Market Insights

Security & Risk Management

Market Insights: Software Defined Perimeter (SDP) for Zero Trust Network Security, 2020

Market Overview and Vendor Landscapes

April 2020

Abridged Report Compliments of Pulse Secure

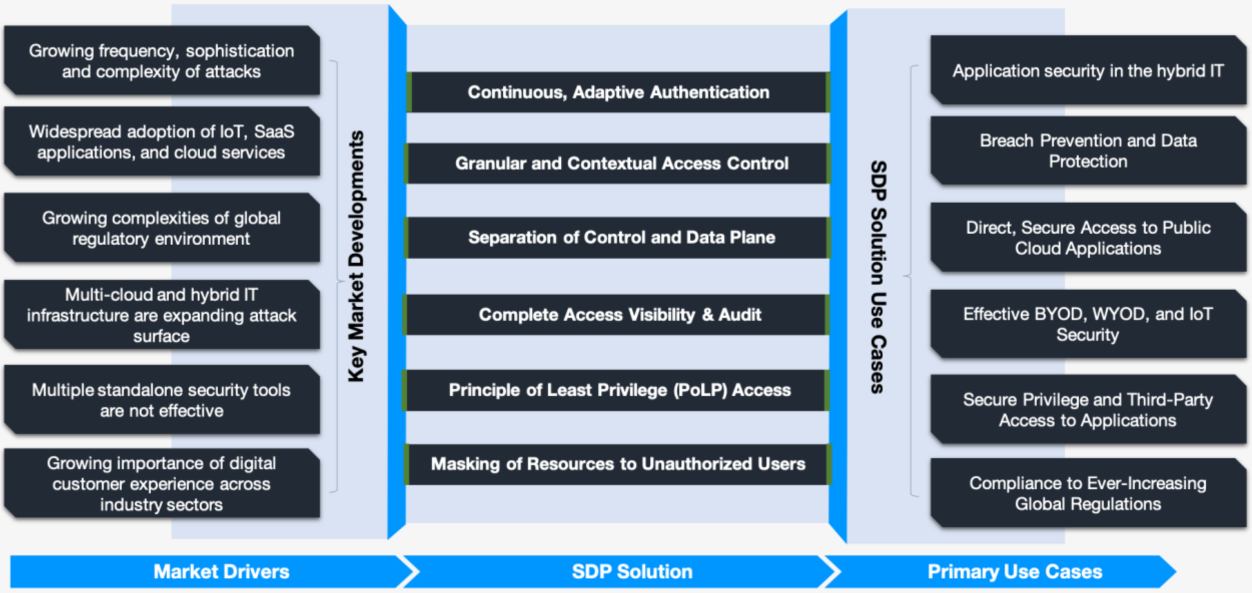
Table of Contents

Software Defined Perimeter (SDP) for Zero Trust Network Security

Zero Trust is a network security concept based on a foundation of strict verification of users, devices, applications, and network infrastructure. It requires that every access request by users or devices is fully securely authenticated and authorized before granting access. Zero Trust framework became popular in the wake of data breaches and modern cyber-attacks. It contends that no entity, whether inside or outside a network perimeter should be trusted without verification. The conventional security practice focused on creating a network perimeter to defend resources and trust entities on the inside, where everything outside the perimeter was untrusted. This model assumed that those inside the perimeter are inherently trusted and gave them more unfettered access to internal resources. This model couldn't adapt to the dynamics of virtual and cloud computing, as well as changing threat landscape with more advanced, coordinated outside attackers and malicious insiders trying to move laterally within the network perimeter to exploit important resources.

