# Going Beyond Regulatory Compliance

## Protecting Your Company, Your Shareholders, and Your Customers

CYLANCE

"*The financial services industry is a significant target of cybersecurity threats…given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted.*" **— The New York Department of Financial Services**

## Introduction

The financial services industry has always been a very attractive target for cybercriminals. The rationale that drove Willie Sutton to rob banks, "because that is where the money is", also drives cybercriminals to target the financial services sector. In addition to targeting the capital of financial services institutions, either directly or through fraud, cybercriminals also target bank records and the personal data of customers. The following statistics illustrate the extent to which cybercriminals target the financial services industry:

- Financial services organizations were attacked 65% more than the average organization across all industies[1]
- 24% of financial services organizations reported a breach in 2017[2]
- While large banks have reduced the number of incidents by 22.5% from 2015 to 2016, the number of lost or stolen records in the same period increased by 1,070% from 1.1 million to 13.3 million[3]
- The financial services industry now spends 28.4% of their IT budget on information security[4]
- 81.8% of IT professionals in financial services expect their overall IT security budget to increase[4]

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[5].

Clearly, capital loss is one of the potential negative outcomes of cybercrime and fraud. Beyond capital loss, however, are the damage to financial services institutions from the loss of customer confidence, as well as potential civil and regulatory liabilities should the financial services institution be found to be negligent in its practices.

## Financial Services Industry Regulatory Frameworks

The financial services industry is subject to regulatory requirements that are designed to help protect customer data. For financial services organizations in the United States, 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 upcoming European Union (EU) General Data Protection Regulation (GDPR). For all of these regulatory frameworks, the requirements are meant to act as minimums that organizations are expected to meet. Failure to do so can result in government sanctions, which can be both monetary and non-monetary in nature.

The NYDFS Cybersecurity Requirements go a step further in their approach[6]. Rather than stating minimums that financial services organizations must meet, the NYDFS Cybersecurity Requirements call for processes and process

improvement processes that are designed to keep financial services organizations ahead of the game. This includes the requirement to conduct periodic vulnerability assessments to identify weak spots in current security tools, methods, approaches, and policies. Organizations are then expected to benchmark their approaches and policies against industry best practices. In theory, this should ensure that organizations learn from each other, allowing security practices to evolve as threats evolve.

## Compliance Risk Management vs. Breach Risk Management

One point which should be obvious, but often isn't, is that managing compliance is like teaching to the test in secondary school. A student has a higher likelihood of passing the test, but it doesn't mean that the student will do well in the real world. Managing compliance risk without managing the underlying risk that compliance is supposed to address has the same dangers – regulatory compliance will reduce exposure to government sanctions in the case of a breach, but it does not necessarily reduce the risk of a breach or the damage to customer trust and civil liability that inevitably follows a breach. This results in a form of cognitive dissonance where financial services organizations may be measured in a way that favors compliance management over true information risk management. True information risk management recognizes an accountability or a duty of care when it comes to managing information security of customer data. Financial institutions are data stewards and must go beyond just checking the box when it comes to compliance regimes.

## Defense-in-Depth As a Compliance Risk Management Strategy

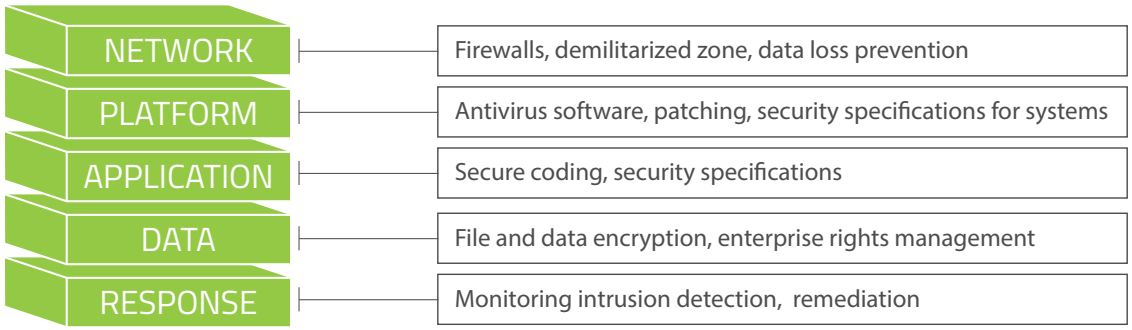
A good example of a compliance risk management strategy for organizational cybersecurity is the concept of defense-in-depth. Defense-in-depth utilizes multiple tools and processes to protect an organization's data assets and IT infrastructure. The concept is that for a cybercriminal or threat to penetrate the defenses from the outside, they need to defeat each of the successive security layers. Each layer theoretically utilizes a different technology to do its job, so in theory, it should be extremely difficult for any threat to overcome all the different layers and technologies to complete its attack. But, the reality is, many of the layers are based on the same design philosophy of detecting known bad files through the use of signatures or heuristics.

