TELUS Business | paloalto NETWORKS

The traditional security perimeter is disappearing: close the gaps with TELUS Managed Cloud Security

Achieve consistent security across your entire network

Table of contents

Introduction

Rapid cloud adoption and the rush to enable remote work have opened new security gaps that organizations have struggled to close. To meet these evolving security needs, TELUS has developed a new fully managed cybersecurity solution that simplifies securing evolving environments and addresses these gaps.

Shri Kalyanasundaram, TELUS' Director for Cybersecurity and Digital Identity Solutions, says, "The rapid adoption of new technologies and the shift to a hybrid work model has changed the risk profile of organizations. As a result, the cyber risks you're facing today are not the same as they were pre-adoption, and investments need to be made to close those gaps. Comprehensive cybersecurity solutions that secure access to all applications and data regardless of where they are stored and no matter where users are working from, help improve an organization's risk profile while ensuring the right people have secure access to your environment, applications, and data."

The way we access data and applications is changing

Software-as-a-Service (SaaS) applications have opened up new, affordable services delivered from the cloud, and most organizations have adopted at least one SaaS platform. Organizations are also moving workloads to the cloud to gain efficiency and flexibility. According to Flexera[1], 87 percent of all enterprises now have a hybrid cloud strategy, indicating that cloud adoption is becoming mainstream. Jason Georgi, Field CTO for Prisma Access at Palo Alto Networks, says, "As organizations look to do more with the cloud, they are looking to provide secure connectivity with consistent, great user experience wherever users are working from and anywhere the apps reside."

The global pandemic accelerated the pace of change. Organizations needed to quickly enable remote work on a mass scale, nearly overnight. "With the onset of the pandemic, a lot of organizations' remote access services were strained due to capacity limitations. So, they were forced to make difficult decisions around sending some traffic directly to SaaS, circumventing VPN." In many cases, he says that while this helped address performance and capacity issues, it opened a new security gap—a gateway to malware. But organizations absorbed the risk of increased exposure to stay operational.

Even though people are returning to the office, remote work will persist. According to Gartner, Inc.[2], "Forty-eight percent of employees will likely work remotely at least part of the time after COVID-19 versus 30 percent before the pandemic." And with more workloads, applications, and data moving to the cloud, organizations are looking for better ways to enable secure anywhere access for employees, contractors, vendors, and others, and to secure data and applications that may be stored anywhere. Organizations are now looking to get the lost visibility and security back, but they need to be able to do it at scale for a dynamically changing workforce. The hybrid workforce is driving that.

87%

of all enterprises now have a hybrid cloud strategy.[1]

48%

of employees will likely continue working remotely at least part of the time after the pandemic.[2]

Traditional security cannot close the gaps

When users, data, and applications were within the data centre perimeter, organizations had the right security in the right place. As data moved out of the data centre and users moved out of the office, organizations had adequate security in one place - the data centre - but outside of it, their security protections were inadequate.

This situation resulted in security gaps that cyber criminals are aware of and are using to their advantage—gaps that legacy security solutions weren't designed to handle. Georgi says, **"When you send hundreds or thousands of people home, the first network they use to access any resource is the Internet, which is not a private or controllable network. It opens up threat vectors."**

Traditional VPN isn't the answer

In most cases, traditional VPN lacks the necessary built-in security and can also lack capacity because it's not designed to scale up to meet the needs of hundreds or thousands of remote users working at full capacity. For example, using VPN to secure SaaS activity erodes performance because access is routed from the user into the data centre, then out to the application. To get better performance, many users opt to access SaaS applications directly through a standard Internet connection, circumventing a secure remote connection. The tradeoff is that this activity isn't secured.

Legacy solutions are costly and cumbersome to maintain

Legacy security solutions require significant manual effort to deploy, manage, and maintain and don't scale easily. Adding new capabilities to handle decentralized users and data adds incremental complexity that, over time, can become costly.

Too many products, too many vendors

According to a report by Gartner, "2021 Strategic Roadmap for SASE Convergence[3]," "Perimeter-based approaches to securing anywhere, anytime access has resulted in a patchwork of vendors, policies, and consoles creating complexity for security administrators and users." Kalyanasundaram says, "This patchwork of solutions means resources spend too much time wading through different systems in their day-to-day work. Consolidating down to as few screens as possible enables resources to better understand what's in their environment, manage who has access and proactively address their risk profile." In addition, patchwork solutions can introduce new security gaps that may go unnoticed.

A managed service can not only remove the complexity of managing a variety of security solutions, but also leverages the collective expertise of a managed service provider like TELUS to guide customers in their transformation journey.

