Solution brief

Verizon Software Defined Perimeter

Verizon Software Defined Perimeter (SDP) is a Zero Trust approach to networking for remote access, internal networks and cloud applications. The high-performance solution can help defeat network-based attacks from unauthorized users and devices.

One of the top concerns of CIOs today is cloud adoption with many enterprises using two or more cloud vendors. This provides great agility, but often involves the hairpinning of data to access the applications. That makes for lower performance and slower access for users.

A second concern is that more employees and contractors are working from home. How can IT provide a secure connection to authorized enterprise applications without providing access to unauthorized applications and the network infrastructure itself? And how can IT provide access that is transparent to the users?

A final concern is how to implement a Zero Trust architecture recommended by National Institute of Standards and Technology Special Publication (NIST SP) 800-207. This is an approach where the organization recognizes that the internal network cannot be trusted anymore because adversaries can easily compromise a PC, add a back door to it and begin scanning the network for valuable data. Additionally, adversaries can obtain the same end result by walking into a branch office and connecting a hacking device to the network.

Verizon SDP can help solve these problems, isolating enterprise and cloud applications from unauthorized users and devices while providing direct, fast access to applications for authorized users on authorized devices. It can provide secure remote access to authorized applications without making the network accessible, and it does it with multifactor authentication (MFA) that is transparent to users.

Verizon SDP is an effective way to implement a Zero Trust architecture.

Theory of operation

Verizon SDP sits between users and servers, and isolates servers to help defeat exploits such as attacks on vulnerabilities and configuration errors. It applies MFA to help defeat credential theft while not requiring the user to continuously reenter their passwords or multifactor authentication tokens. And it encrypts all traffic to help defeat man-in-the-middle attacks.

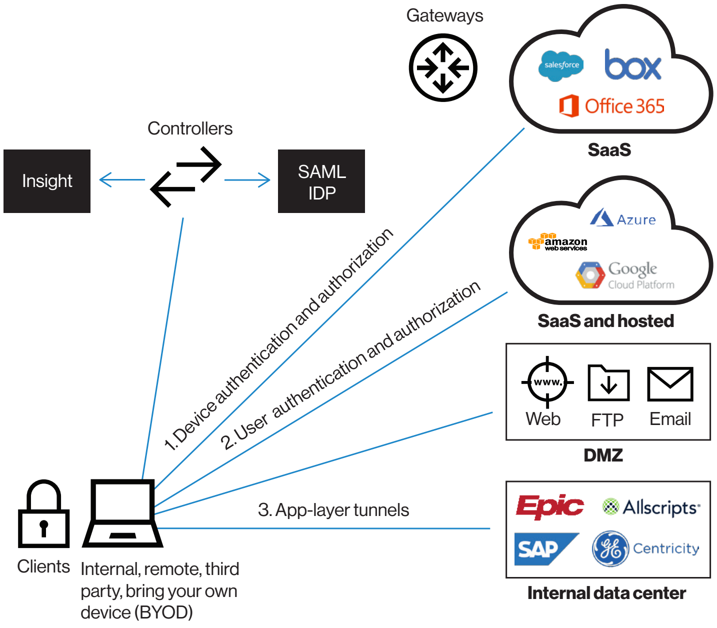
Architecture

Verizon SDP consists of three main components:

- Controllers
- Gateways
- Clients

Together, they help defeat unauthorized users and devices attempting to access protected applications. The figure below shows the protected applications on the right. These include software-as-a-service (SaaS) applications; those hosted in infrastructure-as-a-service (IaaS) or hosting centers; applications on the DMZ; and applications in the data center.

These applications are isolated from the network by the gateways. Therefore, the gateways helps defeat adversaries from exploiting software vulnerabilities and configuration errors on those servers.



On the left, workstations, laptops and mobile devices run the Verizon SDP Client, which implements MFA to help defeat credential theft. It does this by binding the Security Assertion Markup Language (SAML) assertion of what the user knows with the device that the user has. It can help defeat password theft, pass-the-hash, pass-the-ticket and other credential theft attacks, and it is transparent to the user.

In-the-middle, mutually authenticated, encrypted tunnels connect authorized users on authorized devices to their authorized enterprise applications. This helps defeat man-in-the middle attacks by maintaining data secrecy and integrity.

When the Verizon SDP Client starts up, it does device authentication and authorization to the Controller. Then it invokes the user's browser so the user can log in to the enterprise SAML Identity Provider. The SAML assertion that is returned to the Controller cryptographically authenticates "who the user is." This is matched to the device "that the user has" to provide multifactor authentication. This is an ideal MFA because it can help defeat credential theft and it is transparent to the user. The SAML assertion also provides the groups that the user is a member of in the enterprise directory. The groups represent authorized access to one or more protected applications.