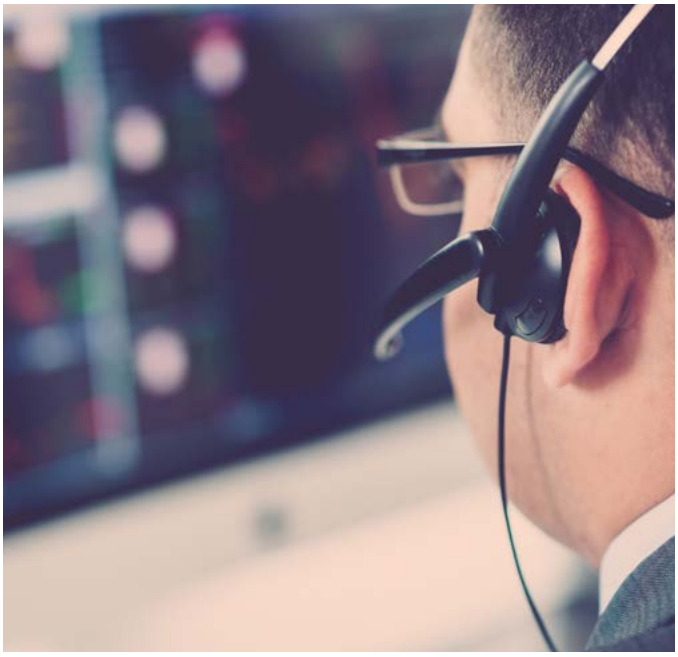
Defense-in-depth works well as a compliance risk management strategy for several reasons:

- It is an industry best practice, especially when combined with vulnerability assessments, which are also required by the NYDFS
- It includes components for intrusion detection, response management, data encryption, application security, endpoint security, and external firewalls
- Major security vendors can provide integrated packages that address many or most of the components that defense-in-depth needs

This makes defense-in-depth relatively attractive to implement because it is providing most, or all, of the infrastructure components required to address compliance risk.

DEFENSE-IN-DEPTH



## Modern Cybercrime Threats and the Weaknesses of Defense-in-Depth

Endpoints represent one of the greatest areas of concern for those in the financial services industry. This is why 64% of global financial institutions see endpoint security as the most important security segment for future spending[2]. With the increased use of mobile devices, such as laptops, tablets, and BYOB devices, the potential for compromise is increased. If malware or a cybercriminal can access these devices when they are outside of the trust zone, the amount of protection the device has is largely limited to its antivirus program. When the compromised device is brought back inside of the protected zone, the cybercriminal can utilize it to launch more attacks to further their objectives.

Today, penetrating most mobile endpoints is not significantly difficult. Protection of these devices when they are mobile is often limited to classical endpoint protection suites, generally consisting of antivirus programs and possibly a personal firewall on the device, which modern malware such as zero-day threats can easily defeat[7]. 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[8]. Financial services organizations understand the danger of this threat. Globally, 64% of financial institutions see endpoint security as the most important security segment for future spending[4].

