Architecting a Secure Business-Driven SD-WAN

Learn How Unity EdgeConnect Delivers Unmatched Protection Across the Cloud-Connected Enterprise WAN

EXECUTIVE SUMMARY

Software-driven wide area networks (SD-WAN) are enabling today's geographically distributed enterprises to realize the transformational promise of cloud computing, reduce capital and operating costs, provide the highest quality of experience for employees and customers, and adapt quickly to changing business requirements.

But cloud computing and business-first networking introduce new security challenges. These include:

- Protecting data in transit across public network links
- Directly connecting users in branch offices to applications using the internet ("internet breakout")
- Overcoming a lack of visibility into dynamic application environments
- Complying with requirements for network and application segmentation

A key benefit delivered by an SD-WAN is the ability to actively utilize low-cost broadband services. However, because broadband services are "public" instead of "private," advanced security capabilities are required to ensure the confidentiality and integrity of application traffic traversing such connections. By segmenting networks into zones that span LANs and WANs, SD-WANs isolate traffic and minimize the attack surface to help compliance with industry standards.

This paper discusses why enterprises are embracing SD-WAN platforms at an accelerating pace, and how a comprehensive SD-WAN security deployment can better safeguard today's dynamic, cloud-first enterprises. It then goes on to reveal the extensive set of security capabilities incorporated in the Unity EdgeConnect™ Software Defined WAN (SD-WAN) edge platform from Silver Peak.

As you'll soon come to appreciate, the net result is an SD-WAN platform that supports key use cases (e.g., internet breakout to improve SaaS application and IaaS performance) and the key principles of a software-defined computing environment (e.g., being application-driven and enabling automation). Today's SD-WAN technology dramatically improves security over traditional networking infrastructures, and delivers a level of protection that meets or exceeds the security and compliance mandates of the modern enterprise.

Why SD-WAN Matters

The primary job of the WAN is to connect distributed users to the applications they need to do their jobs. As applications and computing models have changed, that job has become more difficult, and more important.

Enterprises that try to manage WANs using traditional routers or even basic SD-WAN approaches are faced with continual compromises and trade-offs. Manual processes and complex architectures prevent organizations from provisioning new applications quickly, or responding to changing conditions related to peak loads, unavailable network links, or denial of service (DoS) attacks. It is impossible to guaranty service level agreements for real-time applications, resulting in inconsistent quality of experience for system users. Security concerns can hamper the use of low-cost broadband connections and slow the move toward the cloud in general, and SaaS applications in particular.

Real-time, peer-to-peer communication is driving the need for higher performance and increasingly meshed connectivity. Then there's the Internet of Things (IoT) and big data apps, which are representative on the whole of both the increasing diversity of applications and the growing volume of data that today's WAN must be able to handle… ideally in a differentiated manner that ensures each is treated according to its individual characteristics and needs (e.g., relative to QoS, security, etc.).

The impact of these changes to the application landscape is that the enterprise WAN needs to change too. Traditional, private line connectivity options (such as multi-protocol label switching, or MPLS) and routing practices — backhauling, in particular — are clearly a poor match for cloud-based apps, burgeoning amounts of internet traffic, and peer-to-peer interactions. Key shortcomings include the high cost of such network services and architectures, the negative impact they have on performance (especially for internet or cloud-destined traffic), and the fact that they are too rigid.

In comparison, an advanced SD-WAN platform enables enterprises to shift to a business-first networking model, where the network conforms to the needs of the business instead of the business being constrained by the limitations of the network. In the business-first networking model, resources can be

> More than 80 percent of enterprise workloads will be in the cloud by 2020, with more than 40 percent running on public cloud platforms
>
> LogicMonitor Cloud Vision 2020 survey[1]

re-allocated automatically to match the business priority and security requirements of every application. The network stays in compliance with business and security policies. The enterprise can fully leverage low-cost broadband connections, SaaS applications, and cloud computing platforms. The benefits include:

- Always-consistent application performance and availability
- Reduced WAN total cost of ownership (TCO)
- Increased network and business agility
- Enhanced security[2]

Why Security Is Critical to SD-WAN Success

Strong security is a prerequisite and integral element of many of the benefits of a business-driven SD-WAN.

