ENDPOINT PROTECTION

HYDRO ONE TELECOM CAN HELP YOU TO PROTECT DATA THAT RESIDES OUTSIDE YOUR NETWORK

To mitigate the risks from data breaches, human error, ransomware and other threats, you need the ability to find, secure, protect and control all of your data—wherever it resides. With more business information being created and stored outside the data centre than ever before (on personal laptops, tablets, and other devices), protecting endpoint data outside of your network has become a priority.

With Hydro One Telecom's Endpoint Protection, powered by Commvault, you can protect and secure end-user data to mitigate risk from any number of threats. You can also regain visibility and control over your endpoint and cloud file-share data for compliance and litigation purposes—all from a single solution that can improve productivity for end users and IT through self-service, collaboration, secure file-sharing and real-time mobile access.

WHY IT MATTERS

A 2018 "Cost of a Data Breach" Study by Ponemon Institute[1] reports that the global average cost of a data breach is $3.86 million, up 6.4% from the previous year. The average cost for each lost or stolen record containing sensitive and confidential information also increased by 4.8% YOY to $148 per record.

How much does downtime cost the average business realistically? According to Gartner, the average cost is $5,600 per minute. With so many differences in how businesses operate, their verticals and their environments, the costs can tally up to about $140,000 per hour on the low end, and as much as $540,000 per hour at the higher end.[2] With such great risks, you need a solution that's flexible enough to cover your endpoint protection needs.

[1] Ponemon Institute, https://www.ibm.com/security/digital-assets/cost-data-breach-report/
[2] Gartner, June 18, 2018, https://www.the20.com/blog/the-cost-of-it-downtime/

HOW IT WORKS

HOT's Endpoint Protection Service provides 6 ways to protect your company:

1. **Encrypt stored files:** Encrypt files and folders against would-be thieves on all of your endpoint devices

2. **Control user access:** Keep data safe from fake credentials with two-factor authentication and single sign-on

3. **Remote wipe a laptop:** Full or selective wipes provide complete data security

4. **Encrypt data in-flight:** Secure data transfer protects moving data without a VPN

5. **Track that laptop down:** Geo-tracking lets you narrow down a missing laptop's location by country, province, city, postal code and street

6. **Automate security:** Allows IT to efficiently manage security for an entire mobile network

FEATURES OF HOT'S ENDPOINT PROTECTION

CAPABILITY	BENEFITS
Endpoint control and visibility	• Ensures a consistent end user experience with expedited backups and scheduling based on multiple variables (CPU, power source and network conditions), data transfer speeds and bandwidth consumption
Source-side (client) data de-duplication	• Eliminates redundant data from the client before copying to the server • Reduces server-side storage space, which lowers bandwidth consumption, speeds backup process, and helps to reduce costs.
Optimize security and data loss prevention (DLP)	• Secure data at the endpoint, in transit and in the data centre (with SSL encryption) and at rest (via AES, Blowfish, 3DES and Ghost) • Encrypted at the file- and folder-level with proprietary FIPS 140-1 and 140-2 certified modules • Other capabilities include device geo-location tracking and lock-and-wipe
End user self-service data restore	• Enables end users to search, view and restore their own files and folders from Windows Explorer, Mac Finder, Android/iOS mobile apps, or a web interface
Simple control point for access control and authentication	• Granular, role-based access control (RBAC) based on Active Directory, Domino Notes Directory or LDAP • Commvault two-factor PIN authentication is available • Single sign-on (SSO) support via Windows credentials, SAML and social media sites with OAuth
User-friendly backup policy, workflow automation and reporting	• Reduces IT admin burden with a library of basic tasks, customization capabilities and sautomated workflows • Endpoints are auto-detected to eliminate manual installation and configuration • Real-time visibility into all running jobs and events with customized alerts • Customizable and out-of-the-box reports and graphical dashboards
Accelerated search, compliance and e-discovery operations	• Full-text indexing and searching against a single pool of data from all laptop and desktop users and several cloud repositories accelerates the identification of responsive data for legal hold, compliance audits and investigatory operations • Legal hold (files and devices) workflow automation simplifies the process of ensuring electronically stored information (ESI) preservation
Virtually unlimited scalability	• Scales easily from hundreds to hundreds of thousands of users and from a single location to hundreds of locations globally with an agile and web-scale platform
Deployment options	• Deployment options include on-premises, public/hybrid cloud and SaaS
SaaS app backup	• Sync, store and share with G Suite by Google Cloud and Microsoft OneDrive
Licensing options: • Endpoint data protection • Search add-on	• Backup, restore, data loss prevention • Metadata search and reporting (per user) • Advanced content-based search and legal hold (per user)