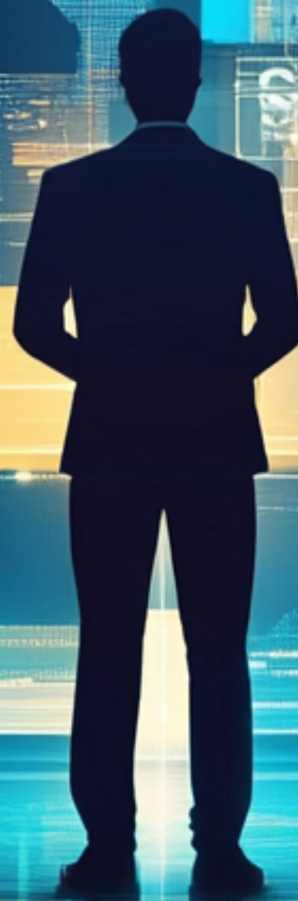


WHITE PAPER

Banking on Security

The Broadcom® Blueprint
for Financial Services



Banking on Security

The Broadcom® Blueprint for Financial Services

TABLE OF CONTENTS

Executive Summary

The Financial Services Landscape

Key Challenges Facing FSI Organizations

Resilience Against Advanced Cyber Threats

Safeguarding Cloud Environments

API Protection for Secure Data Exchanges

Meeting Regulatory Mandates

Conclusion

Executive Summary

As financial institutions embrace digital transformation, they face a new era of cyber threats and regulatory complexity. The Broadcom® comprehensive security suite equips these organizations to navigate the challenges—securing APIs, identities, endpoints, and data—while enabling compliance and operational continuity.

The Financial Services Landscape

Technology has always been a driving force behind growth and innovation in the financial services and insurance (FSI) sector. As pioneers in digital transformation, FSI organizations have reshaped business models and service delivery, fueling the evolution of the digital economy. However, the modernization of IT environments, while essential for innovation and revenue, also increases the attack surface and heightens both security and compliance risks.

Key Challenges Facing FSI Organizations

- **Advanced Cyber Threats:** Financial institutions are targeted by increasingly sophisticated attacks, including AI-driven malware, deepfake fraud, and highly targeted social engineering and phishing schemes. Ransomware, often employing double-extortion tactics, now threatens payment systems, core banking, and treasury operations.
- **Cloud Vulnerabilities:** The shift to cloud and digital services expands the attack surface, exposing organizations to risks such as insecure cloud access and API weaknesses including broken authentication, token exposure, and input validation flaws. Securing hybrid multicloud environments while meeting data residency and cloud-provider risk management standards is a persistent challenge.
- **Secure Data Exchanges:** Financial institutions increasingly rely on APIs to power data exchanges in digital banking, payments, and open banking initiatives, but this API-driven architecture introduces significant security risks. Exposed APIs can become entry points for attackers, leading to financial losses, regulatory penalties, and reputational damage if compromised.
- **Compliance Complexity and Regulatory Change:** Rapidly evolving regulations across jurisdictions require strict data protection, breach notification, resilience testing, and oversight of third-party vendors. Achieving isolation, encryption, multi-factor authentication, and maintaining transparency for audits and board reviews is essential—even for the most advanced security programs.

BROADCOM CRITICAL SECURITY TECHNOLOGIES ARE DESIGNED TO DIRECTLY ADDRESS THE CHALLENGES FACING FSI ORGANIZATIONS

This white paper explores how Broadcom critical security technologies are designed to directly address these challenges.

Resilience Against Advanced Cyber Threats

Today's cyberattackers employ AI, domain spoofing, and obfuscation techniques to hide malicious links, making threats like spear phishing, ransomware, and business email compromise both widespread and difficult to detect. Financial institutions face several key challenges:

- Sophisticated social engineering tactics
- Evasive malware and zero-day exploits
- Increased use of compromised accounts
- Complex attack chains designed to bypass legacy security solutions

Defending Against Email-Based Attacks

Symantec® Email Security.cloud (ESS) is an advanced platform that **strengthens native email defenses** and reduces false positives. ESS utilizes real-time link analysis, cloud sandboxing, click-time protection, isolation, and global threat intelligence to deliver comprehensive protection against email-borne threats.

Defending Against Ransomware

Symantec Privileged Access Management (PAM) enforces granular, host-based controls at the server kernel level—even against root-level attacks. This approach **neutralizes many ransomware vectors** and enables rapid incident response.

Defending Against Compromised Accounts

Broadcom Identity and Access Management (IAM) provides advanced authentication for users, devices, and software, ensuring strong credential protection. Its cloud-native, DevOps-friendly architecture adapts quickly to changing requirements and delivers modern identity fabrics for diverse enterprise needs.

Examples include:

- **A Fortune 100 financial organization that enhanced security and customer confidence while meeting compliance**
- **A European wealth management organization enabling modern consumer applications through cloud-native authentication**

Safeguarding Cloud Environments

As organizations transition to hybrid and private cloud environments, securing these ecosystems—and the APIs that connect them—becomes critical. The Broadcom acquisition of VMware enables comprehensive, end-to-end security across private clouds:

- **Endpoint Protection:** Symantec Endpoint Protection integrates with VMware vShield Endpoint to deliver agentless antivirus and malware defense for virtual machines, minimizing resource overhead and automating remediation.
- **Workload Protection:** Carbon Black® Workload, integrated with VMware vSphere®, provides advanced prevention, detection, and response for ransomware and fileless threats, supported by continuous hygiene monitoring and behavioral analytics.
- **API and Identity Security:** Layer7™ API Gateway secures VMware Cloud Foundation® (VCF) APIs with robust authentication and policy controls. Symantec Identity Security Platform and Symantec PAM offer scalable authentication and privileged access protection for cloud applications and management consoles.