For instance, the use of broadband internet as low-cost connectivity option is core to the SD-WAN value proposition. However, the fact that broadband is "public" instead of "private" introduces the need for capabilities to ensure the confidentiality and integrity of application traffic traversing such connections. And let's not forget, too, that inline deployment of SD-WAN devices places them "in the line of fire" — at least compared to the scenario where a traditional WAN optimizer is implemented in an out-of-path configuration.

Enabling internet breakout is another good example. Although it's essential for enhancing performance and reducing the bandwidth (i.e., dollars) needed for backhauling, it also exposes branch users and their local networks directly to the internet and its myriad threats. So now you need a way to limit outbound destinations, block unwanted/unsolicited inbound traffic and filter allowed/expected traffic for threats.

However, not all web applications are created equal, and some web traffic can expose the enterprise to viruses, trojans, DDoS attacks and other vulnerabilities. Therefore, direct internet breakout must also be secure. For example, a web traffic security policy could be defined as follows:

- Send known, trusted business SaaS traffic such as Office365 and Unified Communications-as-a-Service (UCaaS) directly to the internet.
- Send enterprise data center-hosted application traffic directly to headquarters.
- Send all untrusted, suspicious and unknown web traffic (for example, peer-to-peer network traffic and traffic from countries in which the company does not do business) to a cloud-hosted security service.

To implement such a policy, web traffic must be steered granularly to its intended destination. This requires identifying the application on the first packet because once an application session has been established, it cannot be redirected to an alternate destination without breaking the flow resulting in application disruption. And because IP address ranges utilized by SaaS applications change almost continuously, address table updates must be automated and implemented on a daily basis.

Backhauling and Internet Breakout

The practice of backhauling is where branch office application traffic destined for (or returning from) the internet is routed via a WAN connection between the branch and a corporate headquarters location. This allows it to benefit from the security controls and countermeasures deployed at the headquarters site before being routed to the internet. However, backhauling application traffic results in poor performance due to added latency. The alternative, referred to as local internet breakout, is where selected branch office application traffic is routed directly to/from the internet (i.e., without the need to traverse the WAN and pass through a set of centrally deployed security tools before ultimately reaching the cloud-based application).

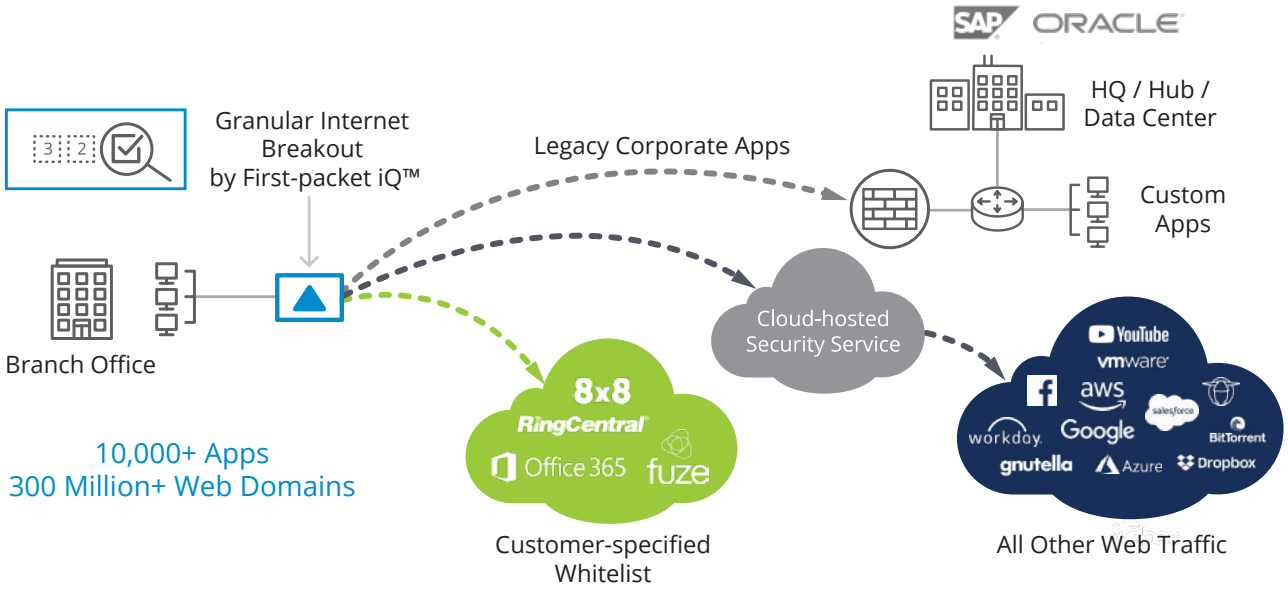


Figure 1: Application traffic must be identified on the first packet to steer traffic to its correct destination to enable granular security policy enforcement. As more applications migrate to the cloud, new cloud-hosted security services have emerged, providing improved application performance. Centralizing security services provides faster response to new threats as they are discovered.

