CYLANCE

# Financial Services

Solution Brief

- The financial services market is a favorite target for cybercriminals
- While security spending in financial services has increased dramatically, the number of compromised records continues to increase rapidly (Verizon Data Breach Incident Report, 2017)
- Organizations in the financial services market are attacked 65% more than the average across all other industries (IBM X-Force Threat Intelligence Index, 2017)
- Large banks had 13.3 million records lost or stolen in 2016, versus 1.1 million records in 2015 (2016 Gemalto Breach Level Index)

Banks are where the money is, and that is why their assets, records, and customer data are so heavily targeted by cybercriminals. 24% of financial services organizations reported a breach in 2017 (2017 Thales Data Threat Report – Financial Services Edition). This is why the financial services industry now spends 28.4% of their IT budget on information security, and 81.8% of IT professionals in financial services expect their overall IT security budget to increase (2016 Cyberthreat Defense Report, CyberEdge Group).

## Regulatory Requirements in Financial Services

The financial services industry is subject to regulatory requirements that are designed to help protect customer data and reduce both the number and severity of cyberattacks and data breaches. These regulations include U.S. federal regulations such as the Gramm-Leach-Bliley Act (GBLA) of 1999 and Payment Card Industry Data Security Standard (PCI-DSS). In addition to U.S. federal regulations, many financial services organizations are also subject the New York Department of Financial Services (NYDFS) Cybersecurity Requirements (23 NYCRR Part 500), as well as the European Union's General Data Protection Regulation (GDPR).

For financial services institutions that fail to meet these requirements, penalties include government sanctions, which can be monetary and non-monetary in nature. While managing compliance risk can limit or eliminate the likelihood of government sanctions, it is not the same as managing breach risk, which can result in civil liability, damage to customer trust, and negative press coverage that can damage shareholder value.

## Understanding the Threat To Financial Services

Endpoints represent one of the greatest areas of concern for those in the financial services industry. The growing use of mobile devices and the ubiquity of web-based banking, both in retail and commercial banking, has accelerated this trend. In fact, web-based banking applications are currently the greatest attack vector cybercriminals utilize against the financial services industry (Verizon Data Breach Incident Report, 2017). This is why 64% of global financial institutions see endpoint security as the most important security segment for future spending (2017 Thales Data Threat Report – Financial Services Edition).

Today, penetrating most mobile endpoints is not significantly difficult. Protection of these devices when they are mobile is often limited to traditional endpoint protection suites, generally consisting of antivirus programs and possibly a personal firewall on the device, which zero-day threats can easily defeat. This problem is also not limited to organizational assets – in an increasing number of cases, home PCs of bank executives and employees are being targeted by cybercriminals. A recent survey showed that in 100% of studied breaches, compromised endpoints were running an antivirus program. Furthermore, 95% of these breaches bypassed company firewalls, and 77% bypassed email filtering (Barkly, Ransomware Survey, November 2016; https://blog.barkly.com/ransomware-attacks-bypassing-antivirus#0).

## About Cylance®

Cylance uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security. Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and other attack vectors. With AI based malware prevention, application and script control, memory protection, device policy enforcement, root cause analysis, threat hunting, automated threat detection and response, coupled with expert security services, Cylance can protect endpoints without increasing staff workload or costs.

## The Cylance Approach

Cylance has proven effective against such cyberattacks and data breaches. This is due to the architecture of the solution. Historically, security providers relied on signatures developed from a historical view of malware. AV-TEST reports new malware exceeding 120 million variants in 2017, rendering signatures based on historical views obsolete. Cylance takes a different approach. At the core of Cylance's malware prevention capabilities is a machine learning approach that harnesses the power of algorithmic science and artificial intelligence. It analyzes and classifies hundreds of thousands of characteristics per file in real time, breaking them down to an atomic level to discern whether a file is safe to run.

Cylance doesn't employ this technology at the expense of simplicity, ease of use, or burden on the endpoint or administrator. CylancePROTECT®, CylanceOPTICS™, and Cylance Smart Antivirus™ utilize a small agent that integrates with existing software management systems or Cylance's own cloud console. The endpoint detects and prevents threats using tested mathematical models on the host, independent of a cloud or signatures. It is capable of preventing threats before they execute in both open and isolated networks without the need for continual signature updates or cloud connections. Cylance's approach stops the execution of threats, including ransomware, regardless of having prior knowledge or employing an unknown obfuscation technique.

## Conclusion

The financial services industry has historically been one of the most attractive verticals for cybercriminals. The combination of this threat and the strict regulatory framework that financial services institutions are subject to means that these organizations are under significant pressure to deploy effective solutions to challenging endpoint security issues. Cylance has responded to this demand with its effective, lightweight, and easy-to-use security products and specialized security services. Cylance's AI based algorithm resides in a miniature model on the endpoint and is updated only semi-annually, requiring no daily deep scans that bog down endpoint and network performance. By leveraging artificial intelligence and machine learning to predict attacks, seeking first to prevent attacks rather than respond, and offering scalable threat detection and response for root cause analysis and threat hunting, Cylance provides outstanding protection to financial organizations around the globe.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618

CYLANCE