Pulse Secure®

Zero Trust Secure Access SDP Solution

Pulse SDP delivers provisioning simplicity, scale, and superior economics for Hybrid IT

Highlights

- Direct secure access to applications and resources
- Deep user and device authentication and authorization
- Enhanced segmentation on per-application basis
- Seamless Zero Trust security architecture end-to-end

Customer Value

- Enhanced security profile & device compliance
- Defends against modern security threats & lateral spread
- Integrated secure access solution with simplicity, scale and lower total cost of ownership
- Improved user experience with application accessibility

"By offering an integrated secure access suite that supports VPN and SDP architectures for data center and cloud, Pulse Secure can provide strong value that can be compelling for customers and service providers."

Jon Oltsik, Senior Principal Analyst, Enterprise Strategy Group

Software Defined Perimeter (SDP) is an access architecture for today's modern application infrastructure. Data breaches are becoming more common and malware is increasingly sophisticated. Meanwhile digital transformation is expanding the boundaries of business to multi-cloud. Traditional defense-in-depth networks are no longer able to adequately prevent many threats. And, users are demanding 24x7 access to applications from a variety of BYOD devices whether they're in the office or on the road.

Pulse SDP™, an add-on solution to the Pulse Secure Access platform, enables direct secure access to individual applications regardless of location. It enforces a Zero Trust "Verification Before Trust" approach so that only authorized users – and their authorized devices -- are able to access resources. Centralized authentication and stringent policy controls enable such one-to-one, on-demand connections. The result?

- Numerous security threats like APTs and DDoS attacks are rendered obsolete.
- "Dark Cloud" support makes resources invisible to unauthorized users, reducing the attack surface.
- Centralized policy control allows per-application connections only to authorized users.
- Seamless co-existence with VPN access, via a single pane of glass and common client.

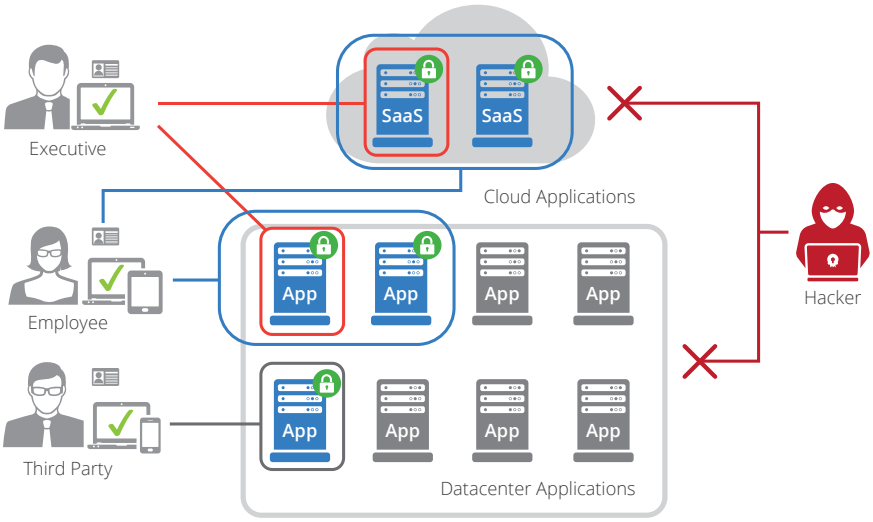

Figure 1: Application sprawl has expanded the attack surface

IT staff worldwide are under increasing pressure to respond to a mobile workforce demanding anytime, anywhere access. Applications are increasingly moving to the cloud, and the number of BYOD devices has exponentially increased. Together this has expanded the attack surface and introduced security and compliance challenges. The need to balance user access to sensitive applications with risk reduction has never been greater.

Today, modern enterprises must ensure:

- Data breaches don't occur and compliance is maintained.
- Users can get anytime, anywhere access to applications from a variety of devices.
- Applications are readily available to contractors and partners.
- Networks enhance business productivity, growth and development.

