



Large Canadian Hospitality Group Consolidates, Simplifies, and Uplevels Security with Integrated Sophos Solutions

CUSTOMER-AT-A-GLANCE



Northland Properties

Industry
Hospitality and entertainment

Number of users
2,000 users

Sophos Solutions

Next-Generation Firewall:
Sophos Firewall

Managed Services:
Sophos Managed Detection and Response (Sophos MDR)

Next-Generation Endpoint:

Sophos Intercept X Advanced with XDR
Sophos Intercept X Advanced with XDR for Server

Email Protection:

Sophos Email
Sophos Phish Threat

Cloud Security:

Sophos Cloud Optix

“After merging our networks, we needed to find a security platform that could support us in a complete and consistent manner. Sophos met our requirements perfectly, and we continue to build on it.”

Farshad Nasimi, IT Director, Northland Properties



Challenge

- › Creating a foundational security infrastructure for a hybrid environment with a single-vendor, fully integrated solution
- › Simplifying security management for the small internal team while empowering them to do more in less time and with less effort
- › Increasing security capabilities without investing in costly staff resources or training

As Canada's most trusted name in hospitality and entertainment, Northland Properties is dedicated to delivering memorable experiences to its guests and customers. The large organization encompasses over 17 well-known brands, including The Sutton Place Hotels, Moxies, Denny's, Chop Steakhouse & Bar, Revelstoke Mountain Resort, Grouse Mountain, and the Dallas Stars National Hockey League (NHL) team. For half a century, Northland Properties has operated in four countries: Canada, the U.S., Ireland, and the U.K. The organization continues to expand primarily through acquisitions.

IT Director, Farshad Nasimi, and his team of 23 people oversee 200 corporate networks in different time zones and over 2,000 corporate users involved in various lines of business who need to access specific applications to do their jobs. Before Nasimi joined the organization, many of the Northland Properties brands operated independently, with their own IT departments, networks, applications, and security software.

“The Sophos MDR team members are dedicated security professionals. When an alert comes in, they know what it means, and they then provide information and feedback to us on how to improve our security posture, whether it’s informing us about what we need to investigate or letting us know about preventative measures that we can take for the future.”

Alex Fleeton, Cloud and Security Administrator, Northland Properties

How do you build out a consistent and unified security infrastructure in a large, distributed environment?

During the past four years, Nasimi and his team were laser-focused on consolidating the disparate networks and strengthening the organization’s security posture to mount a stronger defense against today’s complex and sophisticated emerging threats. With only four professionals on the cloud and security team, Nasimi knew he needed to cultivate a solid, long-term relationship with a security partner that could support the organization’s requirements in a holistic way today and into the future.

After evaluating several vendors, Sophos emerged as the top choice. The comprehensive Sophos product portfolio and its simple-to-use cloud-based management console, Sophos Central, has become the foundation for the organization’s security technology stack.

“When I first joined Northland Properties, we had all sorts of disparate security products from different vendors. After merging our networks, we needed to find a security platform that could support us in a complete and consistent manner. Sophos met our requirements perfectly, and we continue to build on it,” says Nasimi.

Which complementary Sophos solutions lay the foundation for truly multi-layered security?

Nasimi started by deploying Sophos endpoint security solutions. Sophos Intercept X Advanced with XDR, a Gartner Leader in 2021 and ranked number one by AVTEST, provides Northland Properties with a broad array of endpoint protections. These include ransomware protection and recovery, extended threat detection and response, deep learning technology for signature-less malware detection, root-cause analysis, and many more. Nasimi also deployed Sophos Intercept X Advanced with XDR for Server, which features cloud security posture management, server lockdown to safeguard against unauthorized programs, and protection for cloud, on-premises, and virtual server workloads.

“With Sophos Central, we have the ability to control and manage our environment through one portal because of the tight integrations of all the products. And, since all these tools talk to each other, all the information is under one umbrella. Additionally, Sophos Central is more intuitive and user-friendly and can be used by virtually any administrator.”

Farshad Nasimi, IT Director, Northland Properties

Next, Nasimi and his team implemented Sophos Email, which uses a multi-layered approach to prevent phishing emails from reaching users; block malicious URLs, spam, and malware; and keep data safe through machine learning analysis of content, encryption, and policy enforcement. Sophos Email even identifies high-profile targets at Northland Properties and protects against malware-free impersonation and Business Email Compromise (BEC) attacks.

