CASE STUDY

Illinois State Treasurer's Office Sets an Example for State Agency Cybersecurity

Chief Information Officer (CIO) Joseph Daniels for the Illinois State Treasurer is responsible for protecting an extremely large financial institution against cyber threats. "The Treasurer is the Banker for the state, which has $32 billion in assets," says Daniels. "That is a large amount of financial resources to manage and to secure for our constituents."

The agency's legacy security environment was challenging to maintain. To strengthen security and streamline management, the Illinois State Treasurer rolled out several integrated Fortinet solutions. The user interfaces and single-pane-of-glass visibility of the new infrastructure make life easier for the agency's security staff. They have also proven highly effective at threat detection, helping the agency pass, with flying colors, a required external security audit.

The Pursuit of Security Best Practices

Cybersecurity is a major concern for Daniels. "Obviously, the cyber threat landscape changes every day," he says. "If you are not following best business practices and utilizing a layered approach to security, it is hard to combat advanced threats." However, as a relatively small state agency, the Illinois State Treasurer faces staffing constraints that complicate the pursuit of best practices. The IT team has 22 staff members, only 4 of whom have cybersecurity responsibilities.

Each member of the security team specializes in specific components of the infrastructure. Unfortunately, the agency's legacy security solutions were "convoluted and hard to use," Daniels says. "They required a lot of troubleshooting, which was very difficult for our small team." Although the Illinois State Treasurer has the same types of data-protection responsibilities as a commercial bank, "We do not have the human capital to have as robust a cybersecurity team as large private-sector financial institutions can afford," Daniels adds.

The agency had been standardized on another vendor's firewalls and other security solutions for decades, but those products were expensive and difficult to manage. Daniels needed to make a change. The Illinois State Treasurer was already using a FortiGate appliance for virtual private network (VPN) functionality. When Daniels learned that it was a fully functional next-generation firewall (NGFW), he looked into moving into a trial. Daniels had heard positive feedback about Fortinet from his peers at a large private-sector financial firm. His team embarked on a proof of concept with a FortiGate NGFW and immediately liked its ease of use. Within a few weeks of launching the NGFW proof of concept, Daniels had removed a significant portion of his existing cybersecurity architecture and replaced it with Fortinet solutions.

"Without the partnership with Fortinet, we would not have been able to shed light for our partner agencies, very similar to our own, on the importance of looking outside of the box for the way they do security."

– *Joseph Daniels, Chief Information Officer, Illinois State Treasurer*

Details

Customer: Illinois State Treasurer's Office

Industry: Government

Location: Springfield, Illinois

Business Impact

- Simplifies training of limited security staff through single-pane-of-glass visibility
- Enabled rare perfect score on information-security audit, thanks to completeness of weekly threat assessments
- Revealed suspicious applications lying dormant for 2-3 years through sandbox analysis
- Meets unclaimed property monitoring requirements and enables an unclaimed property "museum" with FortiCamera

Daniels and his team also liked the Fortinet Security Fabric that provided the tight integration between FortiGate NGFWs and the FortiSandbox solution, which can execute questionable code in an isolated environment to determine whether the code represents a true threat. When he joined the Illinois State Treasurer two years ago, the organization had a significant security backlog. Its infrastructure included over 2,500 different applications, many of which had not been assessed for potential threats in several years. An internal analysis of applications running on Treasury systems using FortiSandbox revealed several unwanted applications.

Integrated Security Visibility, Improved Usability

In addition to FortiGate NGFWs and FortiSandbox, the Treasurer's Office rolled out FortiGate Cloud, a Software-as-a-Service (SaaS) solution that provides cloud-based management of FortiGate NGFWs. "FortiGate Cloud provides cyber threat assessment reports that I started having delivered every single week because they gave us a really good overview of our environment," Daniels says. The Treasurer's Office is also using FortiWeb, a web application firewall (WAF), to protect a cloud deployment in Microsoft Azure.