Additional areas where security is applicable to the success of an SD-WAN implementation include:

- Enabling applications with different security requirements to share the same physical connectivity
- Enabling faster deployment and more efficient management — for example, with secure, automated provisioning of SD-WAN devices, automated security policy enforcement, and a secure management plane
- Enabling consistent enforcement of an application's specific security policies regardless of where that application is located or accessed

Introducing Silver Peak Unity EdgeConnect

The Silver Peak Unity EdgeConnect™ SD-WAN edge platform, the industry's only business-driven SD-WAN solution, provides enterprises with the flexibility to use any combination of transport technologies — including public broadband services — to connect users to applications without compromising application performance or security. The three main components of the platform include:

- Unity EdgeConnect zero-touch physical or virtual appliances, which are deployed at an organization's branch offices, central sites, and cloud data centers
- Unity Orchestrator™, a centralized management system that enables simplified configuration and orchestration of the entire WAN and provides complete observability into both legacy and cloud applications; QoS and security policies are defined centrally and automatically deployed globally to all appliances in the SD-WAN, increasing operational efficiency and minimizing human errors which can jeopardize branch security
- Unity Boost™, an optional WAN optimization performance pack that enables IT teams to engage Silver Peak market-leading WAN optimization capabilities, where needed, simply by checking a box in the Orchestrator interface

The Silver Peak Unity EdgeConnect SD-WAN edge platform is designed with an extensive set of capabilities that address the security challenges and requirements inherent in SD-WAN implementations.

How EdgeConnect Delivers a Secure SD-WAN

EdgeConnect goes well beyond the basics of ensuring the confidentiality of application traffic traversing public networks. An extensive set of security capabilities provides coverage across four essential areas: the data plane, the management plane, partner integrations, and compliance. The net result is the full-spectrum of protection needed for enterprises to fully realize the benefits of an SD-WAN architecture — enhanced application performance, lower WAN TCO, and increased business agility — without being exposed to greater security risks.

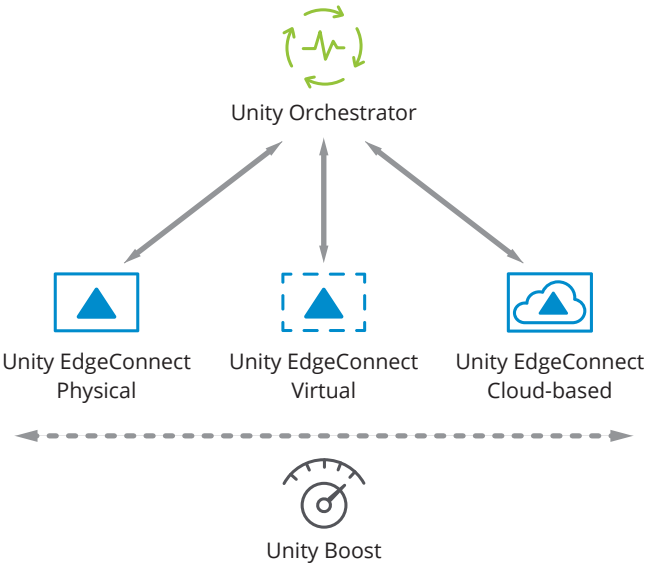


Figure 2: Silver Peak Unity EdgeConnect SD-WAN Edge Platform

Application-driven Data Plane Security

Different applications deserve — or perhaps even require — different treatment when it comes to how they are handled from a security perspective (not to mention other "perspectives," such as QoS, performance optimization, and tunnel bonding policy). For example, a business application that is processing sensitive transactions might require encryption regardless of the type of transport being used to meet compliance requirements, while SaaS applications could be left to rely on their own native capabilities (e.g., TLS). This is why it's important to have an application-driven SD-WAN, where policies and configuration settings can be implemented on a per-application basis.

