SECURE SD-WAN

HYDRO ONE TELECOM CAN FUTURE-PROOF THE NETWORK ARCHITECTURE OF YOUR DIGITALLY TRANSFORMED ORGANIZATION

The spread of digital technology has brought profound changes to the ways that companies operate and deliver value to their customers. Today's digitally driven workplaces demand speed, precision and collaboration from their employees, from headquarters to branch offices, and employees need real-time access to data, resources and critical business applications, including automation and cloud computing platforms.

Legacy Wide Area Network (WAN) services, often based on MPLS, Ethernet and Private Line connectivity, just can't keep up. They're complex, costly and designed to serve traditional client–server networking models where all branch office data traffic, including Internet traffic, is routed back to the main, privately hosted data centre site. This may be necessary for some enterprise data, but it adversely affects latency and network costs. As businesses host more applications on the public Internet, this legacy network topology becomes prohibitive.

Hydro One Telecom's (HOTs') Secure Software-Defined Wide Area Network (SD-WAN) solution deploys a hybrid network architecture that integrates legacy WAN services with direct and secure branch-to-Internet connectivity—bypassing the need to route all network traffic back to the main site. The resulting network provides both cost effectiveness and increased performance while mitigating cybersecurity vulnerabilities.

WHY IT MATTERS

HOT's Secure SD-WAN is a fully managed service that provides customers with convenience and peace of mind, so they can keep up with the pace of digital change. It's an ideal solution for Canadian companies that are switching from legacy WAN to SD-WAN services, or for those wishing to do so. And since cybersecurity is an integral component of HOT's Secure SD-WAN offering (unlike most other SD-WAN solutions on the market), you can feel confident that your critical data is being routed efficiently, safely and at a fraction of the cost of traditional connectivity. With "zero-touch" provisioning, the on-site effort to get HOT's Secure SD-WAN systems up and running is reduced, making network implementation, changes and policy updates significantly faster than with legacy WAN networks. Plus, because Secure SD-WAN makes use of broadband for customer–site connectivity, it can be installed virtually anywhere. It's that simple.

HOW IT WORKS

Powered by top-rated cybersecurity provider Fortinet, HOT's Secure SD-WAN solution combines a number of technologies from today's most powerful WAN Edge devices, including routing, load balancing, Quality of Service (QoS), traffic shaping and Next-Generation Firewall (NGFW) cybersecurity. Delivered as a fully managed service using Fortinet's cloud-based tools, HOT's Secure SD-WAN solution automates service provisioning and implementation, while advanced monitoring tools enable proactive management and troubleshooting for network and cybersecurity incidents.

HOT's fully managed Secure SD-WAN service packages provide industry leading SD-WAN/cybersecurity integration.
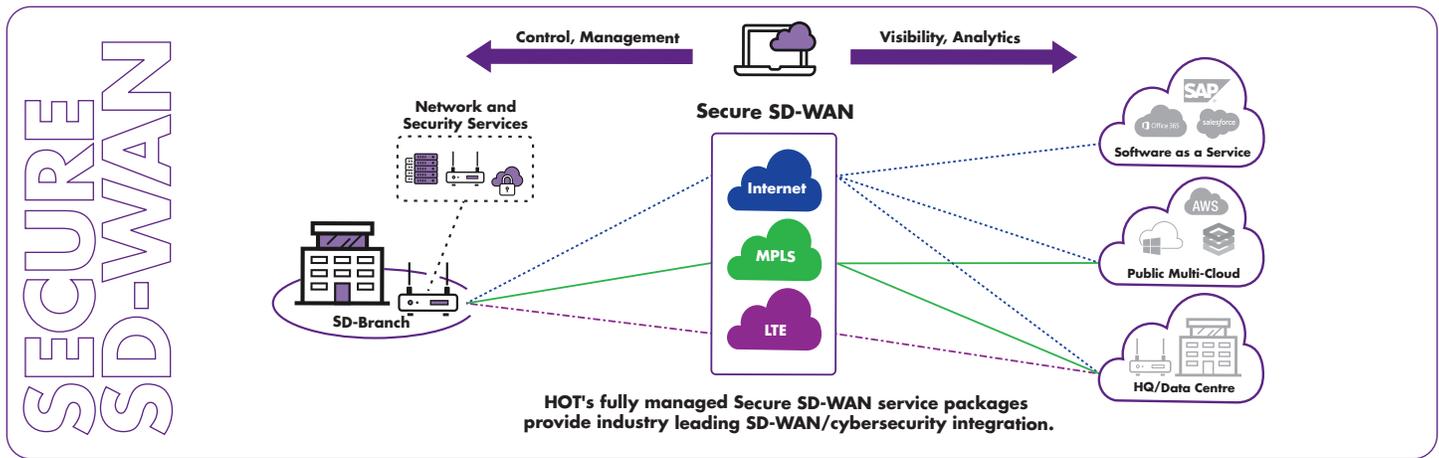
FEATURES OF HOT'S SECURE SD-WAN

Choose from three Secure SD-WAN Service packages:

Features	Secure SD-WAN	Secure SD-WAN with Essential Unified Protection	Secure SD-WAN with Advanced Unified Protection
Customer premises equipment	•	•	•
WAN broadband connectivity	•	•	•
SD-WAN	•	•	•
Stateful NGFW	•	•	•
Managed services	•	•	•
SLA-backed services	•	•	•
Detailed reporting portal	•	•	•
DNS and IP reputation filtering		•	•
Intrusion prevention systems		•	•
Optional log retention and reporting		•	•
Optional SSL inspection		•	•
Anti-virus and sandboxing			•
Application control			•
Web/URL filtering			•

BENEFITS OF HOT'S SECURE SD-WAN

Unified Networking Solution	Application-Aware Routing	Multi-Link Control
Simplifies WAN Edge within one unified solution that delivers SD-WAN and cybersecurity functionality.	Intelligently identifies applications and routes traffic based on defined policies per application and current network conditions.	Uses one or more WAN links simultaneously for carrying application traffic (per defined policies) for bandwidth on demand.

Cloud-Based Automation	Zero-Touch Deployment	Real-Time Dashboard
Configuration through software-defined policies ensures rapid network implementation and faster change management.	Significantly faster deployments at scale and simplified operations at the WAN Edge.	Provides customers with access to WAN link utilization and QoS performance.

End-to-End Security	Site-Specific Security Implementation	Service-Level Guarantees
Inter-site traffic is encrypted end to end using IPSec VPN technology, significantly reducing risks from cybersecurity threats.	Apply site-specific security policies based on user needs, IT resources and business output requirements.	SLAs cover Service Availability/Uptime and Mean Time to Repair.