FORTRA™

CASE STUDY (FINANCIAL INSTITUTION-UNITED STATES)

A well-established financial institution leverages Frontline Vulnerability Manager™ and Frontline Security GPA® to manage risk during their digital transformation.

Background

This leading financial institution has been in business for over 75 years, and as of 2020, had assets exceeding $2 billion and over 200,000 members.

Committed to continually improving the customer experience, the financial institution began a three-year digital transformation. It made innovative updates and changes to systems and overall infrastructure that have ultimately helped make business easier and more secure for its members.

The Challenge

The institution launched a digital transformation project to:

- Modernize its digital platform
- Build automation and efficiencies into the Infrastructure team's technology and processes
- Convert the legacy workstation environment to a virtual environment

Cybersecurity was a central consideration throughout the process. The institution needed a security solution to help maintain and improve cybersecurity and compliance during this digital expansion.

Amid the transitional phases of this project, both the old and the new infrastructures would need to remain tightly secured, protecting vital client and company information. The team needed tools and support to ensure new infrastructure was configured securely and that daily changes to infrastructure didn't create new vulnerabilities.

AT-A-GLANCE

Industry Credit Unions & Banking

KEY SOLUTIONS

- Frontline Vulnerability Manager™
- Frontline Security GPA®
- Frontline Virtual RNA™

RESULTS

- **Secure Digital Transformation** with vulnerability management and automated and on-demand scanning.
- **Improved Security & Risk Management** by tracking security posture with Frontline Security GPA.
- **Intelligent Remediation** with the ability to work smarter and faster to prioritize the highest risk vulnerabilities.
- **Security Expertise** from a Digital Defense PSA, providing more time to focus on deploying their new infrastructure, and confidence they were in expert hands.

Digital Defense

Frontline VM

An essential system in the Frontline Cloud vulnerability management and threat assessment platform, Frontline VM uses patented and proprietary scanning technology to survey the security posture of target IP-based systems and networks.

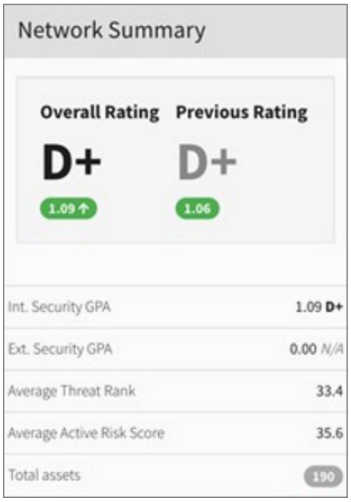
The Solution

The institution was already using Digital Defense's Frontline Vulnerability Manager (Frontline VM™) to perform host discovery and vulnerability scans on external (internet facing) and internal IP-based systems and networks. However, it was not taking advantage of some of Frontline's key features that could help make security efforts easier.

Security GPA

A key feature of Frontline VM, Security GPA, became a more integral part of the processes after the institution's state auditors recommended using Frontline to monitor internal and external risk scores.

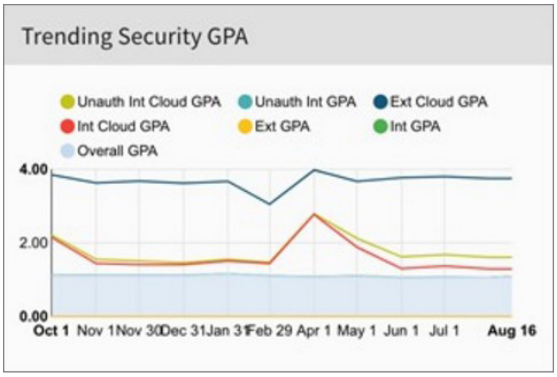
Frontline Security GPA is an intuitive security rating metric provided in a letter (A,B,C,D, F) grade and numerical GPA. The Security GPA weighs asset importance and criticality as well as vulnerability severity to provide a full picture of an organization's security posture. Additionally, Security GPA is dynamically generated and reflects even the smallest changes in vulnerability.



The institution's CTO/CISO began using Security GPA as a motivator and Frontline VM as a key component of the team's vulnerability prioritization. This work earned the institution an award from Digital Defense because their GPA steadily improved and landed in the top 2% of all Frontline users.

Reporting

The institution's oversight committee met monthly to review its business and security landscape. A local statute requires that an oversight committee acknowledges and either accepts or mitigates risk to the institution. The CTO/ CISO used Security GPA as an informative, yet simple metric when presenting to technical and non-technical committee members. These security conversations were greatly simplified by using the easily understood letter and number rating to convey complex security concepts.



Pro Support

The institution had a Frontline Pro subscription, which includes a Digital Defense Personal Security Analyst (PSA). The CTO/ CISO's team worked closely with the Digital Defense PSA who configured the new infrastructure and helped build new scan policies in Frontline for the institution. Pro support gave the project team more time to focus on deploying their new infrastructure, and confidence that their scan policies were in expert hands. Their PSA also helped analyze scan results and provided direct remediation planning guidance. This resulted in a more effective and mature vulnerability management program for the team.

