UNB
UNIVERSITY OF NEW BRUNSWICK

University of New Brunswick
www.unb.ca

Region
North America, Canada, New Brunswick

Sector
Education

Users
11,000 undergraduate and graduate students from 100+ countries, 64,000 alumni located globally

Trend Solutions
- Deep Discovery

IT Environment
- IBM QRadar Security Intelligence and Event Management (SIEM)

Business Benefits
- Deep Discovery identified 4.25% of analyzed traffic identified as malicious among 13,000 threat samples over thirty-day period
- 2,100 hours saved from automated analysis versus human detection
- Proactively prioritize threats with detailed analyses, real-time threat detection, weekly and monthly executive reporting
- Enhanced security posture

University of New Brunswick Gains Visibility into Evolving Threat Landscape with Deep Discovery

Battling advanced threats with advanced technologies

Overview

The University of New Brunswick (UNB) is one of the oldest public universities in North America, and the oldest English-speaking University in Canada. Established in 1785, UNB has two main campuses in Fredericton and Saint John with over 11,000 undergraduate and graduate students originating from more than 100 countries, and 64,000 living alumni around the world.

UNB has always been a technology leader. It was the first Canadian university to offer email services, and it remains on the leading edge of innovation. UNB conducts between $40 million to $50 million in research annually, and has pioneered technologies such as GPS mapping and magnetic resonance imaging. In 2001, IT employees from UNB founded Q1 Labs and sold the company to IBM in 2011. UNB still uses Q1 Labs' flagship product, the QRadar Security Intelligence and Event Management (SIEM) suite, which provides insight into the overall security posture of the university.

Like many universities, UNB operates in a hybrid-centralized model with core infrastructure services such as network connectivity and datacenter provided by the main IT department. Users work on PCs and Macs, and connect to the network using a variety of mobile devices. The The Central IT Department is responsible for core IT infrastructure for the entire university as well as IT security, mobile technology, and web technology. In 2012, following a breach of the UNB webserver by a hacktivist group, the IT department founded the security action team (SAT), which consists of the CIO, the director of IT architecture, the senior network architect, and the Director, Strategic Initiatives.

Challenges

Like any large educational institution, UNB needs to protect student information and its intellectual property, but today's university networks have become some of the most complex to manage and most challenging to defend. Students and faculty use a variety of mobile devices to connect with the university's network, leaving them vulnerable to a wide range of attacks.

"Universities are among the most targeted institutions in the world," said David Shipley, Director of Strategic Initiatives within the Office of the Associate Vice President, Information Technology Services for UNB. "By culture and by history they are places where the open exchange of information occurs at a rapid and continuous pace, and this leaves them vulnerable to attacks."

Some of UNB's biggest concerns were defending its network against malicious activities ranging from denial of service (DoS) attacks to sophisticated attempts to access protected data, such as researchers' intellectual property.

"We've faced everything from teenage hackers upset over an Xbox match with a UNB student and subsequently launching a massive denial of service attack, to sophisticated attempts to infiltrate devices to steal intellectual property," says Shipley.

A key area of concern from many university IT departments is the shortage of resources to protect their IT environments from the sheer volume of attacks. "We see millions of attempts on our network via remote access points every week," said Shipley.

These are machine-scale attacks and go far beyond the available human resources required to respond to them.

"We needed, and continue to need, increasingly sophisticated and automated security tools that can accurately assess genuine threats and help us improve our response time to those issues," says Shipley.

"Trend Micro Deep Discovery™ has been a huge benefit in terms of understanding where the real threats are and in helping us develop better strategies and processes to combat these threats," he adds.

These automated technologies, combined with a cross-functional security team and increased security awareness activities and education for students, faculty, and staff, have helped UNB significantly improve its security posture.

"To better educate our thousands of users about the threats we face, we need to know exactly what we're facing. Trend Micro Smart Protection Network gives us that kind of insight."

David Shipley,
Director of Strategic Initiatives within the Office of the Associate Vice President, Information Technology Services for UNB

"Knowledge is half the battle. Deep Discovery gives us the insight that we need to assess how secure our IT environment is."

