

Digital Defense Helps Large Banking Organization Enhance Their Information Security Posture

Financial Industry Security Challenges

Today, security has become more complex for the financial industry with the progression of technology and moving to the cloud. Identity and data theft are still on the rise, and data compliance regulations are still trailing behind the quickly moving threat landscape. The banking and financial services industry are heavily regulated, and those mandates are ever evolving. Waiting for a regulation to go into place to drive security innovation and fully secure the business is no longer an option if a financial institution wants to retain its customers' trust, as well as gain a competitive edge.

Supply and demand isn't just something that affects tangible goods and services, it also affects the job market. The threat landscape moves at lightning speed, and keeping up with it is next to impossible if you don't have the right strategy, people, processes, and cutting-edge technology in place. Organizations are finding it hard to achieve their security goals with the supply of highly qualified security experts being low and the demand astronomically high.

Financial institutions rely on third-party vendors to help them accomplish particular security goals, such as protecting websites or operational software. Our client's Information Security Officer (ISO) shared, "Relying on third-party service providers is becoming more and more of a necessity. While this takes the responsibility somewhat off of the institution, it still requires intensive due diligence and risk management of these providers. No one wants to be a Target or Home Depot."

Compliance mandates can't keep ahead of the threats, and security leaders struggle with what to do in the meantime.

Information Security Market History

It's hard to imagine now, but the first online banking was launched in the early 1980s (around 38 years ago!) with the best of intentions to provide a more convenient way for customers to bank with the growing adoption of the public Internet. Since then, financial institutions have had to slowly but surely set up security processes to decrease their risk of unauthorized access to a customer's data. We've all learned the hard way that was (and still is) easier said than done.

In 2012, breaches were at an all-time high and continuing to climb. Organizations were scrambling to try to stay ahead of breaches by putting information security best practices in place, but it proved very difficult with the threats evolving faster than they could keep up. Companies across all industries were relying heavily on compliance mandates when building up their security posture, as opposed to leveraging a true cybersecurity framework. Organizations needed security best practices in place and frameworks to guide them then, and they still need direction to try to stay ahead of threats now. Compliance mandates couldn't keep ahead of the threats and security leaders struggled with what to do in the meantime.

Our Client's Security Challenges

The Information Security Officer (ISO) at a large bank in Northern California with nearly 90 branches, serving a variety of commercial businesses, construction companies and the farming community, needed to spin up a more robust data security posture quickly to keep up with the current threats and adhere to compliance mandates such as the Payment Card Industry Data Security Standard (PCI DSS), the Federal Financial Institutions Examination Council (FFIEC), and the Gramm-Leach-Bliley Act of 1999 (GLBA). This bank, with assets of 5 billion dollars, has been around in some form since 1884. It is safe to say they have seen their fair share of industry changes and customer needs over the past 130+ years in business.

Our client shared with us that:

“As a financial institution, we possess massive amounts of sensitive data that has the potential to be exploited if we didn’t put the right safeguards in place. We knew our customers deserved the best banking experience and data protection, and we wanted them to know they could continue to trust we would make securing their data a top priority. That is when I came on board with my organization and partnered with Digital Defense to build up our security posture strength and resiliency.”

The ISO had a big job ahead of him, but he knew if he could build a solid security framework based on best practices he would be successful in protecting his company’s sensitive data, while strengthening their brand loyalty. He knew he had to stay ahead of the curve and that was not a job for just one person or even just one technology.

Digital Defense Solution

According to the bank’s ISO, “Initially, I needed to get the lay-of-the-land and find out where we were susceptible to an attack so we could prioritize what technology to invest in upgrading or

replacing first. Knowing our vulnerabilities and managing them to protect our infrastructure from being hacked was key to building an innovative, cutting edge foundation our customers deserved.

This was 10 years ago so we needed the best product for the best value and price starting out. The more success I was able to prove, the more budget I was able to get to continue to implement new security solutions. It was evident at that time we would need to constantly innovate to try to stay ahead of new threats, and of course that still rings true today.”

