CUSTOMER STORY

Regional Bank Creates Security Strategy for Mergers and Acquisitions

FireEye Offerings Identify and Mitigate Vulnerabilities

FACTS AT A GLANCE

INDUSTRY

Finance

SOLUTIONS AND SERVICES

- FireEye Endpoint Security
- Mandiant Red Team Assessment
- Mandiant Purple Team Assessment
- Mandiant Incident Response Retainer

BENEFITS

- Security recommendations contextualized with operational and business considerations
- Security vulnerabilities identified and mitigated with cyber hygiene assessments
- Customizable evaluations tailor analysis and recommendations to critical controls and procedures
- Fully optimized funding through flexibility of FireEye retainer
- Ability to adapt to latest threats with security solutions informed by frontline intelligence

CUSTOMER PROFILE

The bank is a subsidiary of one of the oldest and largest financial institutions in the United States. The organization provides a variety of retail and commercial banking services to large corporations, midsize companies, small businesses, and individuals. The bank operates in multiple states and has total assets in excess of $150 billion.

Preserving the confidentiality of clients and their personally identifiable information (PII) is a banking imperative. In this case, the institution's manager of information technology affirmed, "We have to protect our customers." From reputational damage to the loss of business, the consequences of a breach could be catastrophic. The impact of a security compromise is further magnified because of the organization's role as a steward of PII in a highly regulated industry.

To protect the sensitive data of its clients, the bank must combat the growing trend of cyber criminals targeting any institution—large or small—with an exploitable vulnerability alongside the growing variety and voracity of attacker tactics, techniques, and procedures (TTPs). "We have to assume that we are a target. As a bank, we need to be prepared to cover the gamut of cyber attacks, from opportunistic threats to nation state actors," described the manager.

The bank continuously invests in reinforcing its security posture to make it less vulnerable to cyber attacks. The bank's cyber defense team consists of 48 individuals whose responsibilities include management of the security operations center, incident response, vulnerability management, threat intelligence and content engineering.

The cyber defense team safeguards a sizable number of laptops, including the devices of back-office employees such as IT and security staff, who often work remotely. Though preparing for a transition to the cloud, the team also protects their current infrastructure, which is primarily Windows at the desktop level and different distributions of UNIX and Linux in the server space.

The bank also is undergoing a series of mergers and acquisitions (M&As), further expanding and their cyber environment. The IT manager explained, "Part of the M&A process is doing our due diligence to evaluate the security rigor of new entities, and to design and implement transition plans for secure integration of technology stacks and infrastructures."

Proactive Preparedness

The IT team partnered with FireEye to incorporate industry-leading cyber security technology and an array of services from FireEye Mandiant into its security stance. The IT manager noted, "FireEye Mandiant analysts are top notch. They have a very high caliber of expertise and a real-world understanding of cyber security. As practitioners,

> "The real-world experience FireEye incorporates into its security technologies creates a critical feedback loop between the latest TTPs of attackers and the capabilities instilled in FireEye solutions. Threats are constantly changing, but FireEye stays at the forefront of cyber security technology."
>
> — **Manager of Information Technology,** Regional Bank

they understand the potential operational impact of a proposed improvement and the business implications to consider when implementing a new control. That quality of guidance is very important to us."

To protect all the devices connected to the bank's network, the defense team used an on-premise deployment of FireEye Endpoint Security with both an internal and DMZ controller. "Having visibility into machines that are off network is great because it gives us more protection against threats directed at our remote workforce. Even if these employees aren't using our VPN, we can monitor their devices and if suspicious activity is detected, contain the machine before it infects our network," reported the IT professional.

The security group collaborates with a Mandiant red team to conduct cyber security effectiveness assessments of new acquisitions and regular evaluations of the bank's security posture. By emulating an attack scenario using TTPs seen on real, recent incident response engagements, Mandiant analysts determine how easily a malicious actor can obtain an organization's critical data and test the internal security teams' ability to detect and prevent threats.

The IT manager detailed, "We work with the companies we're acquiring to deploy FireEye Endpoint Security licenses in their infrastructure and send the intelligence feeds to a cloud controller. This way, the Mandiant team can complete assessments from the cloud without connecting back to our internal controllers and exposing our infrastructure to hidden threats or risks."

The bank's defense team can define evaluation goals that allow the assessment to focus on validating specific controls and procedures. The security team designs these evaluations to analyze defenses from a technology, detection and response, user awareness and reporting perspective to ensure critical security vulnerabilities are identified and risk mitigation strategies are implemented.

"We've used a Mandiant Red Team Assessment for several projects, including one to determine if an advanced threat actor could breach our most rigorous defenses and another to test our team with a random USB memory stick drop. We were pleasantly surprised that a high number of the deliberately infected sticks were reported and turned in by employees; a nice validation of our staff's cyber security preparedness," shared the IT manager.

A No-Waste Approach to Incident Response Retainers

The bank also has a FireEye Mandiant Incident Response Retainer (IRR) to ensure the bank can coordinate immediate support from Mandiant experts in the event of a suspected breach. In addition to obtaining access to world-renowned security analysts, hours contracted through the IRR also can be applied towards Mandiant consulting services such as penetration testing, strategic program assessments or malware analysis training.

The manager enthused, "If we contact the IRR hotline to aid with an attack, we're guaranteed triage support from a Mandiant incident responder within four hours. In our view, it's an insurance policy with the best incident response company in the world. Plus, there's the added value of being able to reallocate unused funds in the contract for other services."

The bank has used this flexible funding on services such as red team assessments and to pilot FireEye Mandiant Purple Team Assessment, a technical service that gathers quantifiable evidence of a security program's effectiveness and teaches teams how to improve processes at each phase of the attack lifecycle.

The IT manager added, "The assessments have helped us validate controls, identify gaps in defenses and architect improvements to our security. We've also used the excess retainer hours for a variety of education programs. Mandiant experts come on site to train up to 20 people at a time. It's a great way to upskill our in-house talent and prepare our team with the latest intelligence and techniques."

Built for the Forefront of Security

In full disclosure, the IT manager shared that his first exposure to FireEye was in a former role as a Mandiant consultant, before the company merged with FireEye. The manager was conducting a proof of concept on FireEye Email Security and recalled being "blown away" by the FireEye approach to cyber security. He stated, "If not the first, FireEye was one of the earliest innovators of sandbox technology and continues to be at the cutting edge of cyber security."

The combination of best-in-class technology with intelligence and expertise from the frontlines of the world's most impactful cyber attacks enables FireEye to continuously adapt its methodology for stopping attackers. The IT manager concluded, "The real-world experience FireEye incorporates into its security technologies creates a critical feedback loop between the latest TTPs of attackers and the capabilities instilled in FireEye solutions. Threats are constantly changing, but FireEye stays at the forefront of cyber security technology."

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd., Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™