Relevant security capabilities available with EdgeConnect include:

Data-in-Transit Protection: Each EdgeConnect data path is protected by IPSec tunnels that use AES 256-bit encryption to maintain application and data confidentiality. EdgeConnect uses an "IKE-less" IPsec UDP protocol; that is, it employs standards-based IPsec UDP encryption but doesn't require Internet Key Exchange pre-shared keys. Encryption keys are never repeated and are directionally unique. Unity Orchestrator manages the encryption keys and rotations automatically, which reduces tunnel setup time without a loss of service. This protocol avoids problems encountered when deploying NAT (Network Address Translation) with IKE, such as failures when branch offices have multiple devices with different VPN requirements. Because IKE-less tunnels use different ports over IPsec, they are unlikely to be limited or blocked by upstream firewalls. These advanced features for protecting data in transit increase the flexibility, security, and robustness of secure communication between remote endpoints.

End-to-end network segmentation: EdgeConnect allows enterprises to create multiple application-specific virtual WAN overlays (also called business intent overlays). Each virtual overlay specifies priority and quality of service requirements for application groups based on business requirements. Using these specifications, EdgeConnect automates traffic steering end-to-end across all underlying WAN transport services.

Each virtual overlay is mapped to a LAN-side zone or zones. A zone may be comprised of VLANs, physical and logical interfaces, and sub-interfaces. Each zone can be assigned security policies that limit connectivity with other zones. For example, a policy could allow only outgoing traffic, or allow incoming traffic only from approved (white listed) applications and services, or block all traffic from less secure zones.

With end-to-end network segmentation:

- Micro-segmentation is extended from the LAN, across the WAN, and to data centers and cloud platforms
- Traffic within each zone is isolated from traffic in other segments, reducing unauthorized access and limiting the scope of incidents
- High-priority applications enjoy faster, more reliable performance across WANs, increasing application availability and improving the experience and productivity of end users

Simple policy creation: IT administrators can create end-to-end network segments in minutes using an intuitive graphical user interface. These segments can connect LANs with other LANs (LAN-WAN-LAN) and with data centers (LAN-WAN-data center). The virtual WAN overlays are defined based on business requirements and intent, not infrastructure details like IP addresses. Zone-based security policies are displayed in a configuration matrix that makes them easy to understand.

Central orchestration and automated enforcement: Once virtual WAN overlays and zone-based stateful firewall policies have been defined, Orchestrator deploys them to all EdgeConnect SD-WAN appliances, where they are automatically enforced. This replaces the time-consuming manual configuration of routers and firewalls every time a policy changes. The benefits include:

- Consistent security policy enforcement across LANs and WANs
- Fewer configuration errors
- Improved compliance with regulations and industry standards
- Increased productivity for security and operations staffs

DDoS Defense: With the rising frequency of distributed denial-of-service (DDoS) attacks, it is imperative that enterprises establish cost-effective defenses for any and all sites that might be affected. With EdgeConnect deployed at branch locations,