Threat landscape is evolving

Hacking for profit is now a huge industry. Cyber criminals, including state-sponsored hackers, are using increasingly sophisticated methods to scale their activities. And **when the pandemic hit, hackers made hay with the situation taking advantage of the new vulnerabilities presented by remote work and unsecured Internet and cloud activity.** Since the threat landscape is continuously evolving, no one can predict what threats will emerge tomorrow, making proactive security a top priority.

Accelerated digital transformation

As organizations continue to adjust to new ways of working and turn to the cloud for modernized resources, **enterprise networks will continue to evolve and change, with more devices**—including bring-your-own-device arrangements—connecting to more applications from locations around the country. As the network evolves, so does the attack surface, giving threat actors different ways to intrude.

The security industry is moving in a new direction

As business priorities shift and the threat landscape evolves, the security industry works to stay in-step with these changes. Rapid cloud adoption and remote work have expanded the traditional security perimeter beyond the four walls of the data centre and office building. Karan Chopra, Manager, Cybersecurity Products and Services at TELUS, says, "With the advent of more cloud-based services such as SaaS solutions, you're no longer managing data and applications within the legacy perimeter. You're now going way beyond that. You want to make sure that the data your employees are accessing is secured consistently wherever they are."

As users, applications, and data become increasingly more decentralized, legacy networking and security approaches —designed to secure data in the data centre and users in the office—have fallen short of their ability to secure everything everywhere without significant erosion in network performance and user experience. That's because elastic security designed to stretch around the new perimeter wasn't available.

While VPN saved the day for many organizations, traditional VPN wasn't designed to scale up to handle the amount of traffic that resulted from the mass exodus from the office, and its security controls are too primitive to protect data and users in the new environment.

IT spending shifting to the cloud will accelerate

66%
of surveyed IT leaders say they will continue to increase overall use of the cloud.[4]

82%
of surveyed IT leaders say cloud use increased in direct response to the pandemic.[4]

45%
of surveyed IT leaders say they plan to accelerate their cloud migrations.[4]

What to look for in a modern security solution

With applications and data no longer centralized in the data centre, and users no longer centralized in the office, **organizations need a security solution that enables users to safely access applications** in the cloud, data centre, and Internet regardless of where they are working.

A flexible, cloud-delivered security model provides the ability for organizations to secure and manage access to all applications and data regardless of where they are stored and no matter where users are working from with unified controls and comprehensive visibility across your network.

To secure all apps, data, and traffic with a cloud-based solution, a modern cybersecurity platform should provide the full security stack anywhere it's needed, and include these capabilities, which can close common security gaps that result from an expanded security perimeter:

- Fully inspect and secure access to all Internet and private application traffic according to your policies using machine learning for threat prevention and data loss
- Provide elastic security that stretches around the new, dynamic perimeter to protect users regardless of where they work, and to protect data, regardless of where it's stored
- Isolate personal and business activity to close a common gateway to malware
- Converge security with networking using Secure Access Service Edge (SASE) when combined with SD-WAN
- Apply unified security policies to all users
- Eliminate complex and inconsistently enforced security for remote users
- Prevent unknown threats in real-time without compromising performance
- Offer a unified approach to user experience, visibility, control, and security

TELUS Business | paloalto NETWORKS

Consolidation of features

To combat product sprawl and incremental complexity, a modern security solution should consolidate multiple security capabilities into a single cloud-delivered platform, including:

Firewall-as-a-service (FWaaS)
Protects inbound and outbound traffic with native user authentication and access control.

Secure web gateway (SWG)
Protects users from web-based threats and includes URL and content filtering.

Zero-trust network access (ZTNA)
Remote access connectivity, which protects remote users and the resources they access regardless of their location by enforcing granular role-based access control.

Consolidation of policies

To provide a consistent security posture across the network, your cloud-based security platform should consolidate disparate security policies into one customizable policy that governs all access.

Scalability and performance

A modern security solution should also scale rapidly, up or down, across all use cases with low latency to meet the dynamic needs of changing organizations. To ensure low latency for the best user experience, a modern solution should eliminate routing web traffic through the data centre with traditional VPN by inspecting data at its source, or at the “edge.”

The solution: TELUS Managed Cloud Security

To create a solution that best addresses these challenges, TELUS chose to build a service based on Palo Alto Networks Prisma® Access, the most comprehensive cloud-delivered security platform that protects traffic, applications, and users across all locations. Based on this innovative technology, TELUS Managed Cloud Security enables organizations to consolidate multiple security solutions into one platform, reducing the number of vendors and technologies, and simplifying administration with one interface. This gives organizations the flexibility and scalability they need to support their businesses as they evolve.

