Verizon Software Defined Perimeter (SDP).

Introduction.

For the past decade, perimeter security was built on a foundation of Firewall, network access control (NAC) and virtual private network (VPN) appliances. However, the growth of outsourcing and cloud computing has increased the cost of operating physical appliances, as resources migrate outside the perimeter. More important, there is a new generation of malware that can spread via compute devices belonging to authorized users.
New cyber-threats coupled with increased network complexity have enterprises looking for a new approach to perimeter security.

Verizon Software Defined Perimeter (SDP) is a cybersecurity service that protects application infrastructure against existing and emerging cyber threats. Verizon SDP defeats existing cyber attacks such as credential theft and server exploitation by blocking connectivity from unknown devices and making them virtually invisible to anyone that is not approved to access them. More significantly, Verizon SDP is a countermeasure against a new generation of malware that has the ability to spread via LAN, WiFi and VPN connections. These two features make SDP an "over the top" security solution that can fit any customer environment without requiring a re-architecture of the existing infrastructure or security elements.

An extension to our Software Defined suite of solutions, Verizon SDP creates a strong barrier around high value apps and implements multiple identity, device and entitlements checks before granting application layer access.

Verizon SDP is an ideal perimeter security solution for enterprises that operate global supply chains, have a large number of subsidiaries, handle regulated data or are US government vendors handling Controlled Unclassified Information (CUI). It can also be combined with endpoint protection systems and micro-segmentation to create secure enclaves that can withstand sophisticated inside and malware attacks.

With the ability to combine cyber security services, such as SDP and network services, such as SD-WAN, Verizon can help you gain additional benefits from the synergy of bringing these services together. Enterprise's not only enjoy significant application security and performance improvements by having Verizon as their global connectivity provider, but Verizon also offers its SDx services in a multi-transport-carrier environment via its ecosystem of leading service providers.

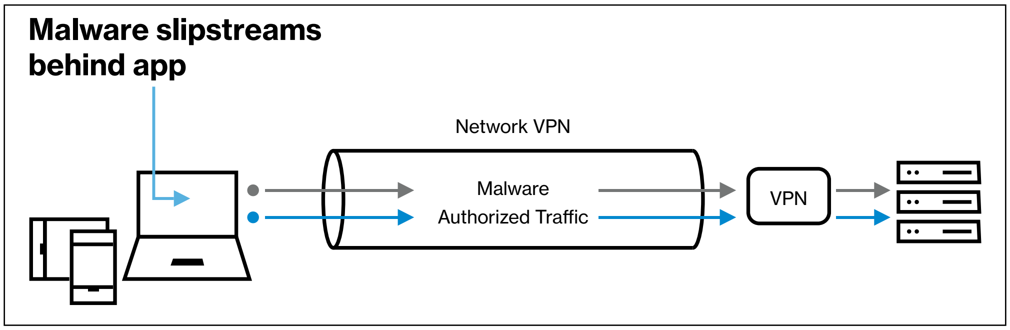
Emerging cyber threats.

For the past decade, perimeter security enterprises deployed a combination of VPN gateways and Firewalls with Multi-Factor-Authentication (MFA) step-up for external access control and NAC gateways for internal access. Unfortunately, the existing perimeter security model has two significant shortcomings. First, the growth of outsourcing and cloud computing has increased the operational complexity due to the requirement to authenticate and authorize an increasing number of external users connecting to external resources. Second, and perhaps more important, existing perimeter security systems are not able to block the new generation of malware that is able to propagate via authorized devices.

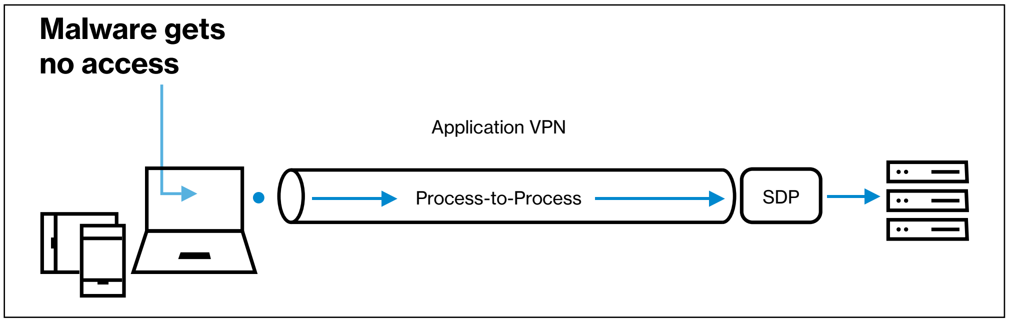
Traditionally, malware got into a user's device via a phishing attack. However, there is a new type of malware that can autonomously hunt for vulnerable devices across LAN, WiFi and VPN connections. 2017 saw three global-scale cyber-attacks involving lateral-moving malware attacks. For example, NotPetya started as a state-sponsored attack on Ukraine government computers but within a few days was impacting un-related companies around the globe. The key aspect that made NotPetya so lethal was its ability to spread device to device.

