Fact sheet

Hackers can’t attack what they can’t see.

Verizon Software Defined Perimeter

Cybercriminals want access to your critical applications and data right now. Their stealthy modus operandi is to prowl at the edge of your enterprise and attack any vulnerable entrance. They strike fast and frequently where employees and customers access your network, web and application servers or cloud services. But we can help you stop these cyber attacks at your virtual border, before they become a real problem inside your IT infrastructure.

With Verizon Software Defined Perimeter (SDP), you can automatically hide application resources and see attacks in real time to help stop attacks as soon as they start. You hear all too often about organizations discovering too late that they’ve been breached, hit with denial-of-service attacks, exploited by credential theft, attacked with server exploits, or pounded with connection hijacking attacks. Now you can defend your organization’s cyber edge from these growing threats.

Verizon Software Defined Perimeter (SDP) helps protect your frontline—where you can be hit the hardest by cyber attacks.

Connect users to applications—simply, securely and reliably

SDP is a cloud-based software as a service (SaaS), managed by Verizon. The service is designed to not just prevent cyber attacks, but also to give you secure access to protected applications regardless of where they live, but only if you’re an authenticated, authorized user. SDP provides secure, encrypted connections between your devices and applications built in real time.

Considering most organizations have gone virtual and left their well-defined physical boundaries behind, our SDP service also replaces physical security perimeters with logical components. And it can be deployed virtually anywhere and run under the control and policy of your application owners.

Your applications will be secure even in different cloud environments because they’re managed by unified security policies. You can also compartmentalize each access interaction based on dynamic policies, which can be context dependent. It’s ultra-secure access to applications at its finest.

Protect access with the ultimate virtual private network

Software Defined Perimeter is the first scalable, managed solution of its kind available today. It’s easy to deploy and can be customized to your unique business needs. SDP is an ideal virtual private network (VPN) solution for organizations of all sizes. It uses cloud-based controllers, gateways and the latest in software-defined perimeters for secure, dynamic virtual connectivity.

Our SDP service goes beyond traditional VPNs and perimeter defense techniques by hiding applications and critical resources in a high-trust environment. Many organizations today are moving their business applications to cloud data centers. Once there, they become limited-trust applications and less secure. Combine that practice with the widespread use of limited-trust mobile devices that are allowed to access internal business applications remotely from limited-trust locations, and the security challenges increase significantly.

You can quickly counter these security issues easily and automatically with our SDP solution. By taking the approach that users typically need to access only a certain set of applications or services, SDP permits you to only expose those services in a need-to-know model. Unlike a traditional VPN, SDP strips out DNS, DHCP and other network-based services that can enable discovery of other services and assets, thereby mitigating lateral movement once inside the enterprise.

Our SDP solution offers:

- Ultra-secure application access which can be defined around space, time, role, identity and persona (STRIPE).
- Virtual Federation across multiple identity stores.
- A real-time, assembled, need-to-know network making enterprise apps and resources invisible to devices until they’re authenticated, fingerprinted and authorized.
- An application-layer VPN: Get easy-to-use, cost-effective and highly encrypted connectivity between limited-trust devices and your most important applications.
- Dynamic VPN provisioning: Automatically deliver application VPN access policies without changes and updates to end devices in a centrally managed process.

Control application access with multi-level authorization

With a software-defined network framework, SDP automatically defines and authorizes access based on various and unique policy criteria. You're granted access to applications after multiple, dynamic levels of authentication. Multi-factor step-up methods can also be enabled in customized SDP deployment scenarios.

How SDP works

It's like getting VIP access to an exclusive private club. There are multiple bouncers at the door who check and double-check member devices and verify all IDs. Then, if you pass their approval, they escort you through body scanners into the club and show you where to get approved again to mix and mingle in a private area.

This is similar to what happens when our SDP Initiating Host on client devices and SDP Controller in our management and profile systems authorize credentials. If you pass their screenings, you get to continue with encrypted traffic to cloud service-provider gateways. Upon authorization, you get information about how to properly enter and interact with SDP Accepting Hosts or Gateways to access your applications, cloud services and other resources. Then, you can use them in a highly secured area

In addition to these access security features, SDP also provides:

- Logical separation of control and data planes
- Dynamic and secure session management
- Automatic secure tunnel setup to accepting hosts

Perimeter security designed to be virtually unhackable

Our simple, yet elegant approach to perimeter security creates an application access method that's incredibly powerful. Although it's possible to compromise individual security components, it's extremely 16difficult to compromise their combined power in SDP. It requires a highly skilled adversary attack on many fronts—Single Packet Authorization, Security Assertion Markup Language and Mutual Transport Layer Security, end-user devices theft—all at the same time.

All your applications, devices, IP addresses, ports and protocols are safeguarded from network-based attacks. In fact, SDP has already successfully endured multiple public hackathons. And more than 15 billion attacks were mitigated by our SDP over a 30-day period without any IP packets reaching any protected workload in public cloud locations. Yes, mission-critical business applications can in fact be distributed across multiple clouds, permitting authorized user access even while sustaining heavy attacks.

Let us adapt SDP to your organization's security and application access needs. Verizon can help you combat cyber attacks both inside and outside your enterprise, wherever your new perimeter happens to take you.

Verizon SDP delivers ultra-secure access to applications, plus real-time attack detection, mitigation and monitoring in a managed, as-a-service offering.

Contact your account representative today:

Find out how Verizon Software Defined Perimeter can give you ultra-secure access to your applications and keep cybercriminals locked out.

verizonenterprise.com