David Shipley,
Director of Strategic Initiatives within the Office of the Associate Vice President, Information Technology Services for UNB

"Deep Discovery identifies malware in a matter of minutes with advanced, automated threat detection that helps significantly speed up our threat response."

David Shipley,
Director of Strategic Initiatives within the Office of the Associate Vice President, Information Technology Services for UNB

Challenges *Continued*

"No one can be completely secure and no system is fool-proof. But with increasingly powerful tools like Deep Discovery, we can be far more proactive, and when an issue does occur, far more effective in our reaction," says Shipley.

"University IT departments are hopelessly outgunned when defending their environments against today's threats," he adds. "We have to rely on technology for protection. Our task was to find the best solution for our needs."

Why Trend Micro?

SAT team members became aware of Deep Discovery after discussing security challenges with a Trend Micro representative at the 2013 Atlantic Security Conference. The idea of a pilot program and partnership between Trend Micro and UNB was born.

"Our partnership with Trend Micro has helped UNB handle several important security issues over the past 18 months," says Shipley. "This tool is helping influence our future approach to IT security, which includes a focus on more automated and proactive technologies designed to fight machine-scale threats."

Solution

With Deep Discovery installed on two-thirds of its network, UNB gets the investigative tools it needs to identify new threats and develop policy insights to further protect against attacks. It allows collaboration across multiple UNB environments and delivers threat intelligence via the Trend Micro™ Smart Protection Network™ infrastructure. "To better educate our users about the threats we face, we need to know what we're up against," said Shipley. "The Smart Protection Network provides that kind of insight."

Deep Discovery helps UNB prioritize threats with detailed analysis, monthly executive reporting, and real-time threat detection. It delivers alerts about malicious thresholds, and the UNB team uses it as a malware encyclopedia for cross-referencing threats.

"One common pitfall when it comes to new technologies is looking at it and thinking you have a silver bullet, "said Shipley.

"But technology on its own isn't good enough. You need the business processes, resources and policies that turn interesting technologies into practical tools," he adds.

"Our SIEM, QRadar is a fantastic tool, but we need deeper insight and a better understanding of malicious activity," said Shipley. "Adding an extra layer of security like Deep Discovery is a huge benefit for us as it adds increased intelligence to QRadar."

Results

Trend Micro's Deep Discovery solution has exceeded UNB's expectations by delivering valuable insights on the volume of threats the university receives every week. "Deep Discovery identifies malware in a matter of minutes with advanced automated threat detection."

This level of automated threat detection means huge savings in time and money for UNB. For example, in one 30-day period, Deep Discovery performed more than 13,000 automated threat analyses, and identified approximately 4.25% of analyzed traffic as malicious. That represented a time savings of 2,100 hours compared to manual analysis—hours UNB simply couldn't procure. "Knowledge is half the battle. Deep Discovery gives us the insight that we need to assess how secure our IT environment is."

UNB is now able to secure its IT assets, student information, and intellectual property thanks to Trend Micro. "The best working technology is the one that's most transparent to users," said Shipley. "Deep Discovery has been remarkably robust, even while handling a huge volume of traffic."

"Trend Micro has been a fantastic partner. When it came time to do a major upgrade to improve system functionality, knowledgeable staff were available on site to help us."

"We are truly grateful for the opportunity to partner with Trend Micro on this initiative," says Shipley.

"Deep Discovery has been a huge benefit in terms of understanding where the real threats are and in helping us develop better strategies and processes to combat these threats."

David Shipley,
Director of Strategic Initiatives within the Office of the Associate Vice President, Information Technology Services for UNB

What's next?

The Deep Discovery pilot program has provided UNB's security team with the advanced security and confidence they needed to protect their network. It has helped the team understand the scale of the threats faced by the university and has enabled the team to use data to help drive decisions about future security measures.

UNB is now implementing increased integration between Deep Discovery and QRadar and is considering the ideas behind automated threat detection and response in its evaluation of all future IT security asset purchases, with an eye to an integrated environment that would one day scale from endpoint AV protection and network access control to automated malware defense at the network level through a combination of Deep Discovery, QRadar and a next-generation firewall solution.

For More Information

For more information, please go to www.trendmicro/deepdiscovery.com

©2014 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo, OfficeScan and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [CS-SuccessStory-UNB-141122US]