Addressing Insider Threats, Cyber Attacks & Data Security

One of the most complex challenges faced by banks is a data breach. While costly in monetary terms, the higher cost of a data breach can be a reduction in customer confidence. Once customers question the safety of their information or feel their bank is putting them at risk of fraud, they are less likely to use that institution for their financial services needs. Some may even leave the bank altogether.

And even though banks are meeting FDIC and FFIEC regulations for security, malware attacks and data breaches are still occurring. Unfortunately, bank IT leaders and executives are often left with a false sense of comfort by maintaining compliance with guidelines set forth by regulators. Banks may be meeting regulations, but are still not meeting customers' security expectations. This can leave banks feeling helpless to stop these cyberthreats, but fortunately, there are new technologies that can solve this challenge.

Securing Every Endpoint

A bank has many endpoints. An endpoint is an infrastructure access point, be it an employee laptop, a datacenter server, an ATM machine, or even a teller workstation. Malicious actors can use any of these endpoints to unleash malware. Applications that can scrape debit and credit card numbers can be covertly uploaded to ATM machines and executives clicking a phishing link on their laptop can give hackers access to a bank's entire network.

Whether the person accessing an endpoint is a vicious hacker, an unsuspecting customer, or an employee with good or bad intentions, the result can be the same – a data breach.

Banks need a way to guard every endpoint against attacks like these. This is not a job that can be handled manually by IT staffers, no matter how skilled or dedicated, or by traditional antivirus solutions, no matter how "advanced". This is a job for artificial intelligence and machine learning.

A Silent Agent

By deploying a technologically advanced monitoring agent on every endpoint that can identify and quarantine many different types of malware, regardless of whether the malware is well known or brand new, banks can ensure their infrastructure is safe from over 99% of potential threats. This is not traditional antivirus software, but an actual endpoint protection agent compiled using artificial intelligence and machine learning techniques that review thousands of characteristics of hundreds of millions of files to learn what constitutes a good file and a bad file, so bad files can be quarantined before they execute.

It is important for banks to know that breaches are not inevitable and technology that can successfully hold back cyberattackers already exists. While cyberattacks will continue to grow ever more sophisticated, this technology stays one step ahead.

The Cylance Advantage

Cylance's next-generation endpoint protection solution, CylancePROTECT, is PCI Section5 and Microsoft antivirus certified. This means we help banks meet compliance requirements, but unlike other solutions, we actually prevent over 99% of malware before it executes. Banks gain an amazing advantage because our product works whether or not security best practices are met, and regardless of whether an attack is the result of a direct, targeted threat, or an employee accidentally clicking on something they shouldn't have. Cylance can provide a safety net, protecting against advanced persistent threats and zero-day malware. With our agent monitoring your endpoints, IT resources are freed up to concentrate on any other problems that may arise. Plus, since our solution meets the requirement for antivirus, it fits into existing budget lines when less effective solutions are removed.

Cylance used this technology to secure the infrastructure of a $40 billion multi-national private equity company, which also provides investment banking, alternative asset management and financial services. Our team has deep experience with financial institutions like yours and is ready to help. Wouldn't you like to learn how our technology can help secure your bank?

Jon Miller
Vice President
Strategy

CYLANCE

Contact Info

www.cylance.com
877-973-3336

Jon Miller is Vice President of Strategy for Cylance, a maker of next-generation antivirus software and provider of breach incident response and other professional services. Miller leads Cylance through insight and direction around technology, partnerships, research and market opportunities. Miller was previously a vice president with Accuvant, where he built and led threat research and customer engagement services. Prior to that he spent five years on the X-Force professional services team of Internet Security Systems. Miller is a well-known hacking expert who gave his first public talk at Def Con at age 20. Jon has delivered dozens of public talks at security and technology conferences including Black Hat, Def Con, IEEE and Toorcon. Miller has been featured in publications including Forbes, Huffington Post and Rolling Stone, and has appeared on "60 Minutes" and Fox News.