TRANSFORM SECURITY

Meet Changing Needs Across a Dynamic Threat Landscape

OVERVIEW

Greater focus on strategic risk is prudent for financial services organizations seeking to expand digital services in the face of increasing cybersecurity threats. VMware transforms security and streamlines governance, risk, and compliance (GRC) by providing a ubiquitous software layer across application infrastructure and endpoints.

BENEFITS

- A holistic approach to IT security
- Secure Application infrastructure
- Identity and endpoint security for BYOD and COPE mobility
- Streamlined governance, risk management, and compliance

Addressing Enterprise Risk Management Requirements

Risk management is the third highest priority for banks, according to a recent CIO Agenda report. While the top two priorities—mobile and online banking—increase share of wallet, risk management is purely a defensive requirement, yet one that banks cannot afford to neglect.

High-growth digital business creates new risks for banks. A recent mobility study, the *VMware State of the Digital Workspace Report*, revealed that the financial services industry leads in successfully executed initiatives—from enabling mission-critical apps for use in a mobile model to upgrading infrastructure to support mobile.[1] While advancing digital agendas, 77 percent of financial services CEOs believe that digital business is bringing new types and levels of risk—particularly cloud. More than two-thirds of CEOs see their risk management disciplines falling behind despite current levels of security investment.

Cloud, mobile, social, big data, and the Internet of Things (IoT) are exciting innovations with the potential to transform how customers, particularly millennials, engage with financial institutions. For banks to embrace IoT in an impactful way, security must be built in from the start, and at every level across the entire IoT ecosystem – from the device through to the network and cloud level. The more devices and points of entry there are on a network, the more opportunities there are for cybercriminals to sneak in.

There is no doubt that financial services organizations want to be "all in" on digital services to stay competitive, but ensuring customers that their personal information is protected is growing increasing difficult.

The Growing Costs of Threats and Compliance

Traditionally, the financial services industry has been considered a model for best security practices. However, that leadership is eroding because financial gain is increasingly the motive for data breaches. The top two enterprise risks for banks are cyberattacks on critical infrastructure and regulatory scrutiny.

- More than half of (55 percent) financial services firms recently reported ransomware as the top attack threat, followed by phishing (50 percent), which previously held the top spot.[2]
- Almost a third (32 percent) of financial firms say they've lost anywhere from $100,000 to a half-million dollars due to ransomware attacks.[3]
- In 2015, the total burden of regulatory compliance costs from construction, healthcare, and financial and insurance industries, in the U.S. exceeded 10 percent of GDP, looking at data from the Bureau of Economic Analysis.[4]

[1] VMware. "The VMware State of the Digital Workspace Report 2016."

[2] SANS Institute. "From the Trenches: SANS 2016 Survey on Security and Risk in the Financial Sector," October 2016.

[3] Ibid

[4] The Blaze, "U.S. Businesses Spend More on Regulatory Compliance than Russia's GDP," November 14, 2016.

A catastrophic hack as well as repetitious non-compliance not only affect an individual bank, but also the stability of national and global markets in the digitally interconnected world. Even endpoints running the most up-to-date software, email filters, and other security layers can be attacked: all it takes is for a user to fall for a phishing email or to open a malicious attachment. Legacy models of securing the network only at the perimeter are inadequate for today's data centers. Once malware has managed to make it inside a data center, it can move easily from workload to workload.

Beyond breaches, ensuring regulatory and industry compliance is also a significant challenge for financial firms, given the sensitivity of their information and transactions. In the U.S., financial organizations must ensure data protection and auditing under FINRA regulations, Gramm-Leach-Bliley (GLB) and Sarbanes-Oxley (SOX) Acts. Transaction processing must also be PCI-compliant.

VMware Solutions for Financial Services Transform Security

VMware is transforming security with a unique approach that addresses today's dynamic threat landscape. VMware delivers a ubiquitous software layer across infrastructure and endpoints, independent of the underlying physical infrastructure or location. The platform provides visibility and context of interaction between users and apps, and enables the insertion of additional third-party security services for intelligent protection.

