Summary:
From mobile to cloud computing, financial services organizations must rely more than ever on innovative technologies to remain competitive. This is more a question of long-term profitability and business success than immediate operational priorities.

How do you balance the need to accelerate the deployment and adoption of new technologies with the mandate for better, more comprehensive security?

How do you move every aspect of your business online with the confidence that you will be able to block today’s high volume of constantly evolving cyber threats and APTs?

Visibility, control, less complexity, automation, and next-generation products are the foundation of a sound cybersecurity strategy.
Take unnecessary complexities (and costs) out of security

Over the years, complexity has quietly invaded security. Additional layers were brought in to patch security products turned obsolete as Internet innovations exploded and bypassed traditional security approaches. As a result, one weak point in many enterprises’ defense today is the myriad of point products that do not always integrate with each other, are costly to maintain, and create silos of data.

Palo Alto Networks® eliminates some of the complexities involved with point products — firewall, IPS, IDS, URL filtering, and more. We provide visibility at all layers, and into every step of an advanced attack with a single inline security appliance augmented with cloud intelligence. This innovative architecture can be operated at a fraction of the cost to deploy and manage an equivalent set of point products.

- Our security platform natively brings together all key network security functions, including advanced threat protection, firewall, IDS/IPS, and URL filtering.
- Because of our deep expertise, commitment to innovation and game-changing security platform, thousands of customers have chosen us and we are the fastest growing security company in the market.

APTs: evolve towards proactive prevention

For financial institutions, the stakes are high; many have already allocated significant resources to protect their assets. But attackers have also learned to use more evasive tactics. An effective response to today’s advanced attacks must move beyond protective measures to add preventive strategies and early detection.

Our threat prevention is built on our platform’s unique ability to inspect all traffic on all ports, regardless of evasion tactics. Armed with significantly improved contextual intelligence about traffic and threats, your security teams can easily see beyond individual incidents and recognize the interconnection between applications, exploits, malware, URLs, DNS queries, and anomalous network behaviors.

Use an automated closed-loop approach for unknown threat protection

Detecting a previously unknown threat is always the first step, but the real value of the Palo Alto Networks platform lies in automatically protecting your users and network with a closed-loop approach: the intelligence about newly discovered threats by Wildfire™, our cloud based sandbox threat analysis is immediately shared and distributed to our next-generation firewalls deployed in your network as points of enforcement.

- Protection and signatures for newly discovered malware (Zero Day threats) are distributed automatically to all our customers worldwide in as little as 15 minutes.
- Our customers say it best: “Everything has become a lot easier. With the old firewall, it took us days to unearth information. Now it’s simply a click on a button. I’m now more in control. The IPS capabilities are doing a great job for us.”

— Head of ICT Exploitation Department, Crédit Agricole Consumer Finance
Put security first, not last, when moving your datacenters to a cloud-based model
Datacenter teams in financial services always need to strive for better economy of scale and maximize the use of available computing power across applications, geographies, and initiatives. Virtualization and cloud computing initiatives are key but benefits can remain elusive if security gets in the way.

Palo Alto Networks provides a security architecture that protects, scales, and evolves as you move your datacenters to a private or public cloud and need to support physical, virtual, and mixed-mode environments. We eliminate the unacceptable compromises you previously faced between security and performance so that you can safely enable business-critical applications and support ever-increasing volumes of traffic.

Secure a new generation of mobile initiatives
A thorough approach to security for mobile devices must include three steps: manage the device, control the communications, and protect the data. Covering these three steps, our platform, including a component on the device, allows you to apply consistent security rules across your enterprise all the way to the mobile devices used by your employees.

Network segmentation: do it right to ensure it remains effective
Network segmentation is an uncontested best practice used to protect highly regulated data. But how can you ensure tight segmentation when controls are applied at such a low level of the stack (port or IP address) that they can be easily bypassed?

Use our unique approach to classify and control network traffic based on applications, users, and content. With higher-level classification, you can use business-relevant attributes to codify the policies that control who has access to what. This reduces the scope of many compliance audits.

“Seeing how well the firewall performed in our production environment, and the ease with which we were able to set up and run our policies on our network in just one day, really sold our team on Palo Alto Networks... We are keenly aware of the sensitivity of the data running on our network every day. We need a solution that ensures our clients’ assets are protected while at the same time ensuring high performance access to applications that help our business run efficiently.”

—Chief information security officer for Raymond James Financial

To learn more, visit www.paloaltonetworks.com and download the full version of this white paper.