elastic

Search. Observe. Protect.

CASE STUDY:
Martin's Point Health Care

Replacing legacy antivirus solution with Elastic Endpoint Security

Martin's Point Health Care (MPHC) is a non-profit primary healthcare and insurance provider headquartered in Portland, Maine. The company employs 800 full-time staff, and has 18 locations across five states.

Company Overview

Martin's Point Health Care (MPHC) leadership needed to better understand their risk posture and be able to securely share patient information across their organization to deliver high-quality patient care. Elastic Endpoint Security offers full-stack protection coupled with ease of use to address cyber threats and provide reporting to determine the health of their enterprise.

Comprehensive threat prevention and hunting

Elastic Endpoint Security provides full-stack prevention, accelerated detection and response, and automated threat hunting across the MITRE ATT&CK™ matrix.

Performing in a highly segmented network for PCI DSS and HIPAA compliance

The unprecedented speed of Elastic Endpoint Security enables Martin's Point Health Care to stop threats in real-time and at scale in a highly regulated environment — with minimal performance impact.

Setting up a nimble SOC team for success

Elastic Endpoint Security's easy-to-use and automated interface enables junior SOC analysts to rapidly triage, investigate, and respond to alerts.

Products Used

Elastic Endoint Security

MPHC's Journey with Elastic

Symantec antivirus failing to safeguard critical patient information

MPHC has a small and nimble enterprise security team tasked with protecting critical patient health records and ensuring their heavy regulatory footprint of compliance with HIPAA (Health Insurance Portability and Accountability Act) and PCI DSS are met. This means the ability to keep pace with targeted attacks that are a constant for MPHC. The MPHC board needed to know their risk posture and the health of the organization.

Their current anti-virus solution from Symantec failed to give leadership the level of visibility and protection necessary to safeguard critical patient information and ensure compliance with regulatory requirements.

The IT team needed a solution that would address three primary challenges:

- Block known and unknown attacks beyond malware.
- Monitor 24×7 device activity, even when offline.
- Provide the MPHC Board and leadership a status of the health of their enterprise network.

Full-Stack protection across MITRE ATT&CK™ with Elastic Endpoint Security

Martin's Point Health Care performed an extensive evaluation of endpoint security options, including cloud-based next-gen AV solutions to replace Symantec's antivirus solution. They chose Elastic Endpoint Security because it was the only solution that provided comprehensive visibility with full-stack protection across the breadth and depth of the MITRE ATT&CK™ matrix. Other next generation-AV solutions were too complex for junior analysts to use and too slow to stop unknown threats. The MPHC team found Elastic Endpoint Security's distributed architecture and robust two-way API could seamlessly integrate with existing network tools and operational processes within their environment.

Elastic Endpoint Security stops targeted attacks and more

Elastic Endpoint Security provided full-stack protection that stopped targeted attacks before they started, stopped ongoing attacks before any damage or loss occurred, and minimized the time IT spent trying to detect and contain threats. Another benefit the security team identified over other solutions was Elastic Endpoint Security's ability to eliminate multiple host agents with one single agent platform. Elastic Endpoint Security replaces existing AV, endpoint detection and response, and incident response agents, drastically reducing the cost and time required to stop emerging threats. The platform provides comprehensive protection and detailed reporting to help their leadership understand their risk posture.

> *Visibility and fast response across our network are critical to protecting our infrastructure. Elastic Endpoint Security's ability to provide full-stack protection gave us the confidence to replace our traditional AV solution and gave comprehensive protection at the earliest stages of the attack lifecycle.*
>
> - **Matthew Witten**, CISO, Martin's Point Health Care

elastic

Search. Observe. Protect.

CASE STUDY:

SoftBank Payment Service

Powering the Search for Payment Service Monitoring and Fraud Detection

SoftBank Payment Service Corporation is a company within the SoftBank Group which provides member ecommerce sites with online payment markets, using payment screening and an API.

Company Overview

SoftBank Payment Service also supports transactions made by mobile operators, transactions in convenience stores, the use of prepaid cards, transfers between bank accounts, and credit card reward programs, as well as standard credit card payments. To date, approximately 80,000 companies have chosen to use this service, in part because it allows clients to reduce development and processing costs.

At the Glance

240M

transactions
as of FY 2016

80k

companies use this service
as of October 2017

40+

payment methods

Products Used

Elastic Stack

Alerting

Machine Learning

Creating Greater Visibility into Online Payment Services

SoftBank's online payment system previously sent failure notifications to technical staff responsible for Softbank systems via email or Slack. This meant that SoftBank's IT support team was responsible for reporting failures to the relevant sales department and, in turn, the sales department would report incident details to the member store where the payment failure had occurred. The IT team was solely responsible for delivering information about failures, tracing the cause of the failure, fixing it, and making the client aware of the situation. This system of failure reporting was not only time consuming, but also prevented delivery of immediate and complete oversight of relevant failure data to the sales and operations departments at SoftBank Payment Services.

