University of New Brunswick Defends Against Ongoing Attacks with Deep Discovery™

Website
unb.ca

Region
North America, Canada

Sector
Education

Users
11,000 undergraduate and graduate students from 100+ countries, 84,000 alumni located globally

Trend Micro Solutions
Deep Discovery™

IT Environment
IBM® QRadar®

Business Benefits

- Deep Discovery™ Virtual Analyzer caught 5,602 suspicious files (146 malicious, 91 high-risk, 236 infected hosts)
- 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

The university can now stay ahead of massive increase in malware attacks

OVERVIEW

The University of New Brunswick (UNB) is one of the oldest public universities in North America, and the oldest English-speaking higher learning institute in Canada. Established in 1785, UNB has campuses in Fredericton and Saint John with over 11,000 undergraduate and graduate students originating from more than 100 countries, and 84,000 living alumni around the world.

UNB has always been a technology leader. As the first Canadian university to offer internet and email services, UNB is on the leading edge of innovation. They conduct between $40 million to $50 million in research annually and have pioneered advanced technologies such as GPS mapping and magnetic resonance imaging. In 2001, employees from UNB's IT department founded Q1 Labs, and sold the company to IBM in 2011. Today, UNB has integrated Q1 Lab's flagship product, the QRadar® Security Intelligence Platform, which integrates disparate monitoring functions into a total security solution.

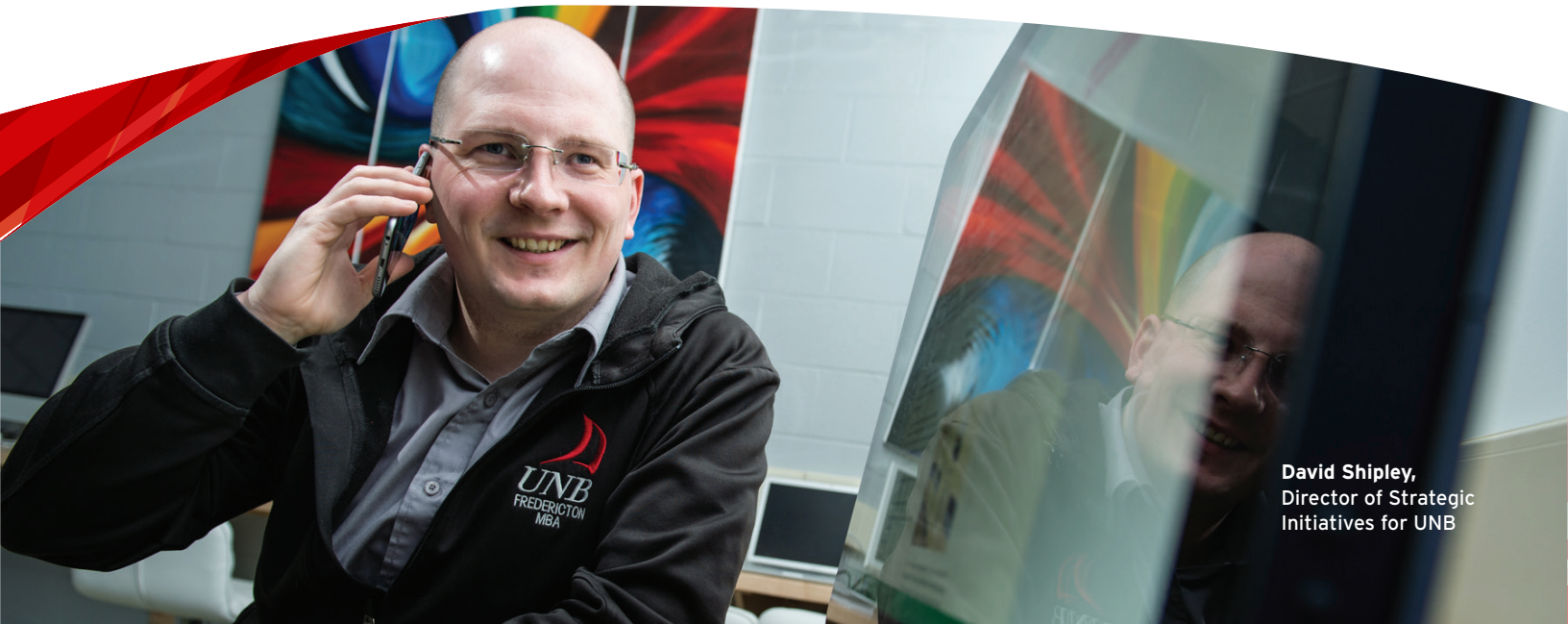
UNB's IT environment consists of a newly renovated datacenter that provides services, including security, for public higher education institutions across New Brunswick and Prince Edward Island. Users work on PCs and Macs, and connect to the network using a variety of mobile devices. With UNB's 65-person Information Technology Services department, security leadership responsibilities are shared amongst its director of operations, director of strategic initiatives, director of IT architecture, and managers of technical, service, and network operations.
This cross-functional and multi-campus Security Operations Committee provides guidance, leadership, and incident response expertise.

UNB recently completed an in-depth security roadmap architecture project and is in the midst of a multi-year data governance project, the final stages of a new IT security policy, and a year-long cyber security awareness program.