Verizon SDP can help protect application infrastructure against existing and newly emerging cyber threats. Existing attacks, such as credential theft and server exploitation, are blocked as Verizon SDP only allows access from devices registered to authenticated users. To combat the new generation of malware that propagates via authorized users, Verizon SDP only allows white-listed application processes on the user's device to connect to application infrastructure. Subsequently malware cannot utilize SDP connections to scan for protected application servers–even from the device of the authorized user.

VPN/NAC problem: malware attacks spread from authorized devices.

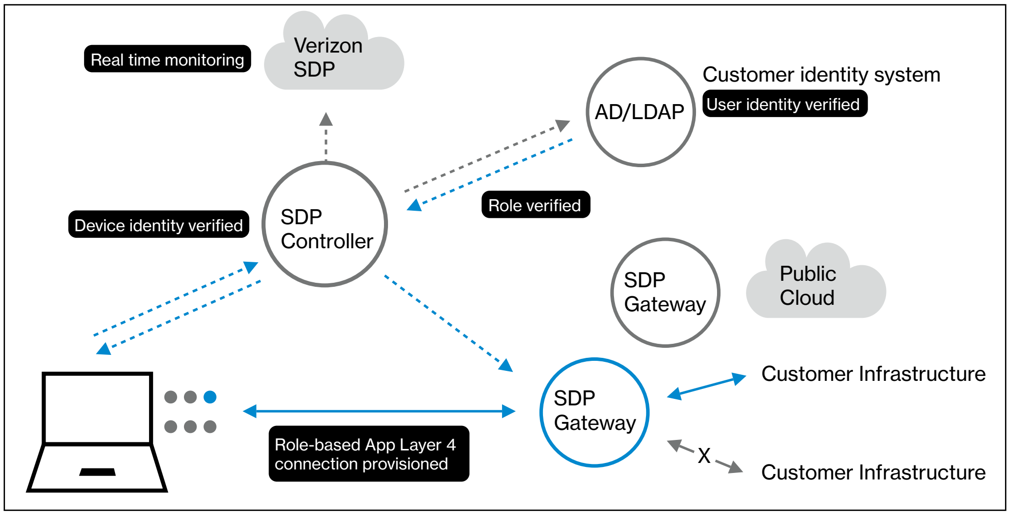


SDP Solution: malware blocked at source.



Software Defined Perimeter (SDP).

Software Defined Perimeter (SDP) represents a new concept in cybersecurity that creates a strong barrier around high value enterprise apps that helps prevent cyber attackers from breaking thru. Verizon SDP is based on the Software Defined Perimeter security architecture. Verizon teamed with Vidder, a leading developer of SDP software components, to create an effective network-based countermeasure against cyber attacks.



The first component of the SDP architecture is a Gateway that is deployed in front of either physical or virtual application resources. The SDP Gateway combines the functions of a Firewall, VPN and application layer gateway in a single virtual appliance. The SDP Gateway only allows approved software on authorized devices to connect to protected applications.

To allow users to connect to protected applications they must utilize the SDP Client. The SDP Client has three distinct purposes:

- To determine if the device and the user identity match.
- To allow remote analysis of software and system processes to detect the presence of malware.
- To provide a secure application layer connection between the user's device and one or more Gateways.

Tying the SDP Client and Gateway together is the Controller. The SDP Controller functions as a hub between the Client and Gateway, as well as external security controls such as the Identity, Issuing Certificate Authority and remote trust assessment systems.

SDP's interlocked security controls protect application resources and data from cyber-attacks. All SDP transactions are cryptographically certified to mitigate real time tampering. SDP's architecture has been rigorously tested in public hackathons as well as government labs.