To address these challenges, the Zero Trust model treats all access requests without inherent trust and gives access permission on a strict need-to-know, least privilege basis. Traditional perimeter-based security models employ tools, such as firewalls, that focus defensive measures on checking entities originating outside the perimeter. This could give users and devices greater latitude within the networks, subnets and

Software-Defined Perimeter (SDP): Market Drivers, SDP Solution, and Primary Use Cases


Growing frequency, sophistication and complexity of attacks
Widespread adoption of IoT, SaaS applications, and cloud services
Growing complexities of global regulatory environment
Multi-cloud and hybrid IT infrastructure are expanding attack surface
Multiple standalone security tools are not effective
Growing importance of digital customer experience across industry sectors
Key Market Developments
Continuous, Adaptive Authentication
Granular and Contextual Access Control
Separation of Control and Data Plane
Complete Access Visibility & Audit
Principle of Least Privilege (PoLP) Access
Masking of Resources to Unauthorized Users
SDP Solution Use Cases
Application security in the hybrid IT
Breach Prevention and Data Protection
Direct, Secure Access to Public Cloud Applications
Effective BYOD, WYOD, and IoT Security
Secure Privilege and Third-Party Access to Applications
Compliance to Ever-Increasing Global Regulations
Market Drivers
SDP Solution
Primary Use Cases

Source: Quadrant Knowledge Solutions

virtual zones. Even if used for further network segmentation, employing multiple firewalls for internal segmentation can be cumbersome and challenging to scale.

The large-scale adoption of cloud and hybrid IT computing by organizations is pushing the network boundary to the cloud and with users accessing applications from the device of their choice; there is a dire need to protect these distributed data center and cloud-based resources. With the definition of network perimeter constantly changing, conventional remote access security, such as next-generation firewall (NGFW) and VPN are being challenged. In the world where business requires anytime, anywhere, anyhow user access, organizations need to consider alternative secure access approaches that can be more agile and adaptive.

In 2014, Cloud Security Alliance started an ongoing project aimed at further modernizing network security. So rather than trusting insiders and creating fixed perimeter security for outsider entities, the new approach would assume everyone as untrusted. All applications would be hidden, and access would only be granted after authenticating and authorizing every endpoint request. This new model of network security is called Software Defined Perimeter.

Software Defined Perimeter is an approach in network security that safeguards user access to application and information irrespective of the location, time and nature of the device used. Software Defined Perimeter follows zero trust approach, wherein the default network security posture is that of deny. Access is granted upon authenticating and authorizing both user and device. By pre-authorizing users and devices prior to making the application layer access (applications and resources), SDP protects enterprises from a range of attacks, such as denial of service, credential theft, server exploitation, connection hijacking and APT/Lateral movement. Unlike security models that work at the network layer, SDP works to the application layer. It provides granular control for secure communications directly from the user and device to the application. Users are only allowed to see and access resources that they are authorized to access.

Followings are the key characteristics of Software Defined Perimeter solution:

- **Zero Trust Alignment**: SDP strictly follows the principle of "trust nothing, verify everything". Any access attempt is checked and validated before resources are made visible to the entities. Also, entities can only access the resources and applications allowed by the SDP controller. All other resources are invisible to the user. Thus, SDP adopts the principle of least privilege (PoLP).

- **Granular and Contextual Access Control**: SDP provides fine-grained and contextual access policy. Access is permitted on evaluating context such as: user and device trust which includes identity authentication, role, device authentication and security, location and time of the day. Less advanced network security systems based on IP address have limited user, device and other access context.

- **User-Centric**: Software Defined Perimeter is a user-centric approach, as it validates the user and the device before granting any access. SDP allows organizations to make access policies based on user attributes. This way, each user, when trying to connect gets a personalized perimeter, which is dynamic and based on user context. This significantly reduces the attack surface and provides better protection than traditional network security systems that are based on just IP addresses.

- **Dark Network Defense**: To make the model robust and immune to attackers, SDP architectures can use protection mechanism, such as Single Packet Authorization (SPA) and mutual Transport Layer Secure (mTLS). By leveraging SPA and mTLS, information about infrastructure as well as requestor’s IP address and connection can be encrypted and validated prior to establishing a connection. SDP components, such as the controller and gateway, are protected through SPA and mTLS. As a result, applications and infrastructures are rendered invisible/inaccessible to the user and devices until authorized by controller for each transaction. These protection mechanisms offer benefits like service darkening, zero-day protection, and protection from DDoS attacks.

- **Consistent Meaningful Policies**: SDP helps to set up access policies that are relevant and meaningful. Unlike conventional IP-based access policies, SDP enforced access policies are based on user and device context. These policies describe which users are permitted to access resources and under all situations. SDP policies are designed to give users "just enough" access to resources and application. These policies apply universally for users across on-premises and cloud-based environments.

