splunk>

CASE STUDY

CanDeal Streamlines Security and IT Operations, Rapidly Improving Security Posture

CANDEAL

Executive summary

CanDeal is the leading electronic marketplace for Canadian dollar fixed income securities and derivatives (www.candeal.com). To build out and improve upon its security posture, CanDeal needed a centralized, easy-to-deploy security solution that could give it an immediate comprehensive view across the enterprise. Since deploying Splunk Enterprise and Splunk Enterprise Security (ES), CanDeal has seen benefits including:

- Improved security posture
- Operational efficiencies
- Faster incident response

Why Splunk

In addition to complying with various regulatory controls and audits, CanDeal needed to proactively address and mitigate against advanced persistent threats (APTs). Furthermore, to support incident resolution, CanDeal wanted to examine traffic and network/wire data across all the nodes at its geographically dispersed datacenters.

CanDeal implemented Splunk Enterprise as its security information and event management (SIEM) solution, allowing the company to gain immediate, actionable insights into its infrastructure from a security standpoint. According to Kristofer Laxdal, head of information security at CanDeal, "Splunk Enterprise was easy and fast to deploy—there was not a whole lot of tuning to get it up and running, as opposed to other SIEMs, which typically require a significant amount of time to implement. With Splunk as our SIEM solution, it's easy to get data in and get results out quickly, which was one of our primary requirements."

In addition, CanDeal deployed Splunk Enterprise Security (ES) for prebuilt correlations, dashboards, reports and real-time alerting to solve advanced security use cases. Says Laxdal, "Splunk Enterprise Security gives us immediate, actionable, meaningful security intelligence that we simply did not have before."

Industry

- Financial services

Splunk Use Cases

- Security
- IT operations
- Application delivery

Challenges

- Lacked comprehensive visibility across the enterprise
- Wanted to strengthen security posture and proactively address and mitigate known and unknown threats
- Needed to provide transparency and comply with regulatory controls and audits

Business Impact

- Full visibility into security-related events to immediately improve security posture
- Provide auditors with overview of environment, to meet industry regulations
- Faster incident response to advanced persistent threats (APTs), saving resources and time
- Improved collaboration between teams to create operational efficiencies

Data Sources

- Data from every critical device across the organization, including all switches, firewalls, IPS devices, endpoints and over 100 servers (Linux, Microsoft Windows)
- Cisco VPN, and ASA and IPS logs
- Host intrusion prevention information from the Symantec (Enterprise) Endpoint enterprise product (SEP)
- HIPS, anti-malware, anti-spyware
- Protocol Stream data, including data streams through core switches for operational issues and troubleshooting: MySQL, HTTPS, DNS, SSL, HTTP

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security (ES)
- Splunk App for Stream

Full operational visibility into security posture

With virus and malware information now centralized and alerts set up within Splunk software, CanDeal has a single pane-of-glass view into weaknesses and vulnerabilities. The company can see the number and types of security attacks against its systems, and can geo-locate individual IPs that are making the attempts.

ES dashboards give internal employees and regulatory auditors an instant overview of CanDeal's complex environment—and enable Laxdal's team to create reports on CanDeal's security posture for the company's C-level executives. Laxdal notes, "Because of the pre-built content and the structure of ES, everything we had wanted to achieve was already there. We can view risk levels associated with each one of the endpoints or risk in general, and aggregate threat stream information so we can tell right away if one of our machines has been compromised. Not only do we have results, we have it in a visual format that is easy to digest."

The Splunk platform enables CanDeal to proactively correlate against known threats, as well as easily identify APTs lurking dormant within its infrastructure. Says Laxdal, "When an APT attempts to connect, it's now as simple as receiving a Splunk alert, and then moving to quarantine the source of the threat and eradicate it. The whole process can take as little as 10 or 15 minutes, which is an obvious win."

Cross-tier visibility helps break down departmental silos

To further improve its security posture, CanDeal uses the Splunk App for Stream to bring in protocol stream data and get on-the-fly ability to capture data streams running through core switches for operational issues and troubleshooting. This has given CanDeal the visibility and lightweight instrumentation it needs to refine its security processes.

"With Splunk as our SIEM solution, it's easy to get data in and get results out quickly. Splunk Enterprise Security gives us immediate, actionable, meaningful security intelligence that we simply did not have before."

Kristofer Laxdal, Head of Information Security
CanDeal

CanDeal's QA and development teams use the Splunk App for Stream for pre-deployment testing to get access and visibility without needing to query the DBA and network teams, enabling faster troubleshooting and quicker release cycles. This cross-tier visibility has improved team collaboration across the enterprise and ramped up the speed and efficiency of problem resolution.

The Splunk App for Stream has also enabled CanDeal to more easily resolve new application and connectivity issues, improving customer satisfaction. Says Laxdal, "When Splunk alerts tell us there's a problem, the Splunk App for Stream allows us to drill down into the nature of the problem and gain actionable information. This is relevant at all levels of the organization, whether it's providing a high-level report to the executive team, or being on point with our customer base."

Looking forward—expanding across the enterprise

Leveraging the Splunk App for Stream is part of CanDeal's broader strategy to expand its Splunk use cases from security toward application delivery and IT operations. CanDeal is investing in its Splunk infrastructure to grow its daily data volumes being indexed. Laxdal concludes, "Splunk provides the visibility across our enterprise that I need to do my job. Without Splunk software in place in our environment, we would truly be flying blind."