Secure Application Infrastructure

VMware is the leading provider of virtualization technology to financial services organizations. Virtualization helps IT secure application infrastructure by abstracting underlying infrastructure from applications running on top of it—whether workloads are running on-premises or in the public cloud. Virtualization enables full visibility into the data path, providing an ideal narrow pathway to compartmentalize applications through micro-segmentation of the network.

Micro-segmentation provides banks with fine-grained security controls that prevent the lateral spread of threats. Virtual firewalls around workloads or network segments enable banks to build a secure environment within the data center, limiting hosts from accessing assets they never need to access, reducing the threat landscape, and mitigating risk. VMware NSX® delivers host-based security and micro-segmentation that supports unit-level trust and flexible security policies down (and including) the network interface.

AL-MAWARID Bank deployed NSX to improve security, accelerate product innovation with IT automation, and meet stringent regulatory compliance requirements. NSX's unique micro-segmentation capabilities provide advanced security inside the company's data center network. Distributed firewalling and automated security policies boost data protection and support compliance with the rigorous regulatory framework of the Lebanese banking sector, as well as international laws such as the Foreign Account Tax Compliance Act (FATCA). With NSX, the bank deploys security controls across its network for a fraction of the cost that would have been required using a hardware-centric approach. NSX also improves application continuity capabilities as the virtualized data center network spans to the bank's active-passive disaster recovery site, and provides IT with the freedom to securely move data and apps across the bank's private cloud. AL-MAWARID Bank also anticipates accelerated provisioning of IT services enabled by NSX will enable the bank to bring product and service innovations to market faster.

Identity and Endpoint Security for Mobility

As banks seek to fully empower workforces with bring-your-own device (BYOD) and corporate-owned, personally-enabled (COPE) device initiatives as well as engage customers in more personalized experiences, standardizing security across every endpoint becomes critical.

The Digital Workspace, powered by VMware Workspace ONE™, unifies identity, app, and device management to reduce complexity by providing secure single sign-on (SSO) access to any application (native, web, remote, virtual) running on-premises or in the cloud—all in a single dashboard. An adaptive, conditional layer of security at each transactional level—from users to the resources they're accessing—improves bank data security and reduces the cyberattack surface without impacting users' consumer-like experiences.

VMware endpoint management solutions, including VMware AirWatch® enterprise mobility management, help ensure secure access to all resources—from smartphones, tablets, and laptops to wearables, vending machines, and IoT devices—across global networks, as well as detect and remediate threats. Personalized and dynamically configured policies together with simplified end-user profile management across any virtual, physical, or cloud-based environment help speed secure desktop and app delivery.

Scotiabank, a Canadian-based international bank with 85,000 employees globally and operations in 55 countries, is using a single instance of AirWatch in the cloud to manage mobile devices (both corporate owned and BYO) and iPads in bank branches globally, according to Andrew Bell, senior enterprise infrastructure services consultant. He says, "AirWatch servers are 'rock solid' and the bank hasn't had a single security breach under AirWatch management."

Streamlined Governance, Risk, and Compliance

VMware's ubiquitous software layer provides a holistic solution for governance, risk, and compliance (GRC), improving the speed, efficiency, and agility of business while streamlining regulatory processes. VMware's GRC platform standardizes automation and seamlessly integrates the implementation of regulatory controls. Through layering, the compliance platform secures and validates additional, dynamically inserted security tools and services—from VMware technology partners—to further streamline GRC processes.

A leading provider of online financial trading services, London Capital Group wanted to adopt a digital-first approach to enable international growth and rapidly launch new products and services. By investing in VMware NSX, it has replaced its traditional IT infrastructure with a reliable, agile, and secure virtual network on which to launch a state-of-the-art trading platform for its customers. Enabling micro-segmentation through NSX and adding security beyond the data centre perimeter, at an individual level within every server and virtual machine ensures customer data remains secure and compliant. As Blair Wright, CIO of London Capital Group explains "NSX has been fundamental to creating an infrastructure with security built into its very core".

Learn More about VMware Transformative Security Solutions for Financial Services

Digital technologies provide scalable, flexible, and convenience capabilities that open possibilities for financial services organizations. Only VMware, with a transformational approach to security, provides a ubiquitous software layer across application infrastructure and endpoints that enables enterprise financial services IT and risk management teams to rebalance resources for greater impact.

Visit http://www.vmware.com/solutions/industry/financial-services.html.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com