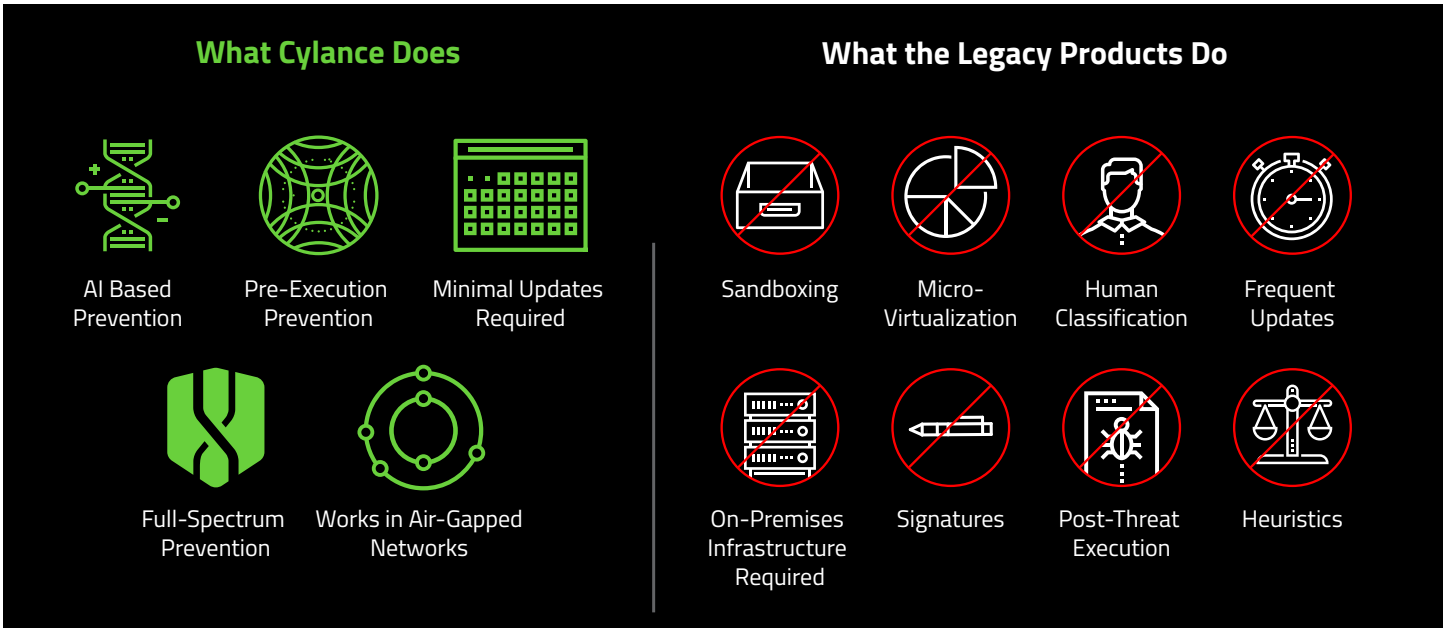
## Using AI and ML To Reduce the Risk of Breaches from Cyberthreats

If endpoints are the most vulnerable components in a financial services organization's infrastructure, what can be done to reduce the likelihood of damaging breaches, while still managing compliance risk? Approaches such as sandboxing and heuristics have the danger of actually executing unknown files and seeing what happens, after which they attempt to put the genie back in the bottle if the files turn out to be malware. Other approaches, such as isolating files until they can be validated, often through a cloud-based system, negatively impact users and businesses by slowing business processes that are dependent upon the exchange of information. And, all of these approaches still struggle to keep up with the rapid evolution of malware and cyberattack methods, which saw an increase in the number of software vulnerabilities by 34.6% from 2014 to 2015[9].

One tactic that has showed real results in the battle between malware, cybercriminals, and anti-malware is artificial intelligence (AI) and machine learning (ML). Research by the Enterprise Strategy Group has shown that 29% of organizations want to utilize AI based cybersecurity technology to accelerate incident detection, and 27% want to use it to accelerate incident response[10]. AI and ML approach malware detection differently than other solutions. By analyzing millions of good (clean) and bad (malware) files, hyperlinks, scripts, and other threat vectors, AI and ML based anti-malware solutions develop a profile of threat vectors. This allows the anti-malware software to recognize threats even if they were not part of the learning sample, such as zero-day threats, even if the program has not been updated.

