

# Sophos Solutions Meet the Evolving Needs of a Canadian Municipality



## Customer-at-a-Glance

**City of Castlegar**

**Industry**

Municipal government

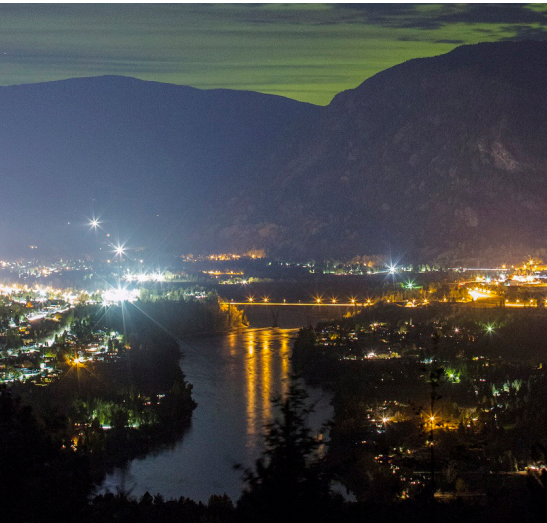
**Number of Users**

105 users across multiple city departments  
25 servers

**Sophos Solutions**

Sophos Central Endpoint Protection  
Sophos Intercept X  
Sophos Intercept X Advanced for Server  
Sophos SG UTM  
Sophos Access Points  
Sophos Phish Threat





*'Sophos Intercept X was extremely helpful and efficient at that critical moment. I can't even imagine what would have happened to the city, its departments, and its services if there wasn't anti-ransomware in place.'*

David Bristow  
Information Technology Manager  
City of Castlegar

The City of Castlegar in British Columbia, Canada is at the midpoint between Vancouver and Calgary. The municipal government of this scenic city, nestled in the Selkirk Mountains, consists of multiple departments with 105 employees: City Hall, the mayor's office, council meeting office, fire services, public works, and an airport that serves 80,000 passengers annually.

## Challenges

- Maximize finite resources to provide the same level of robust security that would be deployed at a big city government
- Provide employees and departments with diverse needs with an integrated security system that keeps data safe and systems running so they can better serve the city
- Save time, increase efficiency, and reduce the number of help-desk calls related to endpoint security issues
- Minimize downtime and provide proactive protection when ransomware and other advanced threats strike

## Can a small city enjoy the same level of security as a big city?

When it comes to securing users, data, and the city's 25 servers, information technology manager David Bristow's biggest challenge is providing the same level of security as a larger city while making the most of limited resources and a tight budget.

As a senior manager and one-man IT department, Bristow's responsibilities are wide-ranging – from planning technology strategies and budgets to fielding IT requests and resolving security issues, ensuring employees in departments with diverse requirements can do their jobs properly and keep things running smoothly. Among his duties, he oversees the data center at City Hall and transactions handled by finance. These include such as fees and property taxes, emergency dispatch systems for the fire department, electronically controlled public works systems, and electronic ticketing at the airport. All of these critical municipal services involve storage and transit of confidential data – from personally identifiable data of residents to the city's financial information.

Bristow was looking for a better way to protect endpoints and servers against today's ransomware threats and other sophisticated malware. The city's existing endpoint protection fell short, and often proved time-consuming to manage, requiring a great deal of manual intervention. Bristow needed a more efficient and automated way to proactively manage security citywide and apply the latest security upgrades to both existing and new systems.

## How does Sophos UTM safeguard a municipal network with multiple locations?

The City of Castlegar has been a Sophos customer since 2013. At that time, the municipality deployed Sophos Unified Threat Management (UTM), which provides all-in-one, next-generation network protection across the city's multiple locations. This offered capabilities including wireless security, web protection, sandboxing to isolate and analyze evasive threats, email protection, and web server protection.

For secure wireless connectivity for the distributed offices, the city uses Sophos Access Points that plug directly into Sophos UTM.

"I can honestly say that Sophos UTM has been completely stable for us. It's easy to upgrade devices and, in reviewing the UTM logs, I've seen quite a number of threats that have been blocked over time. Essentially, I don't have to worry about network security. I know that Sophos is working and protecting our city network as it should," declares Bristow.

## How does a city evolve its endpoint security to keep up with advanced threats?

Since Bristow had a positive experience with Sophos in the area of network security, he wanted to explore Sophos endpoint solutions with the idea of building out an integrated security architecture where all the components work together and are managed centrally. Another key goal was to reduce help-desk calls to free up his time so that he could efficiently and effectively manage high-priority tasks and make sure city services were being delivered as they should.