As this financial institution was selecting a vendor, they had a set of criteria. They wanted:

- A partner and someone proven and trusted in the industry already.
- Solid tech but also great service because this was going to be a marathon, not a sprint, to ensure everything was the best of the best within their budget.
- Clear, automated reporting that could be easily presented at a detailed or high level to the board and C-levels in order to explain their security story’s bottom-line.
- A managed service to cover all the bases while they grew the team.
- Solid technology that was dependable, reliable, constantly innovating and cutting-edge, as chasing down false positives would slow them down from reaching their security goals.
- Robust, user-friendly technology that wasn’t just a scanner but actually part of the bigger vulnerability management picture
- A personal touch with advisory partnerships so they could have guidance as they constructed the security program.
- A one-stop-shop for vulnerability management, penetration testing and social engineering to identify risks.
- Time to value. In the beginning, there wasn’t a big budget and they needed to crawl before they could run. The ISO needed a solution that could help create benchmarking, establish KPIs for success, and show overall value quickly.

“What’s great is that 10 years later, I’m still pleased with the decision to go with Digital Defense.”

Our customer chose several Digital Defense security solutions to help them in their journey to stellar security.



Frontline Pro™ Vulnerability Scanning – As a Managed Security Service, Frontline Pro provides the same industry leading vulnerability scanning solution subscription as Frontline Advanced Vulnerability Scanner, but adds a Personal Security Analyst (PSA) to help lift the burden of vulnerability management.



Social Engineering – Frontline Social Test™ creates conditions and scenarios that lure personnel into engagement – just as if driven by a crafty cyber attacker. Techniques can include phishing calls, targeted emails, and more. Findings are used to educate employees on how to become more astute at discerning legitimate human engagement from trickery.



Internal and External Penetration (Pen) Testing – Performed by trained and certified security analysts, our ethical hackers utilize proven penetration testing methodology and industry best practices to get into the mind of a malicious hacker to find weaknesses the way they do. Our Pen Tests provide clarity around which vulnerabilities are truly exploitable, and which ones could lead to critical data compromise.

Results

This 5 billion dollar bank found that Digital Defense met all their criteria! Their ISO shared with us, “What is great is that 10 years later, I’m still pleased with the decision to go with Digital Defense. The relationships I have with the people in their organization are strong, and their solutions and guidance help me stay successful in my role by protecting our organization’s

customers. Digital Defense helps me measure my overall risk and where I should focus remediation efforts, with the benefit from clear, easy-to-understand reports.

I’ve worked with other vulnerability management vendors in the past, but Digital Defense has remained tried and true.

They have continued to meet our evolving criteria and know my company’s needs well to help us see what is coming on the threat horizon. Digital Defense aids me in continuing to strengthen my security posture. Not to mention, **the proof is there when I have to attest compliance to examiners. Their solution is superior to others I’ve used and they continue to commit to making it better by adding new technology integrations such as ForeScout, as well as creating innovative features like Security GPA.**



Solution Spotlight

Frontline Pro™

Frontline Pro combines our Frontline Advanced Scanning Service with your own Personal Security Analyst (PSA). Frontline Pro PSAs perform the work of running your scans, analyzing the results, generating reports, and providing direct remediation planning guidance for you, as opposed to your security team doing everything themselves. It’s the ultimate outsource for all size organizations and is especially valuable for organizations that have limited security management time or expertise on staff.

Frontline VM yields the industry’s lowest false positive rate – critical to effective vulnerability discovery, productive remediation guidance, and ultimately, true cyber risk reduction. And this solution is not the “throw it over the wall” model seen with many “expert assist” programs. Our PSA will work right alongside you to help define requirements, craft strategy, and effectively execute a vulnerability management program tailored to your organization’s needs.

Our market leading platform's key features include:

- Fully and seamlessly integrated with Frontline RNA™ – the industry's most thorough and accurate vulnerability scanner.
- Advanced filtering of recurring scans to easily identify new risk areas.
- Robust reporting with clear, actionable remediation guidance.
- Frontline Security GPA® – unique, but simple security rating scorecard which reflects each and every improvement – with an appropriate 'relative' score – as vulnerabilities are assessed, and active remediation is performed. Unlike other vulnerability scoring algorithms, Security GPA takes into consideration whether a scanned device is an iPhone, a Domain Controller, etc. – and then rates them accordingly.
- Integrated compliance auditing.
- Patented, endpoint scanning correlation that eliminates "network drift".
- Lightweight, agentless scanning minimizes network and endpoint footprint.
- Industry leading customer support lauded by clients for its responsiveness, expertise, and professionalism. Needs are met from the get go and throughout the life of the relationship.

Enhance Your Security Posture Today

Contact us: Sales@digitaldefense.com

For more information visit: www.DigitalDefense.com

digitaldefense
by HelpSystems

www.digitaldefense.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.