Pulse SDP Enables a Secure Modern Workforce

Today's modern businesses are about enablement: giving workers access to resources regardless of the constraints of location, time, or device. Pulse SDP extends and enhances Pulse Secure's Zero Trust capabilities by authenticating all users prior to accessing applications, restricting access to only specific applications by policy and rendering other resources "dark" — invisible to unauthorized users, threat actors and malware.

- Ensures that every connection is automatically encrypted.
- Delivers a seamless and friction-free user experience, because Pulse SDP uses our unified Pulse client.
- Protects and enables secure access for both multi-cloud and data center applications.
- Increases compliance by checking the security state of every device that attempts a connection.

Pulse SDP Use Cases

Pulse SDP streamlines and secures access to applications, likely the most critical aspect of delivering business productivity, continuity, and growth. Whether you're trying to seamlessly enable secure access for your mobile workforce, or faced with migrating applications to the cloud, Pulse SDP offers significant advantages to help businesses securely enable digital transformation.

Per-app Segmentation in Data Center & Private Cloud

The majority of enterprises today have a hybrid IT infrastructure with data and applications residing in the data center, private cloud, and public cloud. Pulse SDP offers enterprises the ability to tightly control access to applications regardless of location.

CHALLENGES	PULSE SDP SOLUTION
Grant direct access to specific applications on a per-user and per-device basis	Pulse SDP offers direct secure connectivity to specific applications and resources, without requiring VPN or access to the enterprise network. Moreover, it can restrict access on a per-user and per-device basis, further tightening security.
Enable secure access across cloud and data center applications	Pulse SDP is the only solution to provide granular access controls across cloud and data center applications from a single unified client.
Isolate critical applications	Pulse SDP allows administrators to isolate sensitive applications and render them "dark" so that unauthorized users are unable to access them. This reduces the attack surface and risk.
Migrate applications to the cloud	Deploying a virtual SDP proxy in AWS or Azure and granting specific privileges offers a rapid, flexible way of granting access to mission-critical applications and data without compromising security.
Co-exist with existing remote access VPN and NAC solution in data center	The SDP solution seamlessly co-exists with Pulse Connect Secure VPN and Pulse Policy Secure access control on-premises, via a single pane of glass and common Pulse client for access.

Privileged and 3rd Party Access to Apps From Anywhere

With increased workforce mobility and 3rd party access, the rapid influx of IoT into the enterprise, security risks have increased. Pulse SDP gives control back to administrators to secure network borders by enforcing Zero Trust. It does this by checking each and every endpoint before it connects, requiring deep user authentication and authorization.

CHALLENGES	PULSE SDP SOLUTION
Enable privileged access	Pulse SDP ensures that administrators can quickly enable and disable secure connectivity to users no matter their location, such as connecting temporary workers to specific applications or bringing up a new branch office quickly and seamlessly.
Enforce deep user authorization and authentication	Prevents data breaches caused by unauthorized users with authentication procedures that blend multi-factor, single sign-on, and device-specific policies. These can be used to restrict access based on specific device types and levels of authentication.

Direct, Secure Access to Public Cloud Apps

Pulse SDP offers users quick access to cloud applications like Salesforce or Office 365 via direct connections. This reduces network bandwidth and no site-to-site VPN is required.

CHALLENGES	PULSE SDP SOLUTION
Provide seamless application accessibility	Pulse SDP enables fast and responsive application access using a geographic proximity algorithm to connect authenticated users to the Pulse SDP Gateway closest to them. This ensures rapid connections and high throughput to increase worker productivity.
Increase worker productivity	Leveraging Pulse Secure's unified client means that workforces quickly and seamlessly access the applications they need, when they need them.