Bristow worked closely with his trusted Sophos partner, Opus Consulting Group, to map out a more efficient and proactive approach for the city's endpoint security.

Mehernosh Chemi, senior enterprise sales executive at Opus, recommended a multi-layered solution: Sophos Central Endpoint Security, complemented by Sophos Intercept X and Sophos Intercept X for Server to specifically protect against ransomware – all managed from a centralized, cloud-based console.

"The goal was to provide simplicity and to check off all the security requirements that just about any environment would have. With every product or solution that we present to our customers, we focus on what it brings to the table and are not trying to merely sell the latest and greatest in terms of the features and functionalities. For the City of Castlegar and, indeed, any municipality with evolving security needs, we feel that Sophos is an ideal solution – especially for protecting against advanced threats like ransomware," states Chemi. "We brought Sophos Intercept X to Bristow's attention, and after an in-depth presentation, he fully understood the value of the product and made the decision to move ahead with it."

Sophos Central Endpoint Security now provides the city of Castlegar with well-rounded and comprehensive protection for endpoints and data. The solution combines multiple technologies: signatureless anti-malware; malicious traffic detection; data loss prevention; and web, application, and device control. As an added layer of protection, Sophos Intercept X safeguards both endpoints and mission-critical servers, blocking a wide variety of attacks. It detects never-seen-before malware with deep learning, stops ransomware with unique Sophos anti-ransomware technology, and denies attacker tools with signatureless exploit prevention.

## What's the best way to simplify security management?

The unified Sophos Central console provides a single pane of glass that allows Bristow to manage all of his Sophos solutions – network, endpoint, and wireless – from a central web interface. Bristow no longer manually pushes updates out to endpoints, saving him time and effort and enabling him to focus on other tasks that demand his attention. In addition, the easy-to-configure console automatically prioritizes alerts, shares threat intelligence, provides default policies that follow users, and offers detailed and summary reporting.



*'For the City of Castlegar and, indeed, any municipality with evolving security needs, we feel that Sophos is an ideal solution – especially for protecting against advanced threats like ransomware.'*

Mehernosh Chemi  
Senior Enterprise Sales Executive  
Opus Consulting Group

## What happens when ransomware meets Sophos Intercept X?

The new Sophos solution set was put to the test quite quickly after deployment when a ransomware attack targeted the file server. Almost immediately—in mere nanoseconds—Sophos Intercept X locked down the server and automatically cleaned up the ransomware threat, preventing any damage and resulting in minimal downtime.

“Sophos Intercept X was extremely helpful and efficient at that critical moment. I can’t even imagine what would have happened to the city, its departments, and its services if there wasn’t anti-ransomware in place,” relates Bristow. “Sometimes it’s challenging to convince stakeholders and financial decision makers about investing in security. But now they recognize the value of the Sophos solution, because it protected us beyond measure.”

Chemi believes the experience was eye-opening.

“In terms of evolution, it started off with Opus Consulting solely talking about protecting the city’s endpoints. After spending time with David and the city as a trusted advisor, we knew it made sense to scale the solutions to the sophisticated landscape. Sophos Intercept X was another layer of protection that we added to Castlegar’s environment – and a logical choice. It simply worked by keeping the ransomware from affecting the entire city,” he asserts.

With a view to the future, Bristow plans to collaborate closely with Opus Consulting to expand the Sophos footprint by adding next-generation Sophos Firewall XG within the year. He’s looking forward to gaining additional visibility into the city’s network, users, and applications directly from the control center, which will help him solve issues proactively—before they become real problems. With Sophos Firewall XG, the City of Castlegar will further elevate its security with yet another layer of protection that will block unknown threats, automate incident response, and expose hidden risks on the network. “We know where we want to go when it comes to the Sophos solutions and working with Opus. Securing our city, our departments, and our citizens is important – with Sophos we are certain we are protecting everything just like any city would,” concludes Bristow.

Start your free trial of Sophos Intercept X today.

United Kingdom and Worldwide Sales  
Tel: +44 (0)8447 671131  
Email: sales@sophos.com

North America Sales  
Toll Free: 1-866-866-2802  
Email: nasales@sophos.com

Australia and New Zealand Sales  
Tel: +61 2 9409 9100  
Email: sales@sophos.com.au

Asia Sales  
Tel: +65 62244168  
Email: salesasia@sophos.com