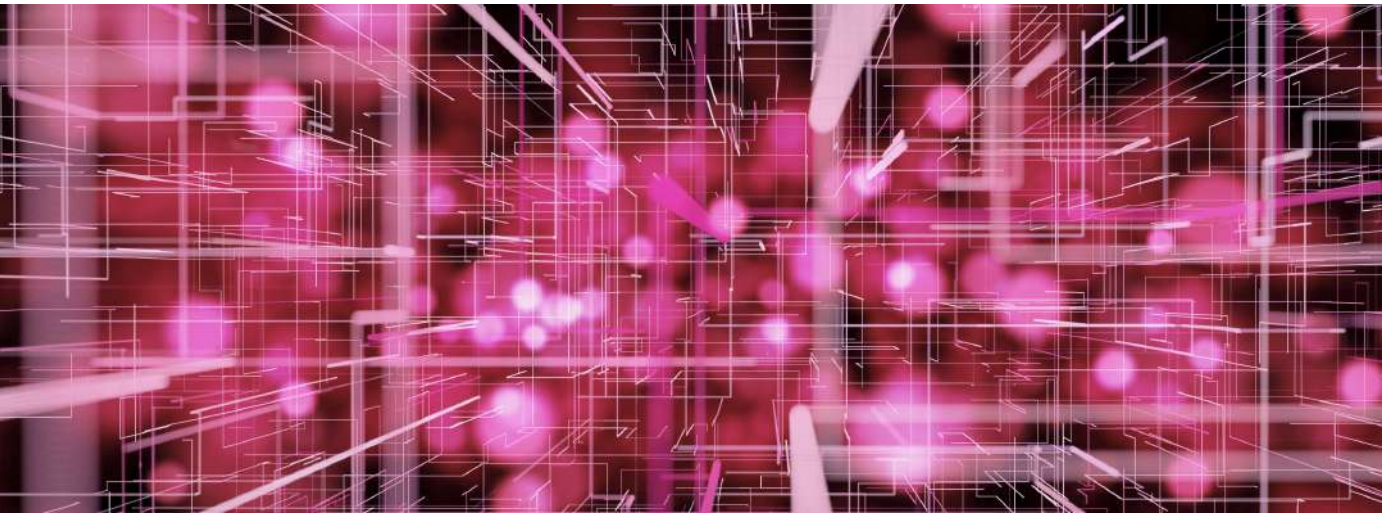
SD-WAN at the forefront:
Securing the modern enterprise edge

The threat landscape growing broader and more complex, and traditional security solutions are increasingly falling short of enterprise demands. With a growing arsenal of next generation advancements, the WAN edge has become a hotbed of innovation and reimagination.

A Frost & Sullivan Executive InfoBrief

FROST & SULLIVAN

Singtel | Trustwave®



01 Examining the role of SD-WAN in an increasingly distributed application ecosystem

The implications of rapid cloud adoption on enterprise networks

With digitalisation at the forefront of the personalised experience, a rapidly growing service backbone of bandwidth-intensive applications is straining monolithic, legacy corporate networks:

> End users are demanding the golden halo of price, speed and reliability.

> Businesses are leaning heavily on smart collaboration services and cloud applications to meet consumer demands faster, and to manage employee expectations better.

> The reliance on Voice over Internet Protocol (VoIP) and videoconferencing is higher than ever, driving enterprises to look for connectivity solutions that are cost-effective, easily managed and dependable.

This is nudging even slow-moving enterprises in the right direction to trim the fat, shave off costly legacy network infrastructure, and invest in secure and reliable connectivity.

The hybrid network era: A vital driver for reimagined, reengineered cloud security

The modern enterprise has an infrastructure footprint that, more often than not, spans over hundreds of geographically dispersed locations. Enterprises with clunky, traditionally physical network architectures are increasingly mixing in virtual infrastructures for easier scalability, bandwidth, cost, and enhanced reliability efficiencies. This is no longer something only IT and security functions are demanding - business development teams are flagging agile, immediately accessible service networks as competitive kryptonite. Consumers are now, more than ever, extremely sensitive to SaaS application downtime, VoIP drops, and network degradation issues in any form.

This very same digitalisation has brought about a multi-cloud universe, into which enterprises are transmitting huge amounts of complex, extremely private data through vast networks of public, private, and hybrid clouds. The usage of the internet across the globe has spiked, even within traditionally 'offline' consumer markets and industry sectors. As a result, business decisions have to factor in the reality that unstable networks and security breaches cause customer churn and organisational inefficiencies that cannot be easily or immediately recovered.