## CylancePROTECT®, CylanceOPTICS™, and Microsoft® Defender Firewall: A New Best Practice for Cybersecurity

Cylance redefines what security products can and should achieve for the financial services market by leveraging artificial intelligence to detect and prevent malware from executing on organization endpoints in real time. By approaching security with machine learning techniques and offering scalable threat detection, root cause analysis, and threat hunting, Cylance helps prevent data breaches that impact customer trust.




CylancePROTECT is an alternative to traditional signature-based antivirus programs. It is the only technology that prevents nearly all advanced threats and malware before it executes and causes harm. It eliminates the need for traditional antivirus software, anti-exploit products, whitelisting solutions, and host-based intrusion detection and prevention systems. Unlike reactionary signature, heuristics, behavior monitoring, and sandboxing, which require an Internet connection and constant updates, CylancePROTECT applies artificial intelligence to analyze a file's characteristics and predict whether it is safe or a threat prior to execution.

CylanceOPTICS utilizes data gathered from CylancePROTECT instances already installed on organization endpoints to gather threat data, which is then sent to a local database for storage. This allows organizations to react faster and more efficiently to attacks as they start, and to emerging threats that escape detection by standard signature-based antivirus programs. When CylancePROTECT and CylanceOPTICS are combined with the firewall capability of Microsoft Defender, the result is an endpoint protection, detection, and reporting solution that is highly effective against all forms of malware and cyberattacks.

## Use Case: Investment Bank

A $40 billion multi-national investment bank with 3,000 endpoints had a dedicated security team, as well as McAfee® and FireEye® endpoint protection products in place to detect and stop any executed threats. However, the organization had no way of knowing if their systems had already been compromised by threats that were lying dormant, or had been implanted before the detection products were in place. Moreover, their threat detection solution required significant amounts of manual review to weed out false positives.

The organization contacted Cylance to perform a compromise assessment across their assets. The Cylance Consulting team found undetected malware had been implanted on company systems three years earlier. The Cylance team also found that a contractor brought in to do penetration testing had actually left tools and open vulnerabilities on the organization's systems.

After addressing these issues, the organization deployed CylancePROTECT on their endpoints to contain potentially unwanted programs and prevent the execution of malware. After the installation of CylancePROTECT, the time required for the security response team of three people to weed out false positives went from nine hours a day (27 hours total) to one and one-half total hours.

## Summary: Managing To Compliance Standards Does Not Equal Information Risk Management

The Financial Services sector has long been a target of cybercriminals and malware attacks for the simple reason that "it is where the money is". As a result, various government agencies have created regulatory requirements and frameworks to help ensure that the financial services industry has the right tools in place to be resilient to these threats. However, simply managing compliance risk and organizational liability doesn't necessarily lower the risk to organizations and customers – organizations can still be breached, creating exposure to civil liability and damaging customer trust. With CylancePROTECT, CylanceOPTICS, and Microsoft Defender, financial organizations can effectively counter these threats while still meeting government regulatory requirements.

## 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.

## References


1. IBM X-Force Threat Intelligence Index, April 2017
2. 2017 Thales Data Threat Report – Financial Services Editin (p 4)
3. 2016 Breach Level Index, Page 10, Gemalto (2017)
4. 2017 Cyberthreat Defense Report, CyberEdge Group
5. Verizon 2017 Data Breach Investigations Report, Table 1: Confirmed Breaches (2016)
6. New York State Department of Financial Services, "23 NYCRR 500", March 2017
7. Slate, "You Can't Depend on Antivirus Software Anymore", Feb 16, 2017
8. InfoSecurity Magazine, "Antivirus Fails to Stop Ransomware 100% of the Time", Nov 6, 2016
9. National Cybersecurity and Communications Integration Center, "Malware Trends", Oct 2016
10. John Oltsik (Principal Analyst, Enterprise Strategy Group, "Artificial intelligence and cybersecurity: The real deal", CSO (Jan 25, 2018)



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


CYLANCE




20180613 - 0560