Kibana's Dashboard Makes Overall Service Conditions Visible in Real Time

Given the lack of visibility into failures when they occured, SoftBank sought a monitoring and visualization tool.They found Kibana, with its clear and easy-to-use dashboards, as the ideal product. Using Logstash to regularly update transactional data within Elasticsearch, SoftBank could then visualize transaction data immediately using KIbana and share that information across their business.

> *"Our focus was on realizing a system that lets anyone check the dashboard anytime, anywhere."*
>
> **– Junya Suzuki,** Senior Architect, Softbank Payment Service

Softbank operational staff created dashboards that show successful payments in green and failed payments in red. Operators monitoring these dashboards can quickly catch changes in the volume of successful and failed payments, organized by the different payment methods, and act on them swiftly.

There are two simple rules that now let operators understand what they are seeing more intuitively, and to quickly pinpoint payment problems:

- Watch for rapid decreases in successful, green-colored payments.
- Watch for rapid increases in failed, red-colored payments.

If any changes are noted, operators can quickly drill down on transactions at both the payment method level and the member store level and discover the origin.

The Elastic Stack also provides credit processing status information. Kibana dashboards can show operators information on which member stores send requests, and what error codes occur. These error codes are used to identify when incorrect credit card numbers are used, if a card has an invalid expiration date, or if the credit card is blocked or unusable. Pie charts on the dashboard provide detailed data on the number of users who are experiencing errors, as well as the credit card numbers involved. This, in turn, helps operators to determine when fraudulent credit card transactions are occurring.

Kibana dashboards can also be securely shared with other teams, both at and away from work. For example, an engineer on-call but not in the office can set up system-trigger alerts for his smartphone. Softbank uses Jenkins to capture dashboard screenshots when errors occur and, using Selenium, repeats this process every five minutes. Those screenshots are then posted to a specific Slack channel that alerts the engineer on duty.

Detecting Fraudulent Credit Card Use with Machine Learning

In July of 2017, SoftBank Payment Service started using machine learning on a trial basis. As a test, Elastic machine learning was used to process data specific to daily total payment transaction trends over the course of three cycles. Any change significantly different from the forecast was identified, processed, and considered to be an anomaly. As an example, credit facilities for online services, such as smartphone games, are usually made available on the first day of every month, usually resulting in increased payments. At first, this situation was detected as an anomaly. But after three months, this pattern was recognized by machine learning, and the system stopped detecting it as a strange fluctuation in sales. Machine learning gave results precisely as expected.

To identify other potential problems, new machine learning jobs were created with different criteria, such as the total number of successful and failed payments divided into different payment methods. Member stores, product names, and error codes, including the error messages, were set as influencing factors. These factors help to identify the cause when certain anomalies are detected, for example, detecting spikes in alerts for incorrect card numbers or expiration dates. Historically, when member stores were analyzed all together, alert data could get lost among the incredible volume of transactions, making it difficult to search for problems. Now, however, when SoftBank Payment Services personnel filter for specific member stores, the Kibana dashboard lets operators immediately find fraudulent uses of credit cards. SoftBank Payment Services has realized, therefore, that visualizing the data alone is not enough when trying to identify credit card fraud.

> *"Thanks to machine learning, we were able to detect fraudulent use of credit cards."*
>
> – **Junya Suzuki**, Senior Architect, Softbank Payment Service

Upon detection of an anomaly, the job name and level of severity are posted to Slack. This process also comes with a unique measurement achieved by a Slack bot which captures and adds screenshots for the machine learning dashboard.

By increasing the level of complicated jobs, personnel can detect fraud earlier and will therefore be able to enhance services for member stores. SoftBank Payment Services IT support aims to also replace the old alert system, which is based on member store thresholds or on payment methods. They are thinking of instead, adopting an anomaly-detection process based on machine learning.

Creating Greater Visibility into Business Data

SoftBank Payment Services has since expanded the test use of the Elastic Stack for data visualization to new departments. In this expansion, the IT support team looked at Excel-based sales data previously managed by the sales department. Targets, such as the number of contracts and the web traffic to service sites, were then set to track against.

For contracts, trends for sales volumes over the course of two years were converted into stacked bar charts and broken down by department or project. Heat maps let SoftBank Payment Services list targets for the sales department that could be further refined to the sales representative level or filtered by month. Any targets met were shown in blue; missed targets were in red. A map was also used to chart the annual status for member stores, at the prefecture level.

For service site traffic, the IT support team at SoftBank Payment Services was able to guess which companies were coming to their site based on the source IP addresses. Access by both contracted client companies and non-contracted companies were ranked to provide the sales department with usable information.

A dashboard was initially created by IT support, upon request from the sales department. At some point, however, the sales department started working on new tasks ranging from adding and visualizing data, to creating new dashboards. The most difficult problem of adding Excel-based data was finally solved by developing a standalone drag-and-drop tool.

These early efforts paved the way for SoftBank Payment Services to conduct analyses in greater detail, using regular expression tools and simple mathematical operations available from Kibana. At the same time, those efforts let SoftBank Payment Services handle massive amounts of data that could not otherwise be processed with Excel. These enhancements now enable anyone to enter data and create dashboards, making improvements to reporting a real collaborative effort.

elastic

Search. Observe. Protect.