Looking forward: The urgency behind dynamic, scalable and flexible security

The WAN edge has become a necessary backbone to the transformation roadmap, but this layer can only be as effective as the enterprise's security posture. The complexity of managing every edge endpoint - along with overlapping point products and applications - exponentially multiplies this challenge:

> Branch offices that often don't have their own onsite IT staff are struggling with the risks that come with an explosion of edges, especially with the volume of business-critical SaaS applications;

> Due to an exponential uptick in the bring-your-own-device (BYOD) culture, an expanding remote workforce and the rising commercial usage of Internet of Things (IoT) devices, end users are connecting a growing number of unmanaged devices to internal networks.

02 Why is cyber security vital?

A 360-degree view of the modern attack landscape

With cloud and digital technologies on the rise over the past decade, businesses were already tasked with guarding the entire scope of their digital presence over virtual networks in addition to their internal networks. Now, with the enormous explosion of devices brought on by employees working from home, today's security challenges are framed by a new objective: to extend the boundaries of cyber security beyond corporate firewalls. Insights from Trustwave's latest Global Security Report[1] point to a few particularly leading trends:

In 2019, incidents involving cloud services more than doubled to 20 percent of overall incidents, catalysed by the growing popularity of services such as Amazon Web Services and Microsoft Azure.

The largest share of incidents involved ransomware, which more than quadrupled to 18 percent of incidents in 2019.

The organisational attack surface has massively increased, making it even more necessary for security efforts to holistically span from the core, to the edge, all the way to the cloud.

Battling complexity and empowering IT teams with a holistic managed security service

Enterprises are increasingly choosing to offload key security services to experienced partners that can provide both co-managed or fully managed security services. Picking the right partner - whether simply for an initial advisory overview or for a fully managed relationship - can help enterprises select tailored security approaches that allow them to meet their custom cost, data privacy and application performance benchmark objectives.

In thinking of the benefits of managed, unified security solutions, simplification is the biggest one. Outdated methods of building separate security strategies for each edge environment usually spells disaster for overwhelmed IT teams. Building smarter, lightweight strategies revolve around seeing each edge as part of a bigger security strategy where:

- Security is extended to branch and other remote locations
- Consistent, reliable security processes are applied over all edge environments
- Centralised mechanisms are in place, controlling the entire distributed network's management, visibility and operational expenses from a single view pane.

03 Graduating from simple to strategic, secure network transformation

From complexity to simplification: Unified security for the digital network

A unified security approach is able to mitigate the challenges brought on by point solutions that lack the visibility and control required to enable data-informed decision making processes. Without the cautious layering of security and strategy, enterprises will continue to be saddled with messy, vulnerability-ridden monoliths of fragmented products with high circuit costs.

CTOs and CIOs must step back, relook at their old technologies versus their newly digitalised ones, and work towards extracting and merging the pros and cons of each to purposefully retrofit their infrastructures to accommodate the needs of today's reality. There are three main dimensions under consideration here: people, processes, and technology.

Leveraging SaaS, PaaS and IaaS: For true, deliberate cloud-readiness

Even before COVID-19 escalated, businesses that had built their core systems on top of legacy IT infrastructure found it very challenging to spin up new services, scale services and staff, and maintain the service levels their customers were demanding. Assets within SaaS, IaaS, and PaaS platforms hence become a mission-critical business necessity. Powered by these tools, enterprises found themselves able to:

- **Scale services faster**
- **Empower their employees with smoother collaboration tools**
- **Identify target customer segments and generate faster, more customised solutions for them**
- **Enforce truly agile business continuity processes**

Prioritising experience: Transformation as a critical employee performance enabler

The volume of data being introduced into enterprise networks today is scaling exponentially, bolstered by larger active user bases and growing customer adoption of digital services. The consequences of this data explosion bring up important considerations for today's CIOs and CISOs:

From the different network layers at play, WANs are open to a high level of risk by function of their role connecting global sites and dispersed cloud infrastructure. With just a singular WAN breach, the enterprise's entire network can be compromised. It is hence all the more important that integrated security solutions factor in the WAN layer as a critical component of the network edge, in addition to mobile endpoints, the core and the cloud.

In a strategically focused security implementation, the endpoint is each user, device, or application, instead of just the data centre infrastructure covering the enterprise campus and extended branch network.

CTOs and CIOs must relook at their old technologies versus their newly digitalised ones, and work towards extracting and merging the pros and cons of each to purposefully retrofit their infrastructures to accommodate the needs of today's reality.