As a complement to these email protection technologies, Nasimi has launched an initiative to foster greater security awareness among users. He is using Sophos Phish Threat training to identify areas of weakness across the organization and to empower users to participate in improving the organization's security posture. Phish Threat provides automated, realistic

simulations and interactive training modules in multiple languages. Detailed, at-a-glance reporting allows the security team to assess overall risk across user groups on a regular basis.

How does Sophos Firewall support a more secure corporate network?

With a unified network architecture firmly in place, the security team added next-generation Sophos Firewall to their security arsenal to maximize protection while providing application acceleration.

Knowing that nearly 90% of network traffic is encrypted, Nasimi and his team rely on the solution's Secure Socket Layer (SSL) inspection to uncover hidden malware. Sophos Firewall's high-

performance deep packet inspection (DPI) blocks ransomware and safeguards against breaches. Its powerful threat protection toolbox comprises intrusion prevention system (IPS), web protection, and application control, along with deep learning and sandboxing. Sophos Firewall also accelerates business application traffic, regardless of where users are located—at home, at headquarters, or at other locations—so security never gets in the way of user productivity.

“If you’re a large enterprise looking for a platform that integrates well with different ecosystems and you want a suite of fully integrated tools that communicate with each other and can be managed with one dashboard, Sophos is my highest and best recommendation.”

Farshad Nasimi, IT Director, Northland Properties

When your security team has limited capacity, how does Sophos fill in the gaps?

To augment his small security team, Nasimi has added Sophos Managed Detection and Response (Sophos MDR) to the mix. This around-the-clock security managed service is staffed by highly trained threat hunters and response experts who actively monitor for threats and incidents, determine their scope and severity, apply business context, and initiate action to contain and neutralize them.

“Building an in-house security team with specialized skills can be extremely expensive, so for companies like ours, Cybersecurity-as-a-Service like Sophos MDR is the best option,” he remarks.

Alex Fleton, Cloud and Security Administrator, confirms the advantages of Sophos MDR: “The Sophos MDR team members are dedicated security professionals. When an alert comes in, they know what it means, and they then provide information and feedback to us on how to improve our security posture, whether it’s informing us about what we need to investigate or letting us know about preventative measures that we can take for the future.”

Shameer PK, Technical Manager for Information Security and Cloud, recalls how, in the past, it was nearly impossible to respond to threats that appeared after business hours or when he and other team members were in a position where they lacked proper network connectivity. With Sophos MDR, the entire team enjoys greater peace of mind knowing that they are backed by experts who are at the ready 24/7.

Another important aid for helping the security team identify and remediate threats faster in the cloud is Sophos Cloud Optix, which provides asset and network visibility across multi-cloud environments. It identifies unusual activity, discovers security vulnerabilities in the cloud (including software development projects), and pinpoints overprivileged users.

How does Sophos Central simplify and unify security management?

The security team manages the entire Sophos security infrastructure at Northland Properties via the intuitive cloud-based Sophos Central management platform. Sophos Synchronized Security technology, which is built into the platform, enables all Sophos products to communicate with each other, share valuable data, and automatically respond to incidents. For Northland Properties, with locations in multiple locations in Canada and other countries, it is the perfect way to gain a comprehensive view across the whole estate and to control risk from one place.

PK appreciates how Sophos Central makes it simpler to manage incidents when they arise. "Instead of looking at multiple platforms and multiple event logs like we used to do, the single pane of glass makes it easier for us to investigate a problem. With one click, I can find out where the problem is and determine how it happened, even down to the user and device level. This saves us tremendous time and effort," he points out.

The team no longer has to switch from one management console to another, which gives them the ability to monitor endpoints, the network, and all aspects of the IT infrastructure much more efficiently.

"With Sophos Central, we have the ability to control and manage our environment through one portal because of the tight integrations of all the products. And, since all these tools talk to each other, all the information is under one umbrella. Additionally, Sophos Central is more intuitive and user-friendly and can be used by virtually any administrator," points out Nasimi.

Northland Properties has emerged as the largest Sophos customer in Canada. Intent on cultivating a lasting relationship with Sophos, Nasimi aims to continue adding new functionalities in the future. He encourages any sizable organization on a quest to consolidate and fortify its security to seriously consider Sophos.

"If you're a large enterprise looking for a platform that integrates well with different ecosystems and you want a suite of fully integrated tools that communicate with each other and can be managed with one dashboard, Sophos is my highest and best recommendation," declares Nasimi.



Learn more about MDR today.
www.sophos.com/mdr