- **Separate Control and Data Planes**: SDP has a different control plane and data plane. Identity of user and posture of the device is verified via the control plane, post authorization, the data plane tunnel is established for data transfer. By keeping the control and data plane separate, SDP hides the protected assets. This reduces all the network-based attacks, as attackers can't attack what they can't see. Separating the control and data planes also increases scalability and application responsiveness.

- **Application-level Access**: SDP facilitates application-level access, where the controller holds the policy to authorize user and device access to applications. Unlike IP-based network security approaches that often provide broader, network-level access, users and devices can only directly access specific applications and resources as permitted by the policy.

The debate of SDP as a complete replacement over VPN (in particular SSL-VPN), that SSL-VPN is insecure, or SSL-VPN lacking Zero Trust capabilities – is all moot. SSL-VPN is a proven, widely used tool for secure remote access. Advanced SSL-VPNs operate at the application layer and offer Zero Trust functionality. It can incorporate identity and device authentication, and security compliance before access and during a connection with support for Multi-Factor Authentication (MFA) and Single Sign-On (SSO). It does offer centralized administration and enforcing granular, contextual access policy to specific applications and resources. It can operate in client and browser-based modes, and certainly supports cloud and data center application access. It can be set up to minimize and even eliminate end user interaction e.g. always active tunneling.

Therefore, the SDP and VPN question for enterprises is determined by such considerations as: the use cases, the applications to be supported, the extend of hybrid IT infrastructure, an organization's current resource investment in SSL-VPN and other existing network security tools (e.g. DLP), and whether the business is adverse to controls being sent outside of its network.

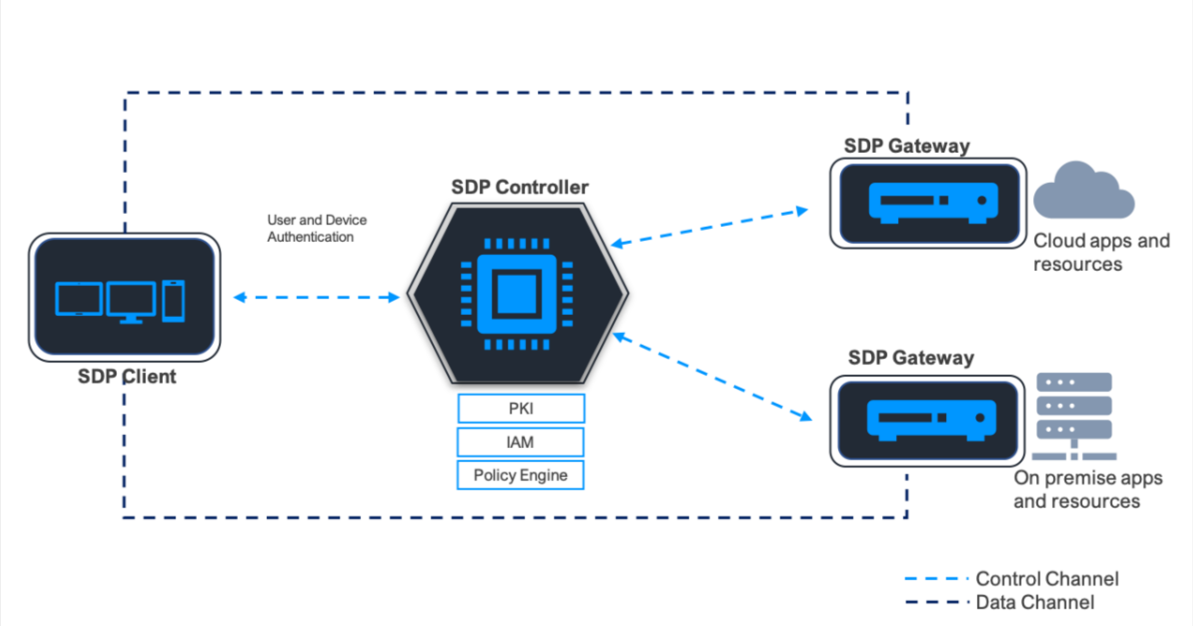
VPN versus SDP: While SDP offers additional advantages, it does not address all considerations for every enterprise, application, or use case. Today, SDP products, for the majority of enterprises migrating to the cloud, are more likely to co-exist with VPN for access security. See further details in Market Recommendations section.