APIs ARE THE BACKBONE OF MODERN FINANCIAL INFRASTRUCTURE

- **Data Protection:** Symantec DLP, CASB, and Zero Trust Network Access (ZTNA) enforce data encryption and classification, monitor user and device behavior, and provide coordinated, policy-driven control over sensitive data in motion, at rest, and in use.

Security is intrinsically built into the private cloud, providing robust protection, streamlined operations, and a resilient foundation for ongoing digital transformation.

API Protection for Secure Data Exchanges

APIs are the backbone of modern financial infrastructure, enabling everything from mobile banking and payment processing to open banking platforms and third-party fintech integrations. As financial institutions strive to deliver seamless digital experiences and comply with mandates like PSD2 and global open banking initiatives, APIs have become essential connectors between traditional systems and innovative services. However, this API-centric approach introduces significant security risks, as these interfaces often oversee extremely sensitive financial data. A compromised API can lead to substantial financial losses, regulatory penalties, and lasting reputational damage.

To address these risks, the financial-grade API (FAPI) framework sets the benchmark for securing high-risk financial transactions and data exchanges. The FAPI Advanced security profile further strengthens protection by employing defense-in-depth strategies that anticipate potential breaches of individual security layers.

The Broadcom Layer7 API Security solution empowers organizations to secure their APIs in alignment with these standards. Layer7 serves as a control plane, managing authentication and authorization, defending against OWASP API security top ten vulnerabilities, supporting advanced security profiles, enforcing policies, and enabling fine-grained authorization based on identity attributes, device posture, and operational context. It also provides rate limiting and quota management to prevent API abuse and denial-of-service attacks. Additionally, Symantec PGP® Command Line integrates seamlessly with commercial and custom data transfer systems, offering versatile encryption options to ensure secure data transmissions regardless of recipient capabilities.

Meeting Regulatory Mandates

FSI organizations face increasingly sophisticated threats, including expanding digital attack surfaces, heightened third-party risks, and demanding compliance obligations. Key regulations shaping the industry include the General Data Protection Regulation (GDPR), New York State Department of Financial Services (NYDFS), Payment Card Industry Data Security Standard (PCI DSS), Payment Services Directive 2 (PSD2), California Consumer Privacy Act (CCPA), and the Digital Operations Resilience Act (DORA), along with additional mandates addressing incident reporting, privacy, and operational resilience.

Table 1. Key Regulatory Mandates Impacting Financial Services.

Regulation	Region/Scope	Impact
GDPR	EU/Global	Data privacy, breach notification, cross-border data controls
NYDFS	US (NY, model for other states)	Cybersecurity program, risk assessment
PCI DSS	Global	Payment data, encryption, access controls
PSD2	EU	Opens banking systems via secure APIs, MFA
CCPA	US (California)	Privacy, breach notification, consumer rights
DORA	EU	Operational resilience, incident reporting, resilience testing

BROADCOM SECURITY PRODUCTS MEET INDUSTRY COMPLIANCE MANDATES

THE BROADCOM UNIFIED
APPROACH SIMPLIFIES
SECURITY MANAGEMENT

Here is how Broadcom solutions are mapped to security and compliance:

Table 2. Broadcom Security Product Alignment to Compliance Mandates

Product	Key Features	GDPR	NYDFS	PCI DSS	PSD2	CCPA	DORA
Identity and Access Management	Multi-factor authentication, central role-based management, audit-ready controls	✓	✓	✓	✓	✓	✓
Layer7 API Security	Defense against OWASP API security top 10 vulnerabilities	✓	✓	✓	✓	✓	✓
Symantec Control Compliance Suite	Security compliance assessments for over 100 regulations, mandates, and best practice frameworks	✓	✓	✓	✓	✓	
Symantec Email Security	Sandboxing, phishing/BEC protection, DLP	✓	✓	✓	✓	✓	
Symantec IT Management Suite	Endpoint lifecycle and patch management, device compliance, rapid threat response		✓	✓			✓
Symantec PGP Encryption	AES-256/PGP data-at-rest/in-transit encryption, policy-driven controls, detailed logs	✓	✓	✓	✓	✓	

By integrating these solutions, financial services organizations can more effectively manage identities and access, secure data across every channel, defend against endpoint threats, and stay ahead of evolving regulatory requirements. This comprehensive approach helps institutions mitigate both cyber risks and compliance risks, ensuring greater resilience and operational confidence.

Conclusion

Partnering with Broadcom empowers financial services organizations to confidently navigate today's complex cybersecurity and compliance landscape. The Broadcom integrated portfolio delivers advanced protection for identities, endpoints, data, and APIs, while streamlining regulatory adherence and operational resilience. With solutions that address sophisticated threats, cloud vulnerabilities, and evolving mandates, institutions can safeguard critical assets and maintain trust with customers and stakeholders.

The Broadcom unified approach simplifies security management, reduces risk, and supports seamless digital transformation. By embedding robust security into every layer of the financial ecosystem, including private and hybrid cloud environments, Broadcom enables organizations to focus on innovation and growth, confident in the strength of their defenses and the reliability of their compliance posture.