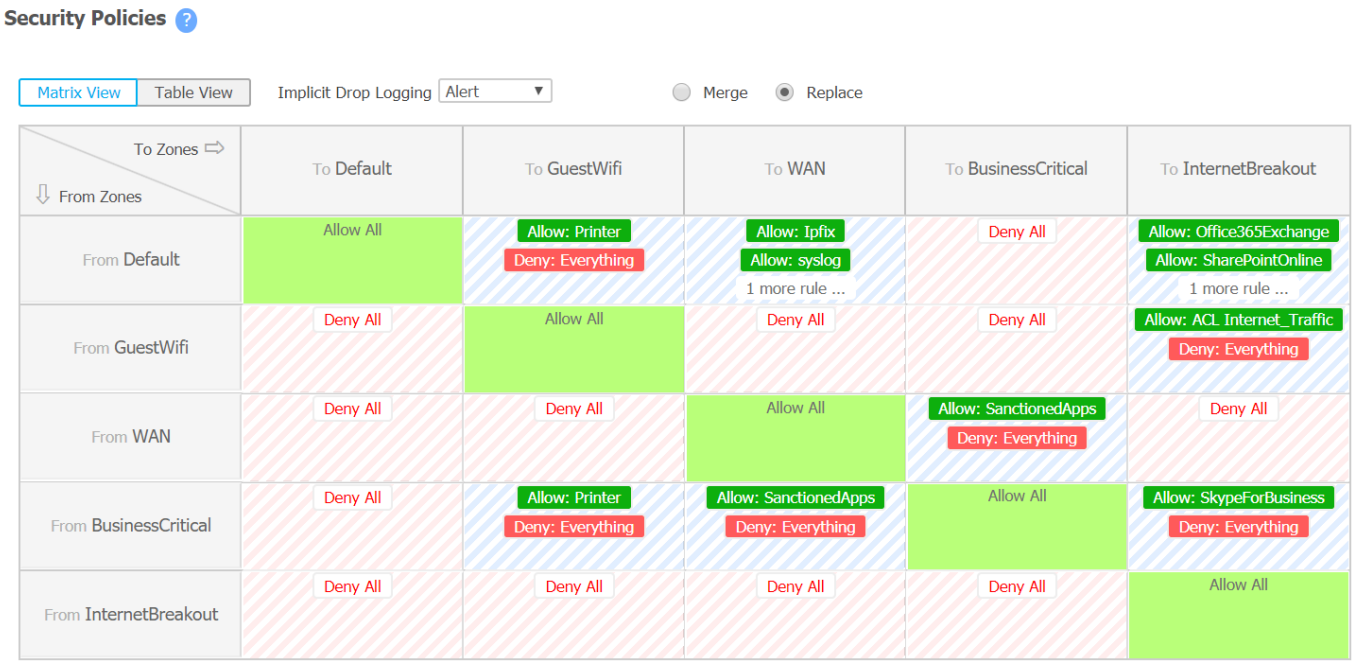


Figure 3: A security policy configuration matrix greatly simplifies the creation and management of segmentation rules.

that's precisely what you get. The built-in zone-based stateful firewall always discards any incoming packets that are not associated with a previously established LAN initiated flow. In the event a broadband connection is flooded by a DDoS attack, EdgeConnect dynamically leverages other available connections to sustain operations with no degradation to application performance or impact to SD-WAN manageability.

EdgeConnect protects not only itself, by dropping the offending traffic, but also protects all of the users and systems both on the local network and over the remaining, operational WAN connections.

Data-at-Rest Protection: All blocks of data that persist within EdgeConnect appliances as a result of the Unity Boost WAN optimization data de-duplication capability are protected with AES 128-bit encryption.

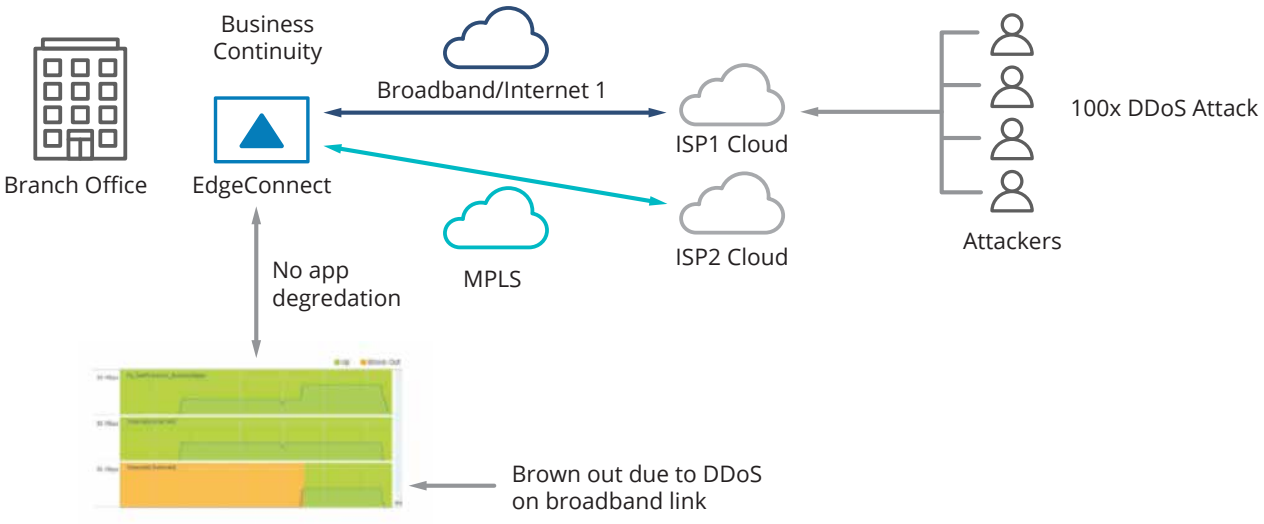


Figure 4: EdgeConnect protects the SD-WAN from DDoS attacks and routes traffic across an alternate transport service to keep applications running, enhancng business continuity.