TELUS Managed Cloud Security enables consistent security that stretches around your entire perimeter, allowing your organization to enable cloud adoption at your own pace. TELUS Senior Cybersecurity Architect, Guri Chattha, says, “We make it simpler for the customer by packaging it all into an easy-to-understand managed cloud security service.”

Cloud VPN for ubiquitous security

The TELUS Managed Cloud Security approach to elastic security is VPN-based, where users connect to network resources using a standard IPsec connection, enabling the service to do a full inspection of network traffic for threats and data loss. Rather than the traditional VPN method of routing all traffic to a data centre that may be hundreds of miles away, users connect to a cloud resource that’s much closer, providing exceptional performance. Users won’t be motivated to turn VPN off for better performance on the web.

SASE for unified consistency

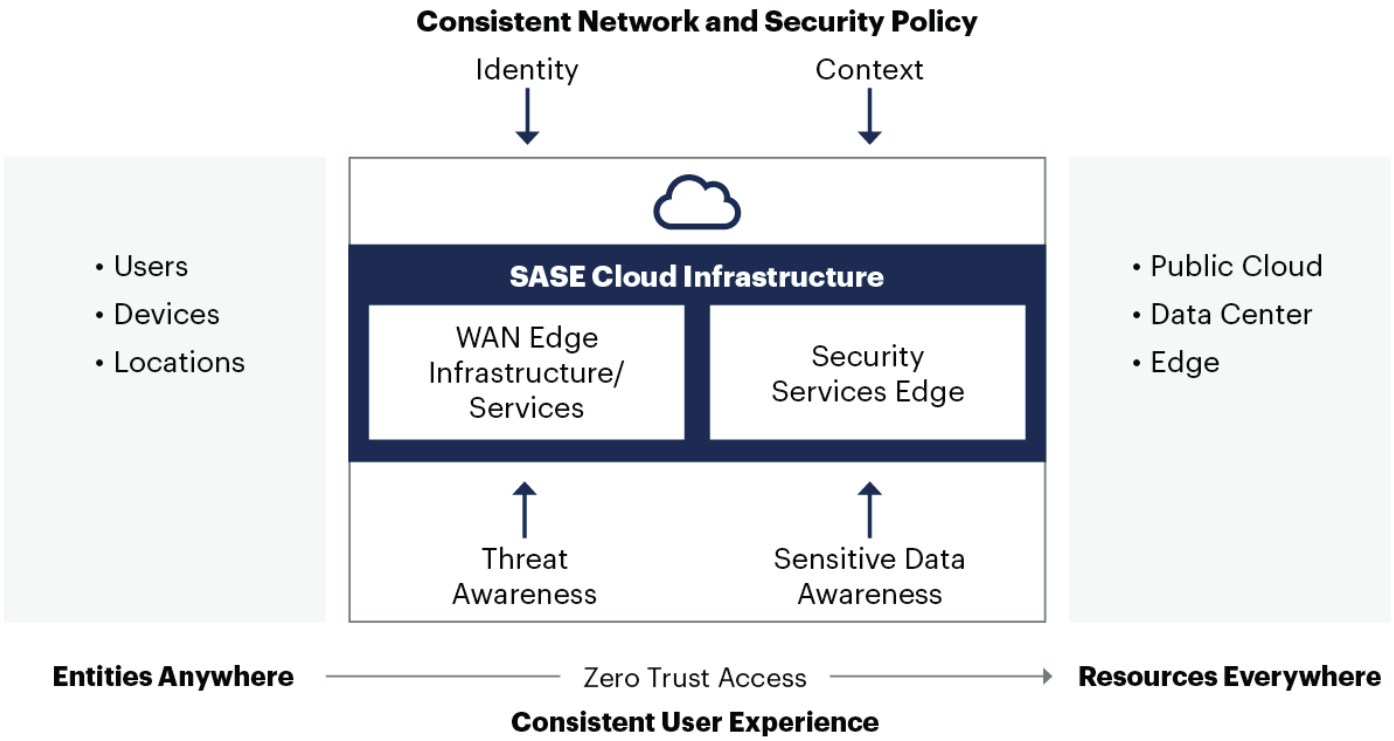
To deliver a consistent, unified security posture across the entire network, when paired with SD-WAN, TELUS Managed Cloud Security merges networking with security using a SASE approach.

SASE merges networking and security at the edge to embed security into your Internet traffic, making it a safer place to do business. Instead of routing all traffic into the data centre to be secured, SASE secures information at its point of origin, whether it’s the data centre, a SaaS application, or the user’s home broadband Internet connection. In this way, SASE is able to better secure remote workers and data.