CHALLENGES

"Universities are the most targeted institutions in the world," said David Shipley, Director of Strategic Initiatives for the University of New Brunswick. "There's been a massive increase in malware attacks on Canadian schools. In just one month, UNB went from 149,000 emails with malicious payloads to more than one million," said Shipley.

University networks have become prime targets for today's cybercriminals. With the market flooded with stolen records from massive attacks on corporate giants, cybercriminals have now shifted their focus to exploits like ransomware. Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.



David Shipley,
Director of Strategic Initiatives for UNB

"When a ransomware incident occurs, Deep Discovery gives us the tools to see what's happening and react quickly to stop it. It's really helping us keep up with these attacks."

David Shipley,
Director of Strategic Initiatives for UNB

"Deep Discovery not only finds malware quickly, it has driven home the need for a second set of eyes on endpoints by consistently finding issues that our current endpoint tool does not detect."

David Shipley,
Director of Strategic Initiatives for UNB

"Deep Discovery has dramatically improved QRadar's ability to understand malware infections—and our ability to correlate the malware with other security activities detected by QRadar."

David Shipley,
Director of Strategic Initiatives for UNB

CHALLENGES *Continued*

"Users can open an attachment with a malicious payload and self-propagating ransomware with a sophisticated worm can spread through your network, or a compromised infrastructure can wreak havoc before the ransomware attack," said 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. The sharp increase in malware has exposed the rising expense associated with the IT team's productivity and capacity associated with massive, ongoing attacks. "We've learned that manual processes are not effective when it comes to identifying critical issues and rapidly resolving them," said Shipley.

WHY TREND MICRO

UNB's relationship with Trend Micro began with a recommendation in 2013. Initial discussions led to UNB's involvement in a pilot program with Trend Micro™ Deep Discovery™ solution to give UNB a full understanding of how the solution would benefit their IT environment. "It gave us the time we needed to build our case for the full implementation," said Shipley.

Since that time, UNB continues to expand and refine its use of Deep Discovery™ to protect its critical data against a growing tide of sophisticated threats. Today, Deep Discovery™ helps UNB to secure its IT assets, student information, and intellectual property.

SOLUTION

With Trend Micro™ Deep Discovery™ positioned to protect its most critical business networks, UNB gets the investigative tools it needs to identify new threats and develop policy insights to further protect against attacks, including ransomware. It allows collaboration across multiple UNB environments and delivers threat intelligence via the Trend Micro™ Smart Protection Network™. "To better educate our users about the threats we face, we need to understand the threats we're facing. The Smart Protection Network provides that kind of insight," said Shipley.

Deep Discovery™ helps UNB identify threats by prioritizing suspicious activity 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. "When a ransomware incident occurs, Deep Discovery gives us the tools to see what's happening and react quickly to stop it. It's really helping us keep up with these attacks," said Shipley.

Deep Discovery™ provides the visibility UNB needs to triage infections, so they have a much better chance of resolving issues before they affect the network. Shipley and his team rely on Deep Discovery daily snapshot reports to identify problems so tactical teams can rapidly respond. "We're as fast as humanly possible with Deep Discovery—and we realize we have to be faster," said Shipley.

To gain an additional layer of protection, UNB integrated Deep Discovery™ with their IBM® QRadar® Security Intelligence Platform. UNB plans to use combined data from the two solutions to better understand and manage the human side of IT security. "Deep Discovery has dramatically improved QRadar's ability to understand malware infections—and our ability to correlate the malware with other security activities detected by QRadar," said Shipley.

RESULTS

"Deep Discovery not only finds malware quickly, it has driven home the need for a second set of eyes on endpoints by consistently finding issues that our current endpoint tool does not detect," said Shipley.

Trend Micro™ Deep Discovery™ provides the targeted attack detection, in-depth analysis and rapid response UNB needs to stay ahead of attacks—despite limited IT resources. For example, in one day, Deep Discovery™ Virtual Analyzer caught 5,602 suspicious files, including 146 that were malicious, 91 high-risk, and 236 infected hosts. Since manual analysis of each malicious file takes three hours, UNB saved more than $17,000 in productivity.

Deep Discovery™ also assists with educating the UNB community to make them more aware of today's evolving threat landscape. "One in 10 users in any organization will open an infected attachment. Deep Discovery provides real numbers and stories that help change the way students, staff and faculty think before they click on suspicious email attachments," said Shipley.

UNB is now able to secure its IT assets, student information, and intellectual properties thanks to Trend Micro. "The best working technology is the one that's most transparent to users," said Shipley. "We haven't experienced a system crash or had to call for assistance with Deep Discovery, even with the volume of threat analysis being performed by the solution on a daily basis."

WHAT'S NEXT?

UNB plans to use the lessons learned from Trend Micro™ Deep Discovery™, IBM® QRadar®, and other tools to build out a digital immune system model. At the heart of that model is an automated response system to manage the growing number of attacks. "We're completely revamping our approach to endpoint security, and Deep Discovery has helped shape our security plan," said Shipley.

MORE INFORMATION

For more information, please visit **www.trendmicro.com/deepdiscovery**

TREND MICRO™

Securing Your Journey to the Cloud