

UNIVERSITY OF WATERLOO CHOOSES “BEYOND BETTER” THREAT PROTECTION

SECURITY AND SERVICE DESK TEAMS REGAIN HOURS OF PRODUCTIVITY PER WEEK



UNIVERSITY OF
WATERLOO

THE ORGANIZATION

Canada's University of Waterloo is home to research, teaching, and innovation that takes its students—and the world—beyond today's boundaries. Its reputation is backed by a slew of awards and recognition. It has ranked as Canada's most innovative university for 26 years; Canada's No.1 comprehensive research university for nine straight years; and among the top 25 in the world for computer science.

THE CHALLENGE

- Protect student privacy and university financial data
- Regain days spent remediating malware and ransomware infections
- Consolidate and simplify security wherever possible

THE SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection with Attachment Defense
- Proofpoint Emerging Threats Intelligence
- Proofpoint Threat Response

THE RESULTS

- Stopped malware and ransomware infections
- Freed security and client services teams from investigating and reimaging up to 40 systems per week
- Gained flexibility to work with existing and future email infrastructure

THE CHALLENGE

Malware and ransomware were coming in through email attachments. The situation was overwhelming the security and client services teams.

The information security services team works with the university's infrastructure teams to secure the campus network and everything attached to it. Student privacy is a main concern and so is the ability to prevent financial and procurement fraud. Before 2014, Waterloo began seeing malware getting into the environment through drive-by downloads. By 2016, threats usually arrived in—or attached to—email messages.

“At one point, we were getting hammered with close to 40 infections per week,” said Jason Testart, director of information security services at the University of Waterloo. “Obviously, our email gateway and antivirus tools weren't doing the job. Rather than trying to redevelop our own, we looked for a commercial solution.”

Malware infections were discovered when machines behaved in unusual ways or performance slowed. In these cases, the team would restore the system in one to two hours. When ransomware infected machines, the antivirus would not detect it until it actually began encrypting files. The client services team isolated the machine, locked out the user to stop the infection from spreading, and re-imaged the machine. Ransomware cases took anywhere from half a day to a full day to re-image.

Mike Patterson, manager of information security operations at the University of Waterloo, noted, “During one week when we had 40 ransomware infections, it took between 160 and 300 hours of time to restore systems to normal, depending on how bad the infections were.”

THE SOLUTION

When ransomware infections reached three per week and kept increasing, the team decided to find a new solution to stop malware. After evaluating several solutions, the University of Waterloo chose Proofpoint Email Protection and Proofpoint Targeted Attack Protection (TAP) with Attachment Defense.

The university piloted Proofpoint with up to 75 IT staff members. They were

“Proofpoint gives us the flexibility to evolve email security as our needs change. We’re always looking for ways to consolidate and simplify our environment, and Proofpoint makes it easier for us to improve email services without compromising security.”

Jason Testart, director of information security services, University of Waterloo

quickly convinced of its effectiveness. Other solutions they evaluated functioned like Internet gateways and required extra routing hops to send traffic to the correct destinations. But Proofpoint fit right into the university’s differentiated email architecture.

University of Waterloo deployed Proofpoint locally on its Exchange email system, which serves employees, faculty, and graduate students. An MX host handles email for the uwaterloo.ca group domain. The host sends the email to either a Sendmail LDAP server, which routes it to the Exchange email system, or to Office 365 for undergraduate student email. The LDAP server worked in concert with several Open Source anti-spam and bulk-mail tools. Now with Proofpoint sitting between the LDAP server and Exchange, University of Waterloo can discard some of the extra tools.

“Proofpoint is key in moving us off those tools because it provides malware and spam protection,” Testart said. “Proofpoint also worked with our existing MX host architecture, which other vendors couldn’t do.”

THE RESULTS

Beyond today’s needs

IT evolution is inevitable for any organization, especially a large university. Proofpoint’s configuration flexibility enables University of Waterloo to evolve its email environment and migrate tools at its own pace.

“Proofpoint gives us the flexibility to evolve email security as our needs change,” Testart said. “We’re always looking for ways to consolidate and simplify our environment, and Proofpoint makes it easier for us to improve email services without compromising security.”

Beyond better

The university still gets phishing and malware attacks. But Proofpoint stops threats before they reach users’ mailboxes. TAP sandboxes malware so users can’t access it but the team can investigate. If a suspicious email lands in a user’s mailbox, the team can remove it, take a closer look, and put it back in the mailbox if it’s legitimate. Proofpoint Emerging Threats Intelligence provides the team with a heads-up to new threats being identified by Proofpoint.

“With Proofpoint, malware and ransomware infections are not just better, they’re virtually nonexistent,” Patterson said. “It does a good job of not delivering suspicious emails in the first place, so users don’t have to sort through emails trying to decide which are legitimate or not.”

Beyond deployment

University of Waterloo used Proofpoint Professional Services to help the team set up, test, and cut users over to the Proofpoint solution. Setup and testing only took two days, and users were notified before actually moving to the new solution. The entire engagement took only three weeks.

Next on University of Waterloo’s project list is deploying a next-generation firewall solution and integrating security functions where possible. Today, they send TAP logs to their SIEM. The university is also deploying Proofpoint Threat Response, which enables the team to automate incident response, such as automatically removing malicious items from users’ mailboxes. Going forward, they plan to do more.

“We’re looking at integrating as many platforms as possible. It’s important that all our vendors can integrate” Patterson said. “Proofpoint is a critical part of that mix.”

For more information, visit proofpoint.com

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today’s mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.