Verizon SDP applications.

Verizon SDP is ideal for enterprises that operate global supply chains, have a large number of subsidiaries, handle regulated data or are government contractors.

Global supply chain and subsidiary networks.
Enterprises that utilize MFA and VPN to manage access to global supply chain network are vulnerable to the new generation of laterally moving malware that spreads from the devices of authorized users. While an enterprise may be able to deploy the latest generation of machine learning endpoint protection on head office devices, it is impossible to know the condition of a partner's device or distant subsidiary.

Verizon SDP is an ideal "over the top" security solution for global supply chain networks or enterprises with a large number of subsidiaries as malware cannot propagate thru it. Additionally for enterprises deploying regional clouds or hybrid infrastructure, the route optimization features of SDP means the best path is taken. Verizon SDP can also be deployed over a SD WAN service integrating MPLS/Internet/Broadband/LTE bandwidth to maintain application performance.

Public cloud deployment for financial and medical organizations.
One of the challenges financial and medical organizations face is meeting security requirements in virtualized cloud environments. For example, financial institutions need a data center with multiple physical controls, thus making it difficult for financial institutions to utilize public cloud services.

Verizon SDP provides these entities with the "equivalence" to physical barriers. SDP's set of interlocked security controls creates a secure enclave when combined with native cloud partitioning and encryption services enabling public cloud usage.

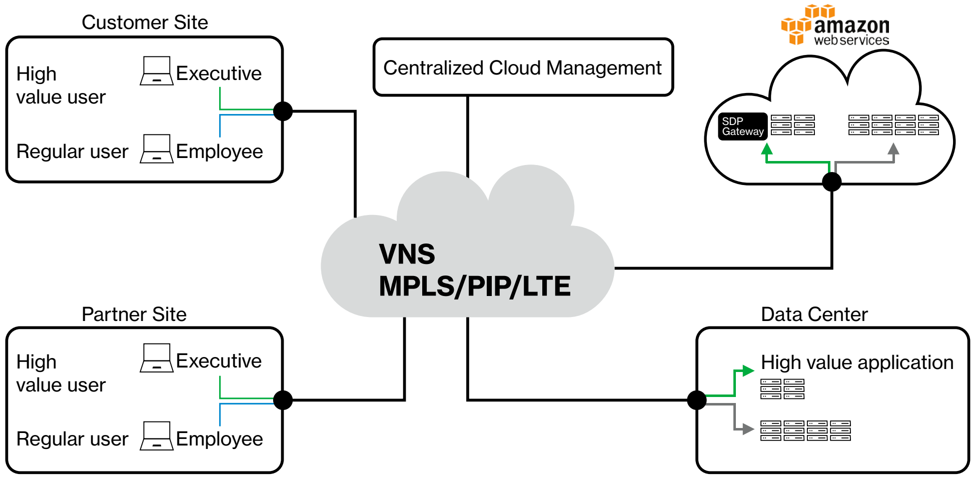
Secure enclaves for U.S. government vendors handling CUI.
State-sponsored cyber-attacks on U.S. government vendors have greatly increased as described in the National Security Strategy released on December 20, 2017. The U.S. government has mandated that all suppliers handling Controlled Unclassified Information (CUI) must implement NIST 800-171.

Verizon SDP is an ideal solution for protecting CUI by only allowing authorized users to access file servers. Verizon SDP supports the access control and monitoring requirements in NIST 800-171 in an integrated solution, and when Verizon SDP is deployed over SD-WAN or Private IP, U.S. government suppliers benefit from the added network security.

Verizon: your connectivity provider.

Enterprises universally seek to increase agility while improving their cost structure. Verizon provides enterprises a complete solution portfolio of application aware security services like SDP and SD WAN that help enterprises meet their strategic objectives of cost and risk reduction.

Looking to the near future, Verizon plans to offer SDP over Virtual Network Services (Verizon's version of NFV). The combination of SDP and SD WAN via VNS will provide even more flexibility and agility to enterprises at premise or cloud sites. Enterprises will enjoy significant application security and performance improvements by having Verizon become their global connectivity provider for SDP, SD WAN and VNS services.


Customer Site
High value user
Executive
Regular user
Employee
Centralized Cloud Management
amazon web services
SDP Gateway
VNS MPLS/PIP/LTE
Partner Site
High value user
Executive
Regular user
Employee
Data Center
High value application

verizon✓