Key Features and Benefits

FEATURE	BENEFITS
Dual-mode VPN and SDP architecture	Pulse Secure provides enterprises with a single pane of glass management and operational visibility across public, private cloud, and data center.
Extensive multi-factor authentication (MFA) and authorization options	Pulse SDP ensures users, their devices, and the applications they access are continuously verified before and during transactions.
Uniform policy management	Enables consistently provisioned secure connections that increase usability and security while reducing configuration errors, policy drift, and gateway sprawl.
Granular, stateful access enforcement	Aligns business and compliance requirements with on-demand, application-level access that supports anytime, anywhere access and preferred device.
Enhanced user experience	Offers users easy and seamless access options including web portal, application-activated, single sign-on (SSO), and captive portal.
Access responsiveness	Control and data plane separation ensures scalability with proprietary Optimal Gateway Selection™ technology to expedite application delivery.
Deployment flexibility	Freedom to move or extend on-premise implementation through public and private cloud, or with a hosting provider or managed service provider of choice.

Pulse SDP is a simple software upgrade

to new or existing Pulse Secure infrastructure. Available using physical or virtual appliances, Pulse SDP can be deployed in your data center, Amazon AWS, or Microsoft Azure clouds.

How SDP Works - Next-generation Secure Access

Pulse SDP is comprised of an SDP Controller, SDP Client and SDP Gateway which are enabled within the Pulse Secure software, hardware and cloud solutions. This approach allows SDP and perimeter-based VPN functionality to work in parallel and provides Zero Trust access security and essential operational flexibility for enterprises and service providers. Pulse SDP is available in the Advanced and Enterprise Suite of the Pulse Secure Access Platform.

With a simple software upgrade, customers can activate Pulse SDP using the latest Pulse Secure infrastructure.

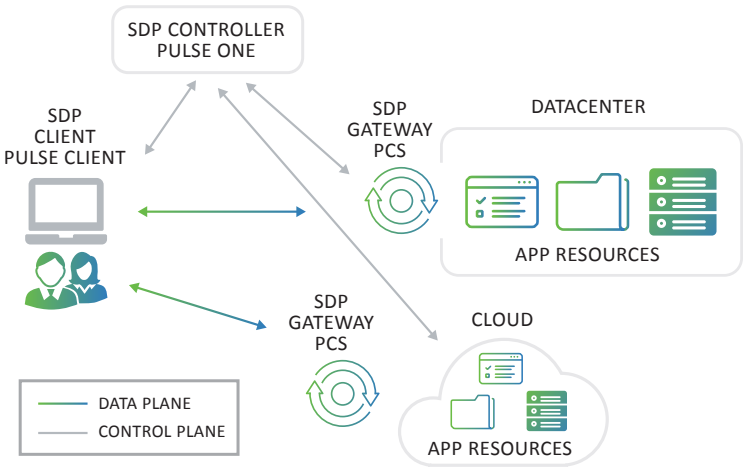

Figure 2: The Pulse SDP Architecture

Pulse Secure Access Suites

ESSENTIALS	ADVANCED	ENTERPRISE
DATA CENTER SECURE REMOTE ACCESS	ESSENTIALS PLUS: MOBILE SECURITY, CLOUD ACCESS & VISIBILITY	ADVANCED PLUS: DEVICE & NETWORK SECURITY
	PULSE SDP	PULSE SDP

CHOOSE YOUR PLATFORM: PHYSICAL VIRTUAL CLOUD

Add the Power of SDP to Your Environment

Find out how Pulse SDP can add seamless Zero Trust secure access across your security environment. Schedule a customized demo by contacting us today: call (408) 372-9600 or send an email request to info@pulsesecure.net.

Pulse Secure®

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
(408) 372-9600
info@pulsesecure.net
www.pulsesecure.net

ABOUT PULSE SECURE

Pulse Secure provides easy, comprehensive software-driven Secure Access solutions for people, devices, things and services that improve visibility, protection and productivity for our customers. Our suites uniquely integrate cloud, mobile, application and network access to enable hybrid IT in a Zero Trust world. Over 20,000 enterprises and service providers across every vertical entrust Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net.

linkedin.com/company/pulse-secure
www.facebook.com/pulsesecure1
twitter.com/PulseSecure
info@pulsesecure.net