SDP Architecture for Zero Trust Network Security

SDP architecture consists of three components: SDP client, controller and gateway. The client is essentially SDP software installed on devices like laptops, tablets and smartphones. SDP gateway protects the data center (network) and cloud application and resources. SDP controller is the central authentication point and policy engine. It acts as an interface between the client and the gateway; while keeping track of all the users, devices, applications and infrastructure. In the secure control plane, the controller initiates client authentication and, if valid, provides the client with access to permissible applications. SDP gateway is a physical appliance or virtual machine located close to the resource. SDP gateway rejects all communications from all endpoints other than SDP controller. SDP controller processes information about the user, device security state and geolocation from the client, compares to application access policy, and if valid, send access authorization information to the gateway in the secure control plane.

SDP controller and gateway are protected, using mechanisms such as Single Packet Authorization (SPA) or Mutual Transport Layer Security (mTLS), in order to make these systems invisible/inaccessible to unauthorized users and devices.

Software-Defined Perimeter (SDP) for Zero-Trust Network Security



Source: Quadrant Knowledge Solutions

As an SDP client connects to the network, it is authenticated by the SDP controller. SDP controller works as a trust broker between the client and the enterprise identity management system. SDP controller is connected to various authentication and authorization services. When a device connects to the SDP controller, the SDP client shares a SPA packet/mTLS with the controller which contains information to verify the user and device. Post that the controller identifies a list of resources or applications the client is authorized to access. Then the controller communicates with the gateway to allow user access. The controller helps the client and gateway establish a secure connection using mTLS. Once the connection is established, the client can securely access the applications. The client communicates directly with the gateway via the data plane without the traffic flowing through the controller. This approach reduces the attack surface as all the resources and applications are initially hidden or rendered 'dark'. Only after extensive authentication and authorization, users can access the allowed applications via a secured data plane.

There are some vendors that have applied a different or variant of the SDP architecture to support Zero Trust. It is important that whichever SDP solution, and its underlying Zero Trust architecture, a company chooses to implement, it should integrate with the organization's existing network, cloud and security infrastructure. Two other architecture examples for zero trust network security are:

Network Micro-Segmentation: Micro-segmentation or network micro-segmentation is slicing the network into small logical segments and controlling access to applications and data on those segments. Dividing the network into smaller segments reduces the attack surface for malicious attackers. Micro-segmentation policies are based on logical attributes or resource identity as opposed to the user's identity or IP addresses. Micro-segmentation creates an intelligent grouping of workloads based on their characteristics. It provides centralized dynamic policy management across networks, independent of the infrastructure. Vendors leveraging network micro-segmentation to achieve zero trust network security often utilizes the concept of software-defined networking (SDN), network overlays, and such others to create micro-segmentation of enterprise network for improved network security, data security, and application performance.

Identity Aware Proxy (IAP): IAP architecture provides access to applications through a cloud-based proxy. It follows the principle of least privileged access like SDP, but applications are accessed through standard HTTPS protocols at the application layer. Unlike SDP that uses direct tunnel for data transfer, IAP architecture provides authenticated and authorized secured access to particular applications using a proxy layer.

Google was the first one to implement Zero Trust security architecture in their business using BeyondCorp, through an Identity Aware Proxy model. BeyondCorp is their internal network and access security platform designed for employees to access internal resources. BeyondCorp is a web proxy-based solution that supports HTTP, HTTPS, and SSH protocols. Following BeyondCorp, Google also launched Cloud

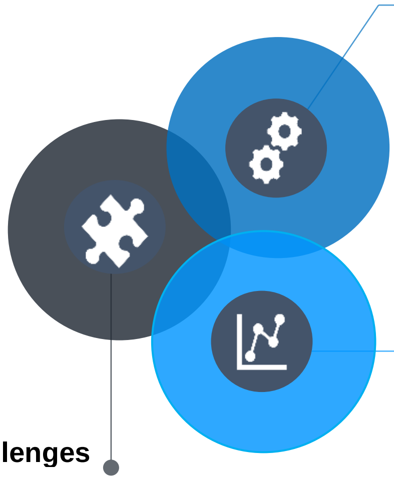
Identity Aware Proxy for access control and protecting data in the cloud. Cloud IAP shifts access controls from the network perimeter to individual users.