Frontline Virtual RNA

Part of the institution's digital transformation was converting to a virtual infrastructure. Digital Defense helped the institution save a significant amount of time by working with their virtual hosting provider to configure a new Frontline RNA virtual appliance. The virtual Reconnaissance Network Appliance (Frontline vRNA™) is powered by Digital Defense's proprietary scanning technology, which enables:

- Cross-context scanning
- Automatic tracking of dynamic and transient assets
- Highly accurate results, significantly reducing false positives

"Moving to the vRNA made economic sense," the CTO/CISO indicated. "In our network setup, a hardware appliance required colocation and hosting, adding costs that weren't tied to a virtual appliance."

Proactively Monitoring the Changeover

During the transition from the legacy infrastructure to the new cloud-based infrastructure, the CTO/CISO's team managed both simultaneously. They were retiring assets from the legacy system and deploying new assets in the new virtual infrastructure on a daily basis, and used Frontline VM to scan both environments. They ran nightly vulnerability scans on the new environment while still running scans on the old IP address scheme twice a week. This helped ensure daily changes weren't creating new vulnerabilities.

The team relied on their Security GPA to monitor and report on risk after making changes to the new environment. If their GPA decreased, they would compare current, previous, and trending scores, with the ability to drill down into at-risk assets if needed.

> *"We trust Frontline. We were decommissioning and breaking down systems daily, and the Security GPA helped us identify and prioritize any new issues."*
>
> **—CTO/CISO**

Benefits

Defense-in-Depth

The financial institution uses a defense-in-depth approach to securing its critical infrastructure. The CTO/CISO's team built out multiple defensive layers to protect its most important assets and data. Frontline plays an important role in the defense-in-depth model. It is used in the network layer to proactively search for weaknesses across infrastructure and is one of the first lines of defense.

Risk Management using Frontline Security GPA

During this digital transformation project, Security GPA provided many benefits. It served as the guiding metric indicating whether daily system updates introduced new vulnerabilities in both new and old infrastructure. It also helped facilitate stakeholder communication with easily understood metrics and reporting. Lastly, this dynamic metric served as a motivator to the team to improve security posture.

Transition Security Oversight and Monitoring

Because Frontline VM comes with the ability to automate or run unlimited, on-demand scanning, the institution was able to conduct vulnerability assessments multiple times a day to check their daily changes and ensure that no new weaknesses were introduced. During the transition, the team also maintained their legacy infrastructure, leveraging the automated scanning in Frontline for oversight as they retired assets.

According to the CTO/CISO, Frontline was essential to a secure conversion.

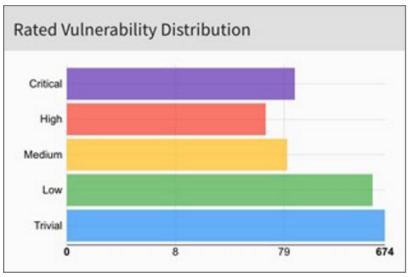
> *"I was in Frontline daily because I wanted to make sure we weren't missing anything that needed to be addressed in the new environment."*
>
> **—CTO/CISO**

Ongoing Workflow Management

The PSA provided by Digital Defense manages end-to-end service delivery, including customized reporting of assessment and remediation efforts. Additionally, the team can view progress through Frontline VM's intuitive online dashboard, Frontline Active View™, and their PSA can respond quickly to any enterprise-wide issues.

Remediation Monitoring

The institution uses a service provider to manage the patching of their new infrastructure. To maintain visibility into the service provider's progress, the CTO/CISO consults scan activity in Frontline VM daily. This level of insight into the vendor's responsibility aligns vulnerability prioritization between both organizations.



Best-in-Class Security Expertise

This institution, as well as all of Digital Defense's clients, benefit from the Vulnerability Research Team (VRT). The VRT proactively analyzes aggregate data to accelerate the discovery of flaws and then analyzes these flaws for the rapid identification of Zero-Day vulnerabilities, further bolstering their security.

Frontline Cloud

The Frontline.Cloud SaaS vulnerability management and threat assessment platform supports Frontline Vulnerability Manager™, Frontline Web Application Scanning™, and Frontline Active Threat Sweep™ that together provide:

- Risk-based vulnerability management
- Asset discovery and tracking
- OS and web application risk assessment
- Machine learning features that leverage threat intelligence
- Agentless & agent-based scanning
- Penetration testing for networks, mobile applications, and web applications
- Compliance management for PCI DSS, HIPAA, FDIC, CUNA, and more.
- One of the world's longest-tenured PCI-Approved Scanning Vendors (ASV)

The Frontline.Cloud platform virtually eliminates false-positives associated with legacy vulnerability management solutions while also automating the tracking of dynamic and transient assets and prioritizing results based on contextualized threats and business criticality. Learn more.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.