Strategic agility: Security as a catalyst for streamlined operational efficiency

By crafting policies and standards that merge objectives across these three dimensions, successful CXOs can stabilise their teams and boost bottom lines by:

- **Shifting from monolithic technology stacks to flexible, dynamic combinations of cloud, micro services, and democratised data access;**
- **Moving from monolithic organisations to smaller, cross-functional, self-organising teams;**
- **Breaking down huge, complex processes with long project timelines to smaller, modular projects run using agile methods to allow for iterative improvements;**
- **And finally, from a security standpoint: reshaping security priorities and adapting threat detection models to factor in new service delivery structures that can address remote and elastic workforces.**

03 A checklist of secure SD-WAN considerations

Evaluating the acceleration of your enterprise into the cloud

Just like any fundamental change in networking architecture, cloud adoption comes with risks that could range from transition errors and security blind spots, to the potential loss of critical data. The single biggest concern is often security, hence the following handy checklist for laying out a SD-WAN implementation strategy:

- [ ] **Resource planning**
  This varies from enterprise to enterprise, but for IT departments that do not have the resources to manage SD-WAN networks, consider roping in a managed services provider that can guarantee service levels to fit your exact business needs and performance sensitivities.

- [ ] **Secure the cloud edge**
  With business-critical applications running over the cloud across large networks of branches, securing the cloud edge is critical. A question for your SD-WAN provider: does their technology provide an exhaustive edge shield with centralised control? Does their platform enable seamless management over both network and security, and across both branches and cloud?

- [ ] **Unify the security layer**
  Ideally, the SD-WAN technology you choose will allow for unified threat protection, leveraging intrusion protection, Domain Name System (DNS) security layer, zero trust security models and threat intelligence to protect the entire connected enterprise network.

- [ ] **Plan for long-term compliance**
  The security and compliance space for just about every industry has been changing drastically over the past 10 years, and there's no stopping this trend just yet. Attacks are getting smarter, and there is immense scrutiny on how businesses are storing, processing and reporting on sensitive data. Your clients and partners care about this, and this can make or break large deals with B2B customers in highly regulated industries like government, banking and healthcare. CIOs need to ensure that technologies they choose today are ready to evolve with changing business needs over the next decade, and can allow for flexible future-proofing.

Streamlining cyber-security amongst your branch offices and remote workforces

Theoretically, adding networking and security technologies right at the branch locations might help manage these issues but, in reality, most teams cannot afford to deploy IT resources onsite to manage these solutions, even temporarily.

With SD-WAN solutions, security vendors are edging to the frontlines of competition by future-proofing their secure SD-WAN offering so that enterprises get the whole package in one solution. On a product-level, this will mean an integrated security solution for the WAN and Access Edge, that accounts for traffic scanning, security enforcement, zero trust access control for wired and wireless connections, IoT device recognition, dynamic segmentation, and integrated management in a single low-touch/no-touch device.

Assessing your network's ability to quickly and dynamically adapt to changing business requirements

In its broadest definition, a secure SD-WAN solution will cover three key domains: data protection; user, device and application control; and, security control and threat protection. This exhaustive trio of functionality spans from data loss prevention, to authentication and access control, application security, unified security enforcement, firewalling, intrusion detection and prevention - all the way to Distributed Denial-of-Service (DDoS) and advanced malware protection.

With this, an enterprise client will not have to worry about the nuts and bolts of all pieces of their implementation - in a single sweep, they will be able to deploy, maintain and protect their far-flung WAN networks.

For enterprises that want to empower themselves with agile, dynamic scalability, simply bringing in a pure-play SD-WAN is not enough. Vendors who offer barebones SD-WAN solutions typically only offer security features that span Layer 1 to Layer 3 at the most. Without a more advanced solution, the step forward that SD-WAN provides could easily become three steps backwards if the new vulnerabilities were exposed in a damaging security breach. Enterprises need to, as part of their WAN evaluation strategy, look into full stack solutions that apply the key tenets of SD-WAN from the core, to the edge, to the cloud.

Simplify and secure with Singtel's managed SD-WAN

Singtel's secure Managed SD-WAN comprises Managed Detection (MD) and Security Technology Management (STM) services, powered by Trustwave, a Singtel company. This combination of services addresses the growth in SD-WAN take-up - driven by the promise of greater flexibility and cost savings - largely through hybrid WANs that augment existing MPLS networks.

With these, organisations can accelerate and embrace digital transformation securely - with assurance that its security posture is boosted, maintained and refined continuously.

Management solutions revolve around:

- **Detecting malicious traffic that traverses through the SD-WAN network 24x7**
- **Implementing robust, data-driven security policies on the SD-WAN edge device powered by the latest threat intelligence**
- **Exponential operating expense (Op-Ex) savings due to enhanced flexibility, security and business agility**
- **Easing the load on thinly stretched IT teams with share co-management of critical security responsibilities**

FROST & SULLIVAN

Singtel | Trustwave®