Intelligent, Secure Traffic Steering

Although it's not a security capability per se, EdgeConnect First-packet iQ™ classification plays an important role in the overall effectiveness of the Silver Peak SD-WAN edge platform. By identifying applications on the first packet of a session, it enables application-driven traffic steering that not only ensures efficient use of WAN resources, but also helps automate security policy enforcement. For example, with First-packet iQ, trusted SaaS and web traffic can be sent directly to the internet (avoiding the performance impact and cost of backhauling), while unknown or untrusted web traffic can be service chained to more advanced corporate or web-based security services. Automated SaaS IP address updates described previously ensure that application traffic is directed correctly according to defined security policies.

Management Plane and System-level Security

Despite being less top-of-mind than its data plane counterpart, system and management plane security is no less important. Relevant EdgeConnect capabilities in this area include:

Secure, Zero-Touch Provisioning: A key part of the EdgeConnect value proposition is a plug-and-play deployment model that enables rapid installation, without the need for a distributed IT presence. Security for this process takes the form of a two-step authentication and authorization procedure. Before receiving its settings and policies and becoming an active part of the SD-WAN, each newly connected EdgeConnect appliance first must be authenticated by the Silver Peak Cloud portal and then "approved" by an IT administrator using Orchestrator. In addition, Orchestrator can also be used to subsequently revoke access for a given appliance (e.g., if it is stolen or otherwise compromised). This results in any in-flight traffic being dropped, and the specified appliance being unable to download configuration information or join the SD-WAN.

Encrypted Management Communications: All communication sessions between EdgeConnect appliances, Orchestrator, the Silver Peak cloud portal, and administrators' web browsers are protected with TLS 1.2. Furthermore, all weak protocols (e.g., SSLv2, SSLv3, TLS 1.0, TLS 1.1), weak hashes (e.g., MD5), and weak encryption algorithms (e.g., DES, RC4) are disabled by default.

System Hardening: EdgeConnect is a hardened appliance that ships with the factory default "harden" mode. This approach ensures out-of-the-box security for appliances plugged in for the first time."

Subsequently, on zero touch provisioning and configuration, a strong password per standard FIPS 140-2 guidelines is always enforced on the appliance. This prevents malware from using default passwords to gain unauthorized access to the appliance. All non-essential management services like SSH, FTP are closed by default.

Other management plane protections include:

Robust user authentication and authorization

- Support for local, RADIUS, TACACS+, and OAuth for authentication and authorization with identity management systems such as Active Directory and Okta.
- Granular role-based access control with read-only users and multiple administrator roles
- Whitelisting for Orchestrator that restricts administrative access to a specific set of IP addresses or subnets

Extensive logging for both Orchestrator and EdgeConnect

- Event logs/alarms — for system errors pertaining to memory, CPU, network interfaces, routing, and management plane connectivity
- Threshold crossing alerts — configurable, rising and falling thresholds to signal imminent/approaching conditions for concern, such as high memory or bandwidth utilization
- Audit logs — for tracking all access to an activity conducted via any of the available management interfaces (CLI, WebUI, or REST APIs)
- Firewall logs — traffic flows inspected by the Silver Peak Zone-based firewall rules can be "Allowed and Logged" or "Denied and Logged". Firewall logs can be streamed to a third party tool (e.g. SIEM).
- Netflow/traffic logs — for capturing full (non-sampled) flow data so that it can be streamed to a third-party tool (e.g., Netflow collector (remove: SIEM)

In addition to being critical for network management and incident response, log data can be valuable for complying with standards such as HIPAA.

Rigorous processes for for vulnerability management: Silver Peak has made significant investments over many years in rigorous processes for detecting and managing vulnerabilities in its technology.

