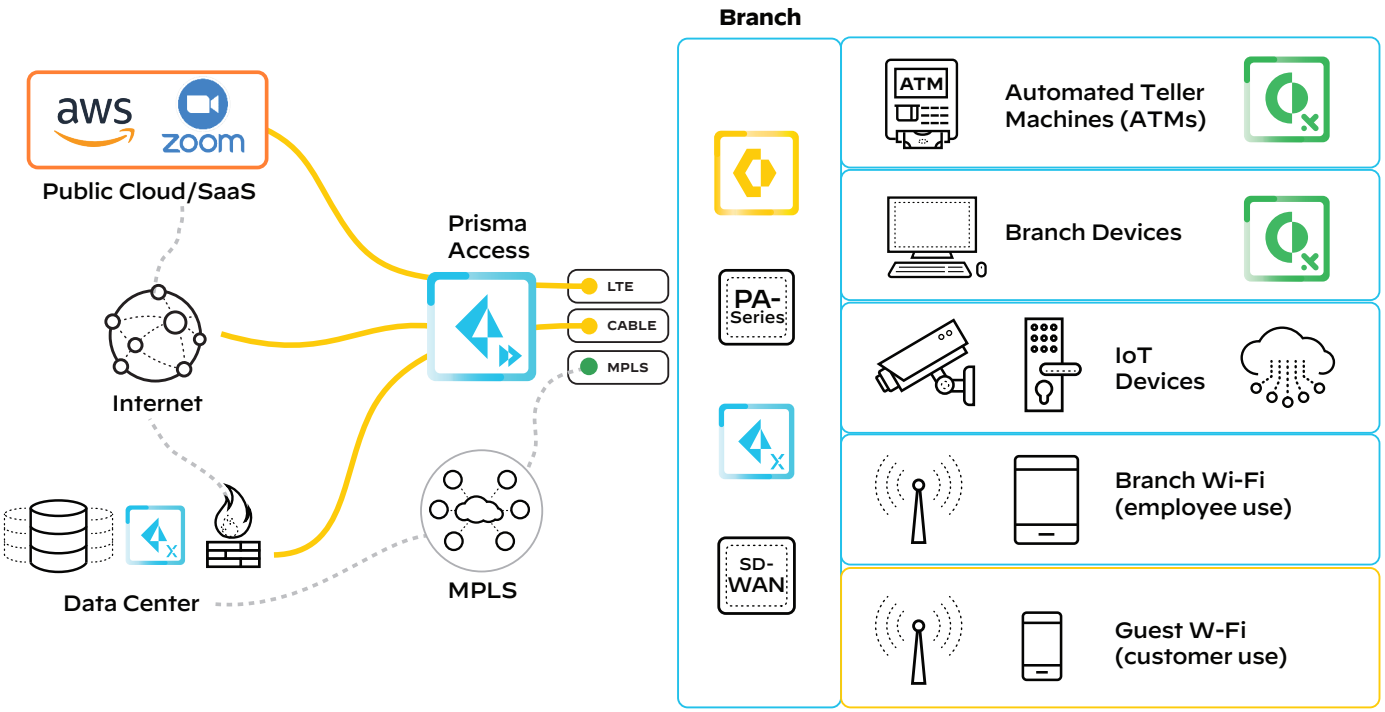

Figure 2: Branch network and security options

internet access, with security controls, is supported to minimize latency for SaaS applications and web browsing from the remote office. Alternatively, NGFWs at the branch can provide full networking and security capabilities for the local internet perimeter. Furthermore, they can serve as segmentation gateways between different departments or business functions at the remote sites as part of a Zero Trust strategy.

Prisma Access is a secure access service edge (SASE) that provides network connectivity and consistent security to branch offices and remote locations, anywhere in the world. It simplifies both networking and security, replacing conventional point products such as firewalls, proxies, secure web gateways, remote access VPNs, CASBs, DNS security, and more. Additionally, Prisma Access may be used as a redundant or even replacement WAN service for traditional multiprotocol label switching (MPLS), but with built-in security capabilities.

Remote Workforce

Large-scale remote work became a necessity during the COVID-19 pandemic, and post-pandemic, many financial institutions will continue to have portions of their workforce regularly working remotely. These employees need consistent security to access data centers and cloud applications. Prisma Access supports this population with Next-Generation Firewall as a service (FWaaS) and cloud-delivered security services. Access to internet- or cloud-based applications is optimized because backhauling to the corporate data center security stack is not required. This results in lower latency and a better user experience for internet- and cloud-based applications while protecting all application traffic, including data center-bound traffic, with best-in-class security. As a SASE solution with both networking and security capabilities, Prisma Access is built upon a massively scalable network with ultra-low latency and backed by industry-leading SLAs to provide a great digital experience for end users.