Next, the Controller tells the Gateways about the identity of the Client and the Client about the identity of the Gateways. The Client simultaneously builds dynamic, encrypted tunnels to all gateways necessary to provide the user access to all the applications he or she is authorized to get. And all in a matter of seconds.

Finally, there is an application called Verizon SDP Insight that continuously monitors the activity of the Verizon SDP service to understand which users on which devices are accessing which applications at what time and for how much data. It also monitors all the servers of the SDP and provides both passive and active monitoring of the protected applications.

Verizon SDP is a software-only solution. Controllers and Gateways are virtual machines that can be located wherever they are needed. It is an over-the-top networking solution that can be typically applied in customer environments without requiring expensive hardware upgrades. And it is the fastest Zero Trust solution. Traffic takes a direct route from the user to the applications with no hairpinning of data or unnecessary trips to intermediary nodes. Verizon SDP is a single-tenant SaaS. One customer's throughput is not affected by another customer's data.

Multifactor authentication

Stolen passwords are a major security issue. According to the *2017 Verizon Data Breach Investigations Report*, 81% of hacking-related breaches leveraged either stolen or weak passwords. Multifactor authentication is the answer.

One of the best forms of MFA is the cryptographic one-time password with replay prevention because it is not feasible to guess the one-time password in a reasonable amount of time. Another form of MFA is mutual Transport Layer Security (TLS) based on public/private key cryptography. While the security of the one-time passwords and the mutual TLS keys are similar, the private key of mutual TLS can be stored in the Windows® certificate store (or the Linux keychain), where it is difficult to view or copy. Verizon SDP uses both the one-time password and mutual TLS for MFA. That is, both the one-time password keys and the mutual TLS keys are tied to the user. Something the user knows is tied to something the user has. It helps defeat password theft, pass-the-hash and pass-the-ticket.

But all MFA products become useless if the PC is compromised. Stored keys, independent factors, phone-as-a-factor, out-of-band soft tokens and even hardware tokens like RSA tokens all become useless if the adversary compromises the PC. No matter how complicated the MFA process, the adversary can just wait for the authorized user to connect to the protected application with the required MFA and then exfiltrate the data directly. Multifactor authentication can help defeat credential theft. It cannot help defeat a compromised PC.

Now that we understand the capabilities and limitations of MFA from a security point of view, what other factors should be considered when selecting a multifactor authentication product?

Probably the most important factor is the best possible user experience. MFA can help defeat weak and compromised passwords, but users must be willing to use it.

If MFA is too painful to use, then enterprise productivity and collaboration will suffer, and the IT department will be the bane of users. However, if the MFA is easy to use, then users will be happy to use it and will be happy with the IT department. The MFA of Verizon SDP is transparent to users and it is applied every time users log in to their computers.

In addition to being transparent to users, Verizon SDP is easy to deploy. Applications can quickly be added to it. It does not typically require any change to enterprise applications.

Verizon SDP is among a few MFA products that can help defeat server exploitation because MFA occurs before user authentication. Normally, MFA is applied after the user logs in. This requires that the application server be exposed to exploitation by the adversaries. That is, the adversary can connect to the server before it is determined that the adversary is not authorized to connect to the server. If the server has vulnerabilities or configuration errors, the server can be compromised. But the MFA of Verizon SDP is applied before the application is exposed to the adversaries. Verizon SDP can help defeat server exploitation because Verizon multifactor authentication occurs before user authentication.

High availability and disaster recovery

High availability and disaster recovery were designed into the Verizon SDP from the ground up. The minimum configuration has two Controllers that are active/active and load balanced, and they can scale out to an almost unlimited number to support more users. And recall two things about Verizon SDP Controllers. First, they are for device and user authentication only. No user data passes through them. Second, a separate SDP is deployed for each customer. Therefore, the total number of users on a Verizon SDP is the total number of a single customer–not all customers.

When each Controller comes online, it downloads the database of users from the master database. The master database is active/standby in region with disaster recovery snapshots out of region. The database only changes when new users or new devices are onboarded to SDP.

Verizon SDP Gateways are always deployed as pairs per geographic location, and they are active/active and load balanced. Gateways can also be scaled out as more and more applications are added to the Verizon SDP at each location.

Therefore, one can see that the Verizon SDP has implemented an architecture that is highly available and with disaster recovery built in.

Customer use cases

The Verizon SDP supports three main categories of use cases: 1) next-generation remote access, 2) business-critical internal applications and 3) secure SaaS access, and each of these has two or more sub-use cases.

Employee and third-party remote access

Today's remote-access VPN provides too much access. The remote users are "off the LAN." They use the DHCP and DNS off the LAN. They have access to many, if not all, of the applications. And they have access to switches, routers and security products that make up the infrastructure. They may even have access to print servers and Internet of Things (IoT) devices. Verizon SDP changes that.