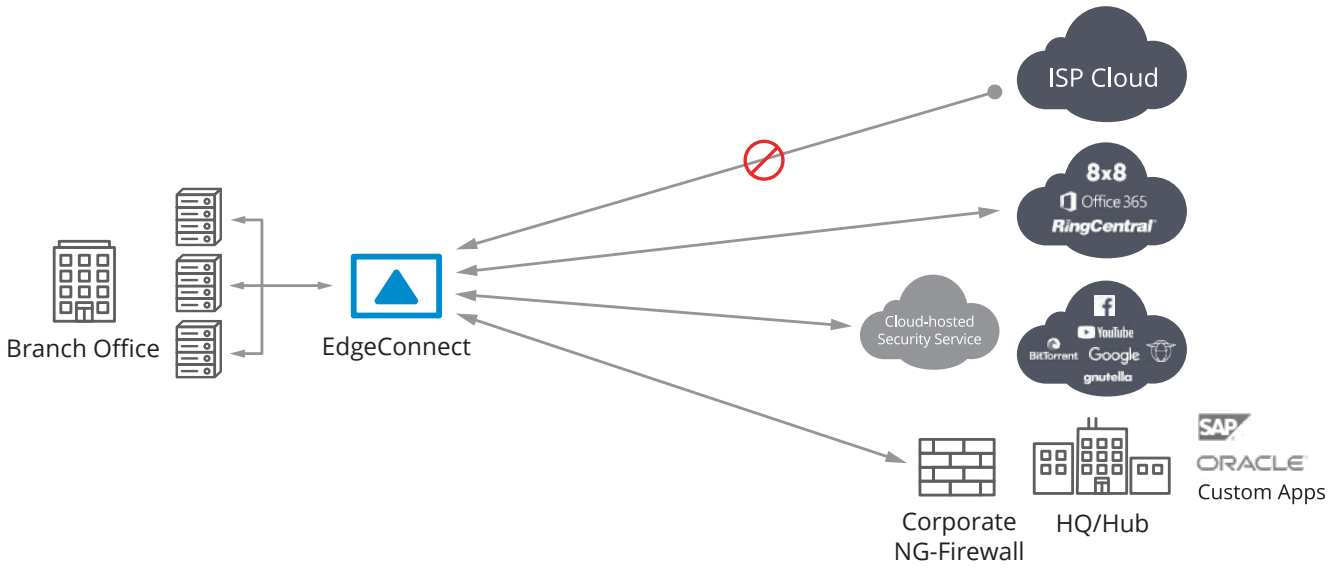


Figure 5: EdgeConnect integrated stateful firewall and simplified service chaining to secure web gateways and next-generation firewalls provides a comprehensive security solution for branch offices.

A dedicated team continually conducts vulnerability assessments and runs penetration tests for every release of every product, including cloud products. Customers and industry researchers are invited to submit security issues and vulnerabilities (and can use a PGP public key to encrypt sensitive information in their reports). The Silver Peak Product Security Incident Response Team (PSIRT) quickly analyzes announced vulnerabilities and security issues, determines if they are applicable to any of the company's products, documents recommended actions for Silver Peak customers, and publishes security advisories on the Silver Peak website.

Security Technology Partnerships and Service Chaining

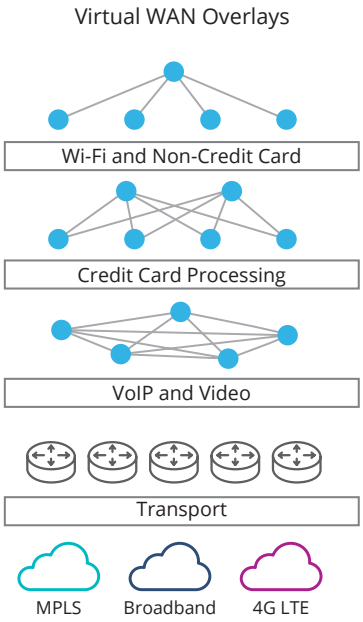
Third-party security products and services are — or, at least should be — another big part of the overall effectiveness equation for an SD-WAN solution.