Factors Influencing Technology Developments and Market Growth

The following factors are influencing the overall technology developments around zero trust network security model and significantly contributing to the market growth:

Massive Proliferation of IoT Devices, BYOD, and WYOD in the Enterprise Network

Massive Proliferation of IoT Devices, BYOD, and WYOD in the Enterprise Network is Driving the Emergence of Next-Gen Security Technologies



Market Developments

- Enterprise organizations are looking at adopting an advanced security solution for effective protection of smart IoT devices, BYOD, and WYOD without compromising on the user experience.
- Organizations are looking at comprehensive authentication and authorization of managed and unmanaged devices in the enterprise network.

Trends

- Zero Trust Network Security model follows the principle of "Trust Nothing, Verify Everything" to provide unmatched security to a wide variety of IoT and BYOD devices.
- SDP solution follows a zero trust secure access model and is expected to find widespread adoption amongst the enterprise organization in the next three to four years.
- Several organizations are already deploying and testing SDP solutions for various use cases.

Challenges

- Massive proliferation of IoT devices, BYOD and WYOD phenomenon in the enterprise network is resulting in more and more unsecure endpoints and significantly expanding the attack surface.
- Security challenges are amongst the biggest roadblock of the digital transformation strategies.

Challenges → **Market Developments** → **Trends & Outlook**

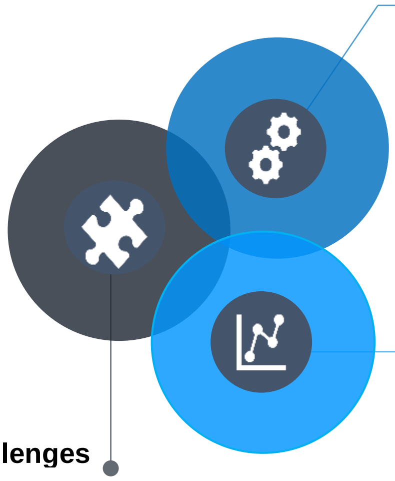
Source: Quadrant Knowledge Solutions

In the era of globalization to increase employee's efficiency and productivity, organizations are offering a higher level of mobility and flexibility. This has resulted in the increasing popularity of IoT devices, BYOD and WYOD phenomenon in the enterprise network. Owing to the BYOD and WYOD phenomenon, more and more people are connecting their mobile devices like smartwatches, tablets, smartphones and others to the enterprise network. This has increased the number of unsecured endpoints and expanded the attack surface. Since the number of managed and unmanaged devices connected to the network is much higher today, there is a dire need for an advanced security solution to protect IoT devices, BYOD and WYOD without hindering user experience. Organizations are looking at comprehensive authentication and authorization of managed and unmanaged devices in the enterprise networks.

A Software Defined Perimeter solution solves this problem by following the principle of "trust nothing, verify everything". By ensuring that all users and devices are authenticated and authorized before permitting access, SDP secures the vast array of IoT & BYOD devices like never before.

Protection Against Growing Frequency, Sophistication, and Complexity of Attacks Require Zero Trust Security Approach

Protection Against Growing Frequency, Sophistication, and Complexity of Attacks Require Zero Trust Security Approach



Market Developments

- Traditional perimeter-based security infrastructures are not designed to handle the modern, sophisticated and complex attacks.
- Attackers are leveraging sophisticated tools leveraging automation, AI and machine learning to launch security attacks.
- SDP solutions have emerged as a promising solution to address modern security attacks.

Trends

- SDP solution provides granular and contextual access control and performs continuous, adaptive authentication to provide comprehensive security against modern threats.
- SDP solution makes application and resources invisible to unauthorized users, and access is granted after authentication and authorization of every endpoint requests.