USER STORY: Bell Canada

Security Events Logging

Note: This post is a recap of a community talk given at a recent Elastic{ON} Tour event. Interested in seeing more talks like this? Check out the **Elastic{ON} Tour** page to see when a stop is coming to a city near you.

By: Emily Mosher

Bell Canada blog link

Bell Canada, one of Canada's largest telecommunications companies, offers mobile phone, television, internet, and landline services to big corporations, small and medium-sized businesses, and individuals across the country. Bell Canada's security operations center (SOC) covers every Bell office and business unit coast to coast and they rely on logs to detect cybersecurity threats.

Sylvain Proulx, Bell Canada's Senior Security Manager, says the business units — like Bell TV, Bell Internet, Bell Media, or Bell Mobility — that deliver services to their customers all use different technologies and applications, so the logs they collect are diverse and uncommon. Logs come from routers, firewalls, web logs, OS logs, application logs, and many other devices, some of which get 'chatty' and generate a lot of data.

The SOC had performed log and event correlation and incident response and reporting using only an ArcSight Security Information and Event Management (SIEM) solution. But over time, as the volume of logs increased, normalizing many new types of logs from a variety of devices bogged down the system. Their SIEM solution also provided only rule-based detection with no machine learning, so it generated a high ratio of false-positive incidents, which threatened to alert-fatigue their analysts.

Proulx said they'd hit their SIEM's limit. They found no single vendor solution that would let them ingest more data faster, build threat detection models, and normalize many new types of logs while also retaining ownership of their data. So, the SOC got to work augmenting their ArcSight SIEM with tools like the Elastic Stack to handle high log volume and traffic spikes automatically and generate meaningful security data that wouldn't overwhelm analysts.

Bell Canada gets data from bare metal servers, virtual machines, and, increasingly, from container infrastructure with Docker and Kubernetes. They needed a log shipper that was simple, lightweight, and straightforward to automate, so they turned to **Beats**. They use **Filebeat** and **Winlogbeat** to ship logs because they're easy to configure, test, and deploy. Plus, they can version control their configurations and there is no loss of data in case of a network outage.

After the data is queued in Kafka, the SOC must parse and normalize their logs in all their various formats in order to perform security analysis. Running **Logstash** instances on OpenShift has helped them scale quickly and automatically in case of traffic spikes without dropping logs, and it consumes less resources than multiple virtual machines. An additional advantage they've found to having Logstash in a container is that they can easily run it through RSpec for testing before moving to production.

Once the logs are normalized, the SOC stores them in **Elasticsearch**. Bell Canada's previous solution was unable to handle increasing log volumes and scale without losing logs. The SOC now does this with Elasticsearch, which allows them to scale quickly and horizontally, making their job a lot easier.

The day events are logged, the SOC searches the data with multiple queries and processes, which puts a heavy load on the cluster, so they've implemented a hot-warm architecture with automated deployment of new nodes. The beefier nodes are ingesting and being searched constantly, but when the logs lose their value, they're shipped to warm nodes for aggregation and lighter analysis. "If you lose a node in Elasticsearch, you can still keep working. Not a problem. You can fix it later," says Mathew Vandystadt, Bell Canada's Security Specialist Software Engineer.

Securing data is a top priority for the SOC. Role-based access control (RBAC) is a must, but RBAC can be painful to manage. With the **security features of the Elastic Stack**, the SOC has control over who has access to the data, they can add a layer of encryption over data transportation, and they can easily perform RBAC management — and it also ties in easily with their existing LDAP, meaning they don't need to spend extra time redefining group roles and can focus on their security mandate.

Once they have their data where they want it, the SOC analysts can use it to find security incidents — and good visualization is key. **Kibana's** straightforward interface means their busy specialists don't spend a lot of extra time learning new query languages.

> *"[Kibana] works great in our use cases. It's simple. We don't have to do a lot of training and we get a nice visualization."*
>
> **– Mathew Vandystadt,** Security Specialist Software Engineer | Bell Canada

Bell Canada found a flexible alerting solution for rule-based detection, but their analysts also needed smart detection that works with different algorithms, so they developed in-house machine learning with open source, ML-centric libraries. Their containers in OpenShift let them easily spin Python containers tied to Kafka or Elasticsearch so all data is accessible. Then they use their ArcSight SIEM for event aggregation and correlation to get a higher ratio of true positives to false positives, sparing analysts from alert bombardment.

They've built this whole pipeline using different software from different vendors, made possible because Elastic allows for simple integration with open security protocols. In the future, the SOC plans to merge a Cyber Threat Intelligence platform with their new security architecture. "Having that infrastructure right there allows us to do more than we were a year and a half ago with only the ArcSight solution," says Proulx.

Ready to learn more about the team's tools and pipeline? **Watch this October 2018 Elastic{ON}Tour presentation** and discover how they accomplish their security mission, including how Bell Canada handles long-term log retention and fast forensic data retrieval without using public clouds.