The FortiGate NGFWs enable the security team to achieve greater visibility into their network and isolate network traffic to a particular endpoint or application, something the legacy firewalls could not do. Any malware attempting to beacon out to a command-and-control server or perform data exfiltration will be rapidly identified and eradicated. Moreover, the Fortinet infrastructure consolidates information about threat detection and response networkwide, which is essential for securing sensitive data, such as account or routing numbers, and connections with external financial institutions. "Having that single-pane-of-glass visibility makes security management a lot easier," Daniels says.

The Fortinet solutions are also meeting expectations with regard to usability. The four-person security team needs to be able to easily onboard new employees and cross-train for different job roles. The FortiGate NGFWs make this possible. "They could come in, use the GUI, look at policies and procedures, follow all the training material out there, and really make the firewall the first secure point of entry for the agency."

Solutions

- FortiGate NGFW with Enterprise FortiCare Support
- FortiSandbox
- FortiGate Cloud
- FortiCamera
- FortiAnalyzer
- FortiWeb

"You can walk step by step, from inception to completion, through all the training videos Fortinet provides. That documentation is critical for agencies without a large staff because you can take anyone and walk them through it."

– *Joseph Daniels, Chief Information Officer, Illinois State Treasurer*

Beyond training to achieve basic familiarity, Fortinet's extensive library of videos and guides have made it possible for the Treasurer's staff to solve many security problems without requiring external support. Daniels says, "You can walk step by step, from inception to completion, through all the training videos Fortinet provides. That documentation is critical for agencies without a huge staff because you can take anyone and walk them through it."

On the rare occasion that the team has experienced difficulties they cannot solve on their own—whether security issues or general IT challenges—the Fortinet support team has always been ready to help. According to Daniels, "If I could say anything, they are probably overly helpful. They keep our staff on track."

Compliance Audit

With being not only a state government agency but also a financially regulated office, the Illinois State Treasurer undergoes frequent audits. Each year, the organization undergoes 12 months of internal audits and 9 months of review by an external auditor.

Daniels' team recently underwent their first information security audit, which occurs every two to five years, under his tenure. At that point, the organization had a partnership in place with Fortinet and had rewritten policies and procedures to follow the guidelines of the National Institute of Standards and Technology (NIST) and Microsoft's Security and Compliance Framework.

During the audit, Daniels says the weekly security reports provided by FortiGate Cloud were a critical resource. They provided him with the hard data necessary to answer auditors' questions and demonstrate compliance with required security controls. As a result, the audit passed without issue.

However, Daniels believes in continuously working to improve his organization's security to meet evolving cyber threats. Since the audit, he has purchased FortiAnalyzer and is working to take advantage of its improved visibility and security analytics. "The FortiAnalyzer provides a much deeper dive into our network, so I am looking forward to the next audit that we have. We will be much better prepared."

An Integrated Platform Unlocks New Capabilities

While network security is a significant priority for Daniels' team, it is not their only concern. The Illinois State Treasurer is also responsible for managing the lost and unclaimed property of Illinois residents. The agency's unclaimed-property division faces stringent security and auditing requirements, undergoing continuous external audits. Since the department is responsible for properly managing and securing property that belongs to Illinois citizens, every transaction and movement in the secure vaults requires constant video monitoring.

The unclaimed-property division had cameras deployed for surveillance of the vaults, but they were not meeting the organization's needs. The video feeds had poor picture quality and would occasionally fail. The team chose the FortiCamera surveillance solution to replace these impractical cameras. FortiCamera not only meets their requirements with impeccable picture quality and advanced monitoring capabilities but also seamlessly integrates into the Fortinet Security Fabric. This integration enables the security team to monitor the FortiCameras from the same dashboard as the rest of the agency's security architecture.

Providing an Example for Other Government Agencies

Deploying Fortinet solutions has enabled the Illinois State Treasurer to act as an example for other state government agencies. Daniels participates in weekly calls with external agencies, where they share information about the security challenges that they are facing and how they are addressing them. According to Daniels, "Without the partnership with Fortinet, we would not have been able to shed light for our partner agencies, very similar to our own, on the importance of looking outside of the box for the way they do security."

May 19, 2020 7:44 AM

625385-0-0-EN

D:\Fortinet\Case Study\State of Illinois\cs-FA-illinois-state-treasurers-office-5192020