splunk> a CISCO company

CUSTOMER STORY

Webster Bank Builds Trust, Drives Operational Efficiency with Splunk Enterprise Security Premier

Key Challenges

Webster Bank needed to expand security capabilities to keep up with stringent compliance regulations, combat insider threats, and increase visibility to demonstrate value and strong governance to stakeholders.

Key Results

Security teams now work from a unified platform that accelerates detection, refines and optimizes response efforts, increases efficiency, and highlights value by elevating key metrics and insights.

Product: Splunk Enterprise Security Premier

Industry: Financial Services

Outcomes

- Decreased MTTR for rapid threat detection and containment
- High incident resolution within SLA for prompt remediation
- Increased visibility and coverage across the computing estate

Security. Trust. Community.

These are the values that Webster Bank upholds every day for their customers, staff, and stakeholders. For nearly a century since its founding, the regional bank has been a good steward, business partner, and corporate citizen in the community for individuals, families, and institutions alike.

Trust is fundamental to their practices and the driving force behind everything Webster Bank does. Part of that trust is ensuring that the bank's financial systems and critical data remain secure and fully compliant. To keep pace with mandates such as New York DFS, OCC, FINRA, and others, Patricia Voight, CISO of Webster Bank, and her team needed to improve and incorporate advanced capabilities for audit trails, user activity monitoring, and increased data storage.

As the New York-based bank's technology footprint expanded, the organization adopted Splunk Enterprise Security Premier to bring its security operations together on a single, integrated platform. The Splunk platform unifies SIEM, SOAR, and User and Entity Behavioral Analytics (UEBA) giving Webster Bank a comprehensive, end-to-end view of its security environment and enabling the team to operate with greater speed, consistency, and confidence. With its ability to perform in-depth investigations and drill into complex datasets, Splunk ES Premier was the perfect fit as Webster Bank's security journey continued to mature.

"We have a long-term partnership with Splunk," said Voight. "We have daily use of our Splunk Enterprise Security solution for our monitoring and compliance capabilities across the organization. It funnels all the machine data coming from every single application and every single data source that we have — it is all going through Splunk. It's the cornerstone of our environment."

Enterprise Security Premier creates transparency — and trust

Trust starts with transparency. On any given day, security leaders at Webster Bank need constant visibility into its technology environment as they face the growing demands of stringent compliance regulations while continuing to demonstrate strong governance to Executives and the Board.

That's where Enterprise Security Premier shines. Combining powerful UEBA capabilities as well as SIEM and SOAR into one seamless integrated platform that offers a comprehensive view across the organization. Now, rather than managing multiple point solutions, Webster Bank's security team works from a single pane of glass that tightly connects detections, investigations, and response actions, reducing complexity while enabling quick, insightful correlations and accurate analysis.

Quick accurate correlations go a long way when detecting phishing and attacks by foreign threat actors. For example, by using the logs available in Splunk, the team can quickly see IP addresses attributed to specific VPN services associated with advanced persistent threats (APTs) and other threat actors attempting to gain access to their environments. From there, the team can rapidly build detections to help mitigate threats and reduce the impact on their systems.

Voight said that in addition to easily accessing critical data, this unified approach helps her team highlight value by showcasing key metrics and insights to everyone across the organization, from Executive and Board members to key stakeholders and colleagues across various business and technology areas.

"We're able to easily visualize our results and efforts — we're headed towards this concept of a single pane of glass that shows Webster Bank's Executive members the benefit for each of their business lines," she said. "I also report up to the board, so I want to be able to show them this sort of single pane of glass, how I get comfort around our environment on a day-by-day basis."

But transparency doesn't just put Webster Bank's Executives and their Board at ease. It also goes a long way to establish and maintain trust with colleagues and clients as their needs and the environment evolves. Voight said that Splunk ES Premier provides a clear and transparent means of demonstrating security and accountability.