EdgeConnect supports the integration of third-party security technologies into the SD-WAN architecture as follows:

Security Partners: Most organizations already have an existing set of security tools and infrastructure in which they've made a considerable investment. Plus, when it comes to security, it's simply not realistic for a single solution provider to do everything on its own. The scope of threats, risks, and corresponding technologies is simply too great. The net result is that it's not only advisable to work with third-party security solutions, but also necessary. This is why Silver Peak maintains technology partnerships covering solution areas such as next-generation firewalls, secure web gateways, anti-malware tools, and sandboxing products from security companies like Check Point, Forcepoint, Infoblox, McAfee, OPAQ Networks, Palo Alto Networks, Symantec, and Zscaler.[3]

Service Chaining: To more closely align with the ease-of-use, automation, and flexibility objectives of today's enterprises, EdgeConnect also enables simplified service chaining. With this capability, administrators can take advantage of a drag-and-drop interface to logically interwork a combination of Silver Peak and partner security capabilities in whatever arrangement best meets their needs. A few, straight-forward (yet powerful) examples include:

- A service chain where internet-bound traffic is routed through cloud-based security services for Layer 7 access control, threat filtering, and analytics
- A service chain where EdgeConnect and a next-generation firewall are collocated in select branch offices that are locally hosting one or more enterprise applications



Access Policy	Topology	Connection	QoS
Guest VLAN	Hub Spoke	Internet	Min. Cost
Data VLAN	Dual Hub and Spoke	MPLS – Internet	Max. Availability
Voice VLAN	Full Mesh	MPLS – Internet – LTE	Max. Quality

Figure 6: EdgeConnect extends micro-segmentation across the WAN to help enterprises meet compliance standards.

> A service chain where EdgeConnect and a next-generation firewall are collocated at regional hub/office to provide advanced security screening for untrusted applications that are still being backhauled

Security Certification and Compliance

Last, but not least, there are many ways EdgeConnect helps ease the burden of complying with relevant industry regulations, including: Health Insurance Portability and Accountability Act (HIPAA)[4], Payment Card Industry Data Security Standard (PCI DSS)[5], Sarbanes-Oxley Act (SOX), the European Union GDPR, and others. One example is certification to the Federal Information Processing Standards (FIPS 140-2), which provides assurance of correct implementation and failure handling for supported cryptographic functions.[6]

Then there are all of the security features covered so far, most of which are applicable to multiple requirements spanning multiple regulations. Authentication, authorization, and auditing capabilities, for instance, are a fundamental requirement of NIST Special Publication 800-53 (Security and Privacy Controls for Information Systems and Organizations) — and, therefore, of practically every regulation that invokes it. Notable too, especially for its uniqueness among SD-WAN solutions, is EdgeConnect's support for micro-segmentation. The ability to create encrypted, application-specific overlays can help IT teams control access to systems that store and process electronic private health information (ePHI) to support HIPAA compliance, segment off credit transactions and associated systems to substantially reduce the scope of their PCI DSS compliance efforts, and reduce the risk of unauthorized access to information about customers to meet GDPR and other privacy rules.

Conclusion

Fully realizing the many compelling benefits of an SD-WAN depends to no small extent on having a solution that accounts for the security issues, challenges, and opportunities that such an approach presents. In this regard, the extensive security capabilities of the Silver Peak Unity EdgeConnect SD-WAN edge platform go well beyond the minimum-required level of protection afforded by transport-level encryption and message authentication.

By combining robust data and management plane security features with numerous security technology partnerships, and simplified service chaining, EdgeConnect delivers a level of security that better meets the actual protection and compliance needs of today's enterprises and enables business-first networking, the highest quality of experience for system users, and continuous adaptation to changing business and technical conditions.

For more information about the EdgeConnect SD-WAN solution from Silver Peak, click here.

FOOTNOTES

1. LogicMonitor Cloud Vision 2020 survey: https://www.logicmonitor.com/resource/the-future-of-the-cloud-a-cloud-influencers-survey/
2. For details of how SD-WAN delivers improved ap- plication performance and other benefits, click here.
3. Related solution briefs are available here.
4. For details on how EdgeConnect supports HIPAA compliance, click here.
5. For details on how EdgeConnect supports PCI DSS compliance, click here.
6. For details on FIPS certification status, click here.

Company Address

Silver Peak Systems, Inc
2860 De La Cruz Blvd.
Santa Clara, CA 95050

Phone & Fax

Phone: +1 888 598 7325
Local: +1 408 935 1800

Online

Email: info@silver-peak.com
Website: www.silver-peak.com

SP-WP-SD-WAN-SECURITY-050620