When evaluating vendors, keep in mind that not all SASE is created equal. According to Gartner, Inc.[3], "Some SASE offerings only focus on cloud-delivered security edge services and avoid SD-WAN. Likewise, some SASE vendors focus on SD-WAN, and have only basic security capabilities for cloud-delivered security edge services." TELUS Managed Cloud Security offers a comprehensive SASE solution that gives organizations the ability to seamlessly merge SD-WAN networking with security to fully enable business transformation and secure the hybrid workforce.

TELUS Managed Cloud Security offers a solution that seamlessly merges SD-WAN, giving organizations the ability to combine networking with security to fully enable business transformation and secure the hybrid workforce.

Secure Access Service Edge



Source: Gartner
741491_C

Gartner

Additional benefits

Consolidating security in the Cloud with TELUS Managed Cloud Security can save time, enable innovation with the cloud, and future-proof for inevitable changes.

Consistent security with fewer policies to manage

TELUS Managed Cloud Security helps reduce security gaps and policy errors by consolidating disparate policies into one unified policy, which is applied to every user regardless of their location. With fewer policies to manage, organizations have a more consistent security posture across the network.

Less hardware to operate

TELUS Managed Cloud Security alleviates the need for organizations to purchase and manage the lifecycle of various hardware-based firewall solutions, reducing the need for extensive capital investments and helping organizations manage their budget more effectively.

Predictable cost

Partnering with TELUS allows organizations to pay a predictable cost, making budgeting for security tools much easier.

Accelerates cloud adoption

As more resources, data, and workloads migrate to the cloud, a cloud-based security solution enables and accelerates cloud adoption, giving organizations the ability to easily adapt to future needs as the organization grows or changes.

Enables secure remote access at scale

One of the most important benefits of a cloud-based security solution is the ability to enable secure remote access at scale for a hybrid workforce, including remote employees, contractors, partners, vendors, or anyone else who has an authorized need to access your online resources.

Adapts for the future

As a cloud-based service, TELUS Managed Cloud Security can easily scale up or down as your organization expands or changes.

What to look for in a technology partner

The TELUS advantage

TELUS offers a comprehensive cybersecurity portfolio, consisting of Managed Security and Professional Services, designed to help organizations manage their security environment, mature their security posture, identify and respond to threats, and restore normal operations.

As a trusted partner, TELUS leverages our expertise and security services to deliver the cybersecurity outcomes organizations need. We do this by drawing on our extensive experience managing security for hundreds of Canadian organizations along with our own complex security environment. With our depth of capabilities, we can implement, optimize and audit an organization's security policies along with managing and monitoring their overall security posture.

As a national telecommunications service provider, TELUS can provide an integrated secure connectivity solution by combining our TELUS Managed Cloud Security and Network as a Service offerings. This allows TELUS to function as a single point of contact to organizations for all their managed network and security needs. The Managed Cloud Security service can also be integrated with an organization's existing connectivity solutions.

Organizations benefit from our long standing relationship with Palo Alto Networks and our extensive expertise supporting their technology. As a Palo Alto Networks Diamond Innovator, TELUS has met stringent training requirements, making us the most certified partner in Canada.

As a Palo Alto Networks Diamond Innovator, TELUS has met stringent training requirements, making us **the most certified partner in Canada.**

The Palo Alto Networks Prisma® Access Advantage

Prisma Access is designed from the ground up to lower the costs and complexities of securely connecting users and devices to any service required, anywhere. The cloud native architecture of Prisma Access ensures on-demand and elastic scale of comprehensive networking and security services across a global, high-performance network.

Prisma Access provides the foundation for consistent cloud-delivered security for all users and locations, including:

- **Superior protection** for all applications and data by securing remote access to all privileged data across web and non-web-based traffic, reducing the risk of data breaches.
- **Complete best-in-class security** with industry-leading capabilities converged into a single cloud-delivered platform, providing more security coverage than any other solution.
- **Optimized user experience** built on a massively scalable network with ultra-low latency and backed by industry-leading SLAs, ensuring the best digital experience for end-users.

Palo Alto Networks enables organizations to transform their infrastructure with the most complete SASE offering while realizing a market-leading ROI of up to 247 percent. Palo Alto Networks SASE solution combines a global high-performance network to simplify the delivery of consistent security at scale while ensuring an optimal work from anywhere experience.