Challenges

- Data breaches, DDoS and ransomware attacks are making headlines on a regular basis, increasingly causing significant concern amongst the organizations.
- With the advancements of technologies, attackers are using advanced tools and technologies to launch sophisticated and complex attacks.

Challenges → **Market Developments** → **Trends & Outlook**

Source: Quadrant Knowledge Solutions

Data breaches, DDoS and ransomware attacks are not only increasing in frequency but also becoming more sophisticated and complex. With the advancements in IT and security technologies, cybercriminals are increasingly utilizing advanced techniques to launch sophisticated, complex, and targeted attacks. For cybercriminals, the integrated power of IoT botnets, automation, and AI and machine learning tools will enable them to cause next wave of prominent and dangerous attacks to launch DDoS attacks, gain unauthorized access to enterprise network and resources, and perform information theft. The advanced AI-based hacking tool will help them find and exploit the new vulnerabilities for their target organizations.

Ransomware attacks are growing in number and are becoming sophisticated. Cybersecurity research has tracked over 1000 different types of ransomware variants, and the numbers are continually increasing. Some of the popular ransomware are WannaCry, Bad Rabbit, Cerber, Dharma, GandCrab, Jigsaw, Katyusha, LockerGoga, PewCrypt, Ryuk, SamSam, Crysis, CryptoWall, GoldenEye, Locky, and such others. While Ransomware attacks may become less frequent in the coming years, it is increasingly becoming more targeted and sophisticated to cause more considerable damage to the target organizations.

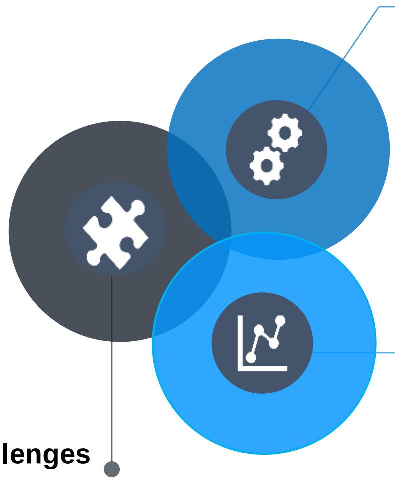
Since the traditional perimeter-based security models are not equipped to handle these complex and sophisticated modern attacks, organizations need access model to be more robust, reliable and agile. A Zero Trust SDP solution addresses this problem by providing a holistic security architecture. By providing granular and contextual access control and performing continuous adaptive authentication, SDP offers comprehensive security against modern threats. By making applications and resources invisible to unauthorized users and granting access post-authentication & authorization of every endpoint request, SDP drastically reduces network-based attacks.

Cloud and Hybrid IT Infrastructures are Expanding Attack Surface

Growing adoption of multi-cloud and hybrid IT environment is considerably increasing the enterprise attack surface. Organizations are looking at enhancing their threat defense measures to address ever-growing security risks, internal threats, external malware, and compliance requirements associated with hybrid IT infrastructure. With applications and infrastructure moving to multi-cloud and hybrid locations, organizations are looking for measures to protect these resources from attacks and at the same time make sure that authentic users get uninterrupted and seamless access. Organizations are required to manage multiple devices and access points to secure access to cloud application and resources.

Enterprises are embracing zero trust security philosophies of comprehensive authentication and authorization of users and devices prior to access. An SDP solution provides direct and secure access to public cloud application & resources and hence is becoming the popular security measure for hybrid IT environment.

Cloud and Hybrid IT Infrastructure are Expanding Attack Surface



Market Developments

- With applications and infrastructure moving to multi-cloud and hybrid locations, organizations are looking for measures to protect these resources from attacks and at the same time make sure that authentic users get uninterrupted and seamless access.
- Organizations are required to manage multiple devices and access points to secure access to cloud application and resources.

Trends

- Enterprises are embracing zero trust security philosophies of comprehensive authentication and authorization of users and devices prior to access.
- SDP solutions provide direct, secure access to public cloud application and resources and thereby is becoming a popular security measure in the hybrid IT environment.

Challenges

- