OPSWAT.

DATASHEET

Software Defined Perimeter

Securing the new perimeter

The digital business landscape is changing, and so has the need to protect it from a rapidly changing world of evolving threats. No longer are employees tied to a desk, nor are applications tethered to devices. The traditional network perimeter has expanded; so too should your ability to defend it.

Traditional threat-facing security infrastructure will have its place in networks for years to come. But according to Gartner, alongside these legacy technologies emerges the Software-Defined Perimeter, and the security around it will bring speed and agility to the enforcement of security policy regardless of the location of the user, the information or the workload. [1]

The Software Defined Perimeter

A traditional enterprise network with its fixed perimeter and walled-off architecture has largely allowed the devices, applications and services within it to remain secure from external threats. BYOD, IoT and SaaS models have all tested this traditional infrastructure by introducing blind spots in visibility, control of users and devices that need to access these internal resources.

The growth of devices moving inside the perimeter and the migration of application resources to outside the perimeter has stretched the traditional security model used by enterprises.

SafeConnect Software Defined Perimeter (SDP) renders an organization's critical IT infrastructure "invisible" or "dark"—meaning no DNS information or IP information is visible, and protected application resources cannot be detected from the Internet or other internal networks.

After all, you can't hack what you can't see.

Benefits

Easy to Install
No additional hardware or network integration required; rapid deployment and maintenance-free with 24/7 support

Zero-Trust/Least-Privileged
Greater security with Verify-First, Connect Second access to public & private cloud applications

Mutual TLS Encryption
Easier to deploy, high-performance VPN per-session application access

Control Beyond Your Perimeter
Prevent data loss from devices accessing your cloud application and data from outside your network perimeter

Decreases Network Attack Surface
Hide your applications from the Internet and corporate networks to mitigate DDoS attacks, credential theft, connection hijacking & data loss

Addresses Regulatory Compliance
PCI, HIPAA, SOC2, SOX, GLBA & GDPR compliant security controls

Predictable & Cost Effective
SaaS annual subscription model with term commitment discounts

OPSWAT.

SafeConnect SDP

Features

SDP's **Zero-Trust Access** model hides enterprise resources from the Internet and internal networks, and offers more secure "verify-first, connect second" authentication.

Multi-Factor Authentication and Identity Access Management integration delivers a streamlined, consistent user experience.

As a customer-provisioned cloud offering, SDP **deploys rapidly and comes with 24/7 support**, offering you maintenance-free security.

Includes **cloud-hosted SDP gateway connector** for Public Cloud SaaS applications.

On a **VMware virtual appliance or AWS AMI instance**, protect private cloud and internally hosted applications.

Components

- SDP Client – available for Windows, macOS, iOS and Android devices; can be distributed to managed devices or downloaded as part of the BYOD onboarding process.
- SDP Controller – cloud-hosted trust broker between the SDP Client and security policy controls such as IAM providers, Issuing Certificate Authority and Device Compliance.
- SDP Gateway – termination point for mutual TLS VPN connection from the Client, the Gateway is provided with the Client's IP address and Certificates after the identity of the requesting device has been verified and the authorization of the user has been determined by the Controller.

Use Cases

Legacy VPN Replacement

Zero-Trust security at a fraction of the price, without the throughput degradation that comes with VPN encryption

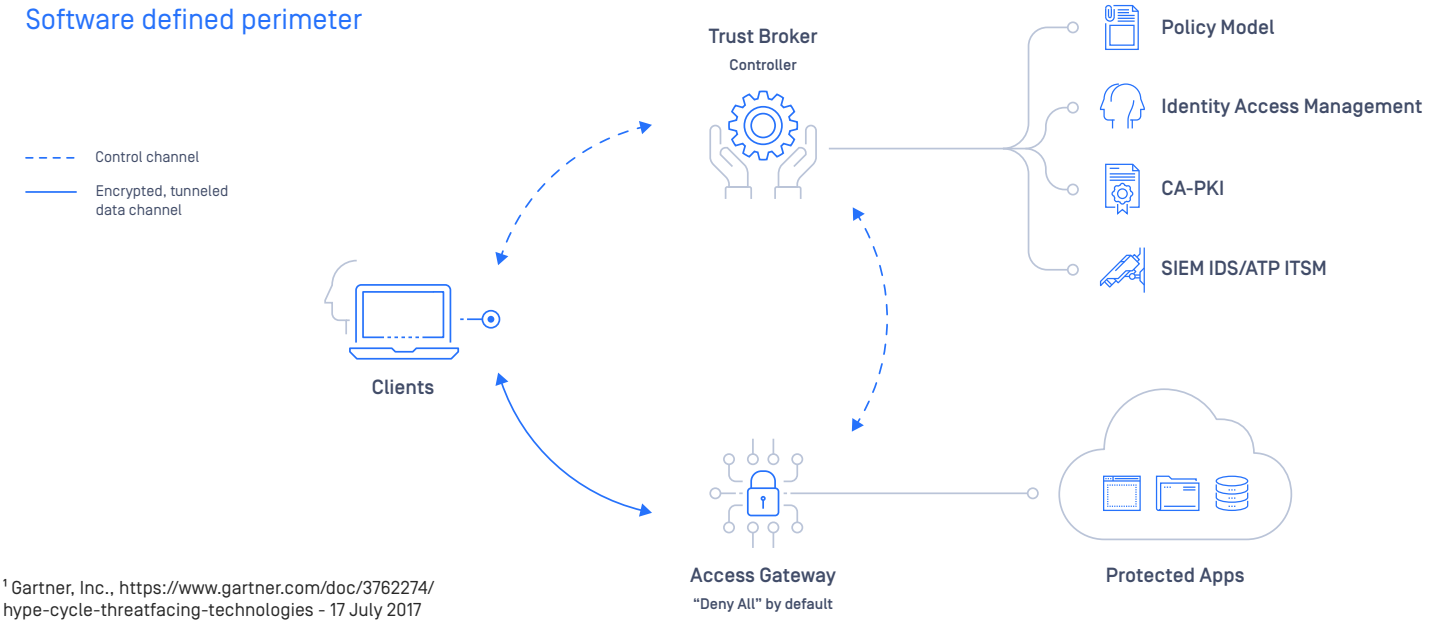
Beyond-Perimeter Cloud Access

Secure access to your public and private cloud resources from devices outside of the network perimeter with mutual TLS encryption

Protect Critical Applications & Data

Seamlessly integrate with existing network access control offerings for policy-driven access to exactly the data and applications needed, regardless of connection location

Software defined perimeter



[1] Gartner, Inc., https://www.gartner.com/doc/3762274/hype-cycle-threatfacing-technologies - 17 July 2017

OPSWAT.

Trust no file. Trust no device.

opswat.com/contact