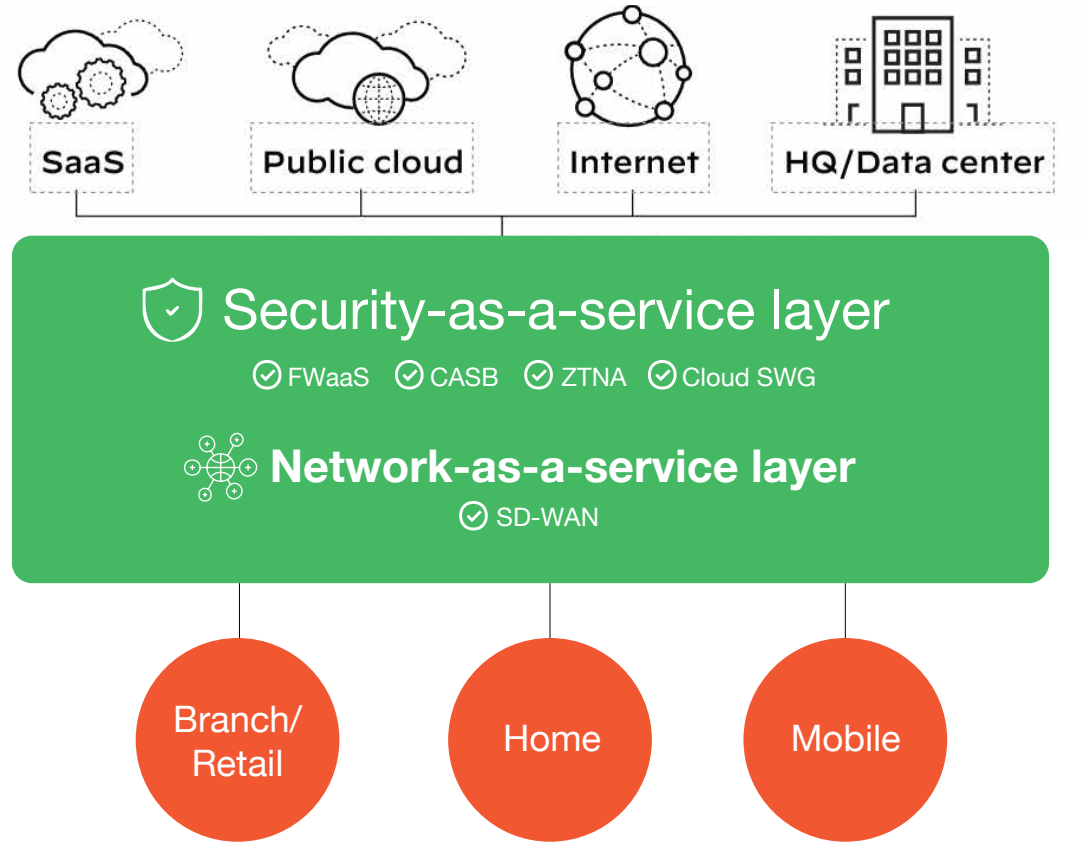


Figure 1: Prisma Access architecture

About TELUS

At TELUS, we are committed to using our world-leading technology to create meaningful change. By reinvesting 5 percent of our profits back into our communities, connecting Canadians in need and committing to become a zero-waste, carbon neutral company by 2030, we hope to make the world a better place. To help make cybersecurity more accessible, we established TELUS Wise, a free digital literacy education program that offers workshops and resources to help Canadians of all ages stay safe in a digital world.

As a cybersecurity leader and national telecommunications service provider, TELUS is well positioned to offer a unique perspective on the security threats and trends businesses face today. We leverage our 20+ years of experience securing our own employees, national network, and customers across Canada to help organizations achieve their desired security outcomes. We are one of five companies in Canada (and the only telecommunications and security provider) to have secured the “Global Privacy and Security by Design” certification.

For more information, visit **www.TELUS.com/cybersecurity**

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. Palo Alto Networks helps address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.

For more information, visit **www.paloaltonetworks.com**

Sources

1. https://www.flexera.com/about-us/press-center/flexera-releases-2020-state-of-the-cloud-report.html
2. Smarter with Gartner, 9 Future of Work Trends Post-COVID-19, April 29, 2021
3. Gartner, 2021 Strategic Roadmap for SASE Convergence, Neil MacDonald, Nat Smith, Lawrence Orans, Joe Skorupa, 25 March 2021
4. https://www.computerweekly.com/news/252484865/Coronavirus-Enterprise-cloud-adoption-accelerates-in-face-of-Covid-19-says-research

TELUS.com/cloudsecurity

TELUS Business | paloalto NETWORKS

Cybersecurity that works for you.

Looking to learn more about how TELUS can help deliver the cybersecurity outcomes you need?

Contact us today