> **We have a long-term partnership with Splunk. We have daily use of our Splunk Enterprise Security solution for our monitoring and compliance capabilities across the organization. It funnels all the information including the machine data coming from every single application and every single data source that we have — it is all going through Splunk. It's the cornerstone of our environment.**
>
> Patricia Voight, CISO, Webster Bank and Webster Financial

"It brings together all the security elements across our organization," Voight said. "We use the unification of SIEM, SOAR, and UEBA — powerful capabilities combined together into one seamless integrated platform. It's a comprehensive security view that we use across our organization and across all of our teams."

Automation accelerates innovation

If transparency accelerates trust, then automation is the engine that drives it. By integrating SIEM and SOAR capabilities within ES Premier, analysts were able to automate routine security tasks that once took up their valuable time. Automation now streamlines playbooks, standardizes processes, and helps keep documentation current — an essential requirement in a heavily regulated environment. Automation not only helps lighten the load for analysts, it allows them to respond faster and more consistently to incidents. Specifically, automation helps prioritize and offload low-severity alerts, which allows analysts to turn their attention to the most critical security threats, in turn enabling senior team members to focus on oversight, risk management, and continuous improvement. Voight said that ES Premier also allows her team to integrate data from Splunk into ServiceNow, which helps support first through third line risk teams and compliance activities.

"Automation is critical to our success and critical to our unification story," she said. "We've integrated the SIEM and SOAR capabilities together to have easier adoption baked in automation. Our goal is to empower our level one and level two teams to free up some of the subject matter experts so they can focus more on strategic work."

While Webster Bank is just beginning a comprehensive AI implementation, looking ahead, Splunk's ES Premier will be at the center of future innovation. As AI-driven capabilities mature, the bank plans to further accelerate detection, triage, and response, especially within the security operations center (SOC) to address and eradicate data theft and malicious threats. Voight said that her team will continue to prioritize task automation, anticipating AI's "significant acceleration" in security over the next year.

"We're really in the early stages of our AI journey," Voight said. "Splunk is the central data point for all of our data collection and integration from end-to-end enabling all of the machine data to come together. It has been and will continue to be part of our strategic plan and is very important to us as an organization."

UEBA gives leaders an inside look

Customers and employees alike need to know, not just feel, that they're secure from malware attacks, data breaches, and other threats — both outside and inside their organization. That's why ES Premier strengthens Webster Bank's ability to detect insider threats and data exfiltration, two of the most significant risks facing financial institutions. By embedding UEBA directly into the platform, their security team has access to new behavioral insights that help bring anomalous activity to light early, without taking up valuable time from the security team to build out different complex queries. As an early adopter and design partner, Webster Bank worked closely with Splunk to help shape these capabilities, ensuring they aligned with the real-world needs of customers as well as regulatory demands. When combined, unified visibility, automation, and behavioral analytics allow the security team at Webster Bank to accelerate detection, refine and optimize response efforts, respond to incidents faster, scale use cases to other technical teams, and operate more efficiently, all without introducing additional tools or overhead.

> **It's been an incredible journey with Splunk ES Premier. It brings together all the security elements across our organization. We use the unification of SIEM, SOAR, and UEBA — powerful capabilities combined together into one seamless integrated platform. It's a comprehensive security view that we use across our organization and across all of our teams.**
>
> Patricia Voight, CISO, Webster Bank and Webster Financial

"We want to make sure we've got the right kind of platform in place and that's where we leverage Splunk and our partnership with Cisco in the broader sense," said Voight. "We want to build on our ES Premier success, integrate SOAR, Mission Control, and other capabilities into our environment, and focus more on automation to reduce manual tasks so that we can focus on leadership and growth, while staying prepared for the dynamic threat environment."

For Webster Bank, the ultimate measure of success is that customers don't have to think about security. They can trust, with confidence, that it's doing its job — customer data is protected, and transactions are secure and free from disruption.