Endpoints—Laptops, PCs, Servers, and More

One might think that endpoints dedicated for use by business process outsourcing or third-party software developers may warrant greater protection than employee desktop devices. However, attackers are more than happy to compromise any endpoint to establish a beachhead for further malicious activities. Consequently, your strategy should cover all endpoints, including desktops (physical/virtual), laptops, ATMs, servers, and virtual machines.

Protecting this quantity of physical and virtual endpoints takes a toll on the SOC. To offer some relief, Cortex XDR™ transforms and simplifies SOC operations with a holistic platform, including native integration of data spanning all key security sources, incident management, automated root cause analysis, and comprehensive response actions across the entire infrastructure.

For endpoints, the Cortex XDR agent includes multiple layers of protection, including AI-driven local analysis, to stop zero-day and advanced malware, fileless attacks, and exploits. A comprehensive suite of endpoint security modules reduces your attack surface and provides application visibility. Integration with the cloud-based WildFire malware prevention service offers you coordinated and consistent security across your enterprise.

With Cortex XDR, Palo Alto Networks delivers enterprise-wide protection by integrating key security data into one platform for extended detection and response. This category-defining approach speeds response times, eliminates blind spots, and improves security outcomes, giving our financial institutions peace of mind knowing that their data is safe.

Cortex XDR uniquely offers multiple types of machine learning to uncover more threats with an exceptionally low rate of false positives. To accurately detect different attack vectors, Cortex XDR provides:

- **Behavioral analytics that dynamically profile the unique tools, applications, and servers in each customer's environment to identify anomalies indicative of attacks.**
- **AI-based malware prevention to block malware before it can execute, using a local machine learning model powered by millions of diverse file samples and thousands of file attributes.**
- **Cross-customer threat analysis, which enables Cortex XDR researchers to fine-tune protections, identify emerging risks, and drastically reduce false positives.**

Security Operations

SOCs are commonplace in the financial services industry. In some institutions, they are part of a cyber fusion center that may also include physical security, fraud detection, and so on. Wherever they reside, SOC analysts struggle with too many alerts from too many tools, manual processes for incident response, and an ever-evolving threat landscape.

To better equip the SOC for these challenges, Cortex XDR spans key security data sources to stop modern attacks using the following approach:

- Automate investigations by providing a complete picture of every attack and revealing the root cause of alerts from any source.
- Eliminate blind spots by extending visibility across all assets.
- Improve detection accuracy by analyzing multiple attack indicators across data sources.
- Reduce TCO with a holistic approach that eliminates siloed detection and response tools.

This approach reduces the event overload from multiple sources, easing the demand on SOC analysts to react, investigate, and respond via multiple standalone tools and consoles. Cortex XDR offers a holistic view of the environment, shortening investigation times and providing more clarity on the symptoms of a cyberattack.

Furthermore, Cortex XSOAR supercharges SOC efficiency with the industry's first extended security orchestration, automation and response (SOAR) platform. With Cortex XSOAR, security teams can take actions on threat intelligence, standardize processes, and automate repeatable tasks to efficiently manage incidents across their security product stack and reduce response times. Cortex XSOAR integrates with more than 450 third-party products to provide playbook-driven responses that span teams, products, and use cases. This response automation is tightly integrated with fully customizable case management, enabling teams to retain control over incidents while improving response times and analyst productivity.

An accurate asset inventory of all public-facing assets is foundational to SOC processes. Maintaining this is challenging due to a sprawling estate scattered across multiple internet service providers and/or CSPs, and with workloads instantiated on demand by assorted business units or subsidiaries, with or without the awareness of IT. Cortex Xpanse™ fills this gap by providing a single source of truth for all public-facing assets (internet- and cloud-based). This becomes the SOC's authoritative system of record for internet assets with thorough network coverage and complete attack surface management.

Ultimately, a more efficient and more knowledgeable SOC can better defend your financial institution against cyberthreats and minimize business disruptions caused by security incidents. This becomes even more critical as financial regulators around the globe continue to focus on operational resilience.

V. Conclusion

Breaches and data loss have serious consequences for financial institutions. An integrated approach to securing sensitive data and critical applications across the enterprise is key to reducing risk, achieving compliance, and appropriate governance. Financial institutions that implement effective security controls with Zero Trust policies and the Palo Alto Networks portfolio can effectively protect their environments, maintaining confidentiality, integrity, and availability while advancing their business goals.

Our three-pillar strategy—with Strata, Prisma, and Cortex—offers threat intelligence, automation, analytics, machine learning, and AI to provide comprehensive coverage across the enterprise, cloud, and your future environments. The key objectives are to:

- Leverage integrated best-in-class capabilities for the greatest visibility, control, and efficiency.
- Respond quickly and at scale to reduce security operations tasks and eliminate threats.
- Free your teams up to operate and innovate both rapidly and safely.

This approach, as outlined in this reference blueprint, enables financial institutions to deliver responsive security solutions that enable and protect their business by staying ahead of threats instead of merely reacting to them.

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

paloalto NETWORKS

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