It combines the encrypted tunnels and MFA of the traditional remote-access VPN but makes the remote access more secure by operating as an application-layer tunnel such that the user is not "on the LAN." The result is that the user can access authorized applications, but nothing else. Then Verizon SDP adds "always-on" and "transparent MFA" to create a transparent user experience (UX).

Access to multiple clouds and data centers

Enterprises are moving to the cloud. And many enterprises are moving to multiple clouds. But they also still have data centers. Therefore, when remote users connect to the corporate network, their data is hairpinning all around. Ideally, the data path would be directly to each cloud and directly to each data center. But that would put cloud and data center servers "on the internet." However, Verizon SDP Gateways completely isolate servers in the cloud and in the data center while providing the shortest path possible to the data. The result is greater security and happier users.

Secure enclave

The term "secure enclave" is becoming popular these days. To create one, put an application in a virtual private cloud and access it with Verizon SDP. One gets the advantage that the application is accessible from around the world, but invisible to unauthorized users. Note that Verizon SDP is one of the few products that can create a secure enclave because it is one of the few products that does multifactor authentication before user login. Therefore, the servers in the secure enclave don't need to be exposed to the internet.

Business-critical applications

If you believe in the Zero Trust model, then critical applications such as intellectual property, financial data or personal information on the internal network must be removed from the internal network. By putting servers for those applications behind an SDP Gateway, you truly are implementing a Zero Trust architecture by isolating those resources from all internal users but providing access to authorized users on authorized devices.

Unsupported OS/app

Many enterprises have a small number of applications running on old, unsupported operating systems that cannot be upgraded. Typically, there are fewer than 100 users for each of these applications, but the users are often distributed throughout the company. Therefore, simple firewall rules do not work, and exposing these servers to the internal network may result in a compromised server and often causes an audit finding. Verizon SDP can isolate these systems from unauthorized users and unauthorized devices. This protects the data and, often, eliminates the audit finding.

With and without NAC

Typical network access control (NAC) installations create three networks: production, guest and quarantine. But, to implement a Zero Trust architecture, one must segment the production network such that no unauthorized user can connect to the business-critical servers. This is not practical with NAC, but Verizon SDP does this, and it does it over the existing network topology, typically with no hardware upgrade.

Privileged access

Verizon SDP doesn't have all the bells and whistles of a dedicated privileged-access management (PAM) product, but Verizon SDP implements multifactor authentication; the Gateway is effectively a hardened, Bastian host/jump box; and SDP tracks which users on which devices access which applications from where and at what time of the day. But the real reason to use it instead of a dedicated PAM product is that the admins and application owners can use the native tools they prefer, such as BASH, FileZilla, PuTTY, RDP, etc., and be more productive at their jobs.

IP whitelisted SaaS access

Many SaaS applications support IP whitelisting. Typically, this is used to allow users access to the SaaS from their corporate network (i.e., their corporate Classless Inter-Domain Routing [CIDR] block) and nowhere else. Assuming users are either on the LAN or have remote access that requires MFA, IP whitelisting can mitigate credential theft. A simple alternative is to IP whitelist the SaaS to a Verizon SDP Gateway. This helps defeat credential theft, and man-in-the-middle attacks, and, typically, provides a short path from the remote user to the SaaS.

SaaS authentication via the internal IdP

For those SaaS applications that do not support IP whitelisting, external users can be directed to the internal SAML identity provider (IdP) by Verizon SDP. This helps defeat credential theft by eliminating the path to the IdP by external adversaries.

Verizon SDP is a Zero Trust approach to networking. It isolates servers to help defeat server exploitation. It integrates MFA to help defeat credential theft. And it builds end-to-end encrypted tunnels with one of the strongest cryptographic algorithms commercially available to help defeat man-in-the middle attacks.

Great user experience

Transparent multifactor authentication means no phone to respond to, no token to enter. "Always on" means you can sleep your computer, wake it up in another location and it's connected to the Controllers and Gateways that give users access to their authorized applications. It uses "over-the-top tunnels," meaning it works over existing networking hardware typically without modification. It also means that Verizon SDP provides a direct route from client to server, which, in turn means users get a faster response from their applications. The fact that it connects to multiple Gateways simultaneously means no hairpinning of data, which again means faster application access. Verizon builds a separate SDP per customer. It is single tenant, not multitenant. Therefore, there's never any congestion in one customer's SDP network from another customer.

Easy to install

It is delivered as a service, so you don't need subject matter experts to run it. It's software defined, so there's no hardware to buy. And it's compatible with existing networks, so typically you don't need to upgrade hardware.

Total visibility

Verizon SDP Insight provides actionable, real-time visibility into the protected applications, their users and their devices. It tells you which users on which devices access which applications, when and from where.

Keep your network secure.

Help defeat network-based attacks from unauthorized users and devices. To find out more about Software Defined Perimeter, please contact your account representative.

Contact your account manager ›

Learn more about other Verizon network services and products ›

verizon✓