Verizon Software Defined Perimeter

Fact sheet

The fast, zero-trust solution.

Verizon Software Defined Perimeter (SDP) is the zero-trust approach to networking for remote access, internal networks, and cloud applications. It can defeat network-based attacks from unauthorized users and devices. It is fast and user-friendly, and it can be used standalone, or combined with Verizon's Private IP or SD-WAN services to create trusted networks.

Zero trust

Remote access: SDP provides authorized users on authorized devices access to authorized applications. However, unlike traditional remote access VPNs, SDP does not provide the user or their devices access to the internal network. This is especially important for 3rd party access.

Internal network: Due to phishing and other social engineering attacks, the internal network may be just as insecure as the Internet. SDP segments the internal network–isolating servers from unauthorized users.

Cloud access: Software as a Service (SaaS) applications are vulnerable to credential theft and multi-factor authentication (MFA) is a proven solution. Verizon SDP includes an MFA that is transparent to users.

Architecture

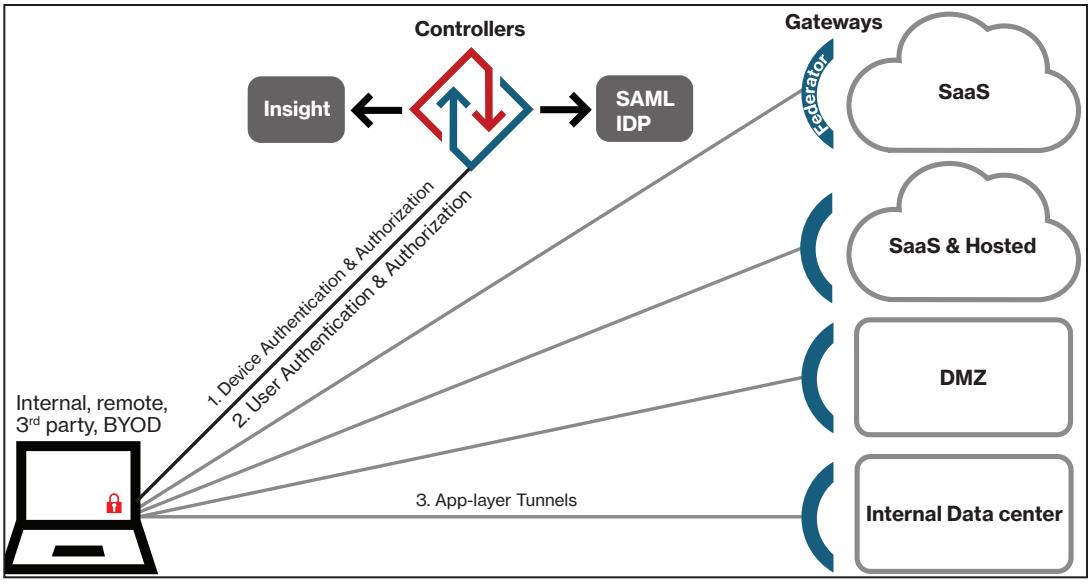
The SDP consists of three main components:
- Controller Cluster
- One or more Gateway Clusters
- Clients

Together, they can defeat unauthorized users and devices attempting to access protected applications.
The figure below shows the protected applications on the right. These include SaaS applications, those hosted in Infrastructure-as-a-Service or in hosting centers, applications on the DMZ, and applications in the data center.

These are protected by the Gateways, which defeats adversaries from exploiting software vulnerabilities and configuration errors of those servers. Then, on the left, workstations, laptops, and mobile devices run the SDP thin client, which implements MFA to defeat credential theft. It does this by binding the SAML assertion of what the user knows with the device that the user has.

In the middle, mutually-authenticated, encrypted tunnels connect authorized users on authorized devices to their authorized enterprise applications. This defeats man-in- the-middle attacks by maintaining the secrecy and integrity of the data. Finally, Verizon SDP Insight provides visibility and reporting on which users are accessing which applications on which devices.

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 applied in all customer environments without requiring expensive hardware upgrades. And it is the fast zero-trust solution. Traffic takes a direct route from the user to the applications with no hair pinning of data or unnecessary trips to intermediary nodes.



verizon

Use cases

Employees / third-parties: users get fast remote access to authorized applications from virtually everywhere but are prevented from accessing other unauthorized servers or the LAN infrastructure.

Hybrid cloud: enables enterprises to extend their data center into an IaaS environment while blocking access from the Internet. SDP isolates users from applications and then applies role-based access.

Cloud-based secure enclave: consists of a self-contained Virtual Private Cloud (VPC) with role-based SDP access from the Internet. This prevents unauthorized connectivity from outside the container and exposure of internal IP addresses or infrastructure.

Business-critical applications: intellectual property, financial information, and personally identifiable information about employees, customers, and partners are three key areas of concern. Verizon SDP isolates adversaries on the internal network from the applications that house that data.

Unsupported applications: some applications outlive their vendor support. Vulnerabilities continue to be discovered but cannot be patched. Verizon SDP isolates these applications and the servers they reside on from unauthorized users, and only provides access to the few users who have a need to know.

Privileged access: SDP provides the four most important factors of privileged access. 1) It isolates the servers from all unauthorized users. 2) It implements MFA for all authorized users. 3) It defeats man-in-the-middle attacks between the authorized users and the protected servers. 4) It records which authorized users on which authorized devices accessed which protected servers and from where.

SaaS: enterprise SaaS applications implement Single Sign-On (SSO) via SAML and WS-Fed. If an adversary obtains access to the credentials of an authorized user, the adversary has access to all SSO applications. SDP provides the ideal security for SaaS. It defeats credential theft and provides a transparent experience to the users.

Multi-cloud approach: implies access to two or more clouds such as AWS, Azure, Compute Engine, IBM Cloud, and Oracle Cloud at the same time. Most enterprises also still have more than one data center. When applications are distributed like this on traditional networks, data routing can be complex with lots of hair pinning of data. SDP is cloud agnostic and takes a direct route to each application to create a fast user experience.

Features and benefits

Zero-Trust Model: Verizon SDP is the zero-trust approach to networking. It isolates servers to defeat server exploitation. It integrates MFA to defeat credential theft. And it builds end-to-end encrypted tunnels with the strongest cryptographic algorithm currently commercially available to 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. And it uses over-the-top tunnels, meaning it works over existing networking hardware. It also means that Verizon SDP provides a direct route from client to server, which, in turn means users get a fast response from their applications. And the fact that it connects to multiple Gateways simultaneously, means no hair pinning of data, which again means faster application access. And, 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 no hardware to buy. And it's compatible with most networks so you do not need to upgrade any hardware.

Total Visibility: SDP provides actionable, real-time visibility into the protected applications, their users, and their devices.

Learn more

To find out more about the Software Defined Perimeter, please contact your account representative.

For more information about other Verizon network products and services, visit:
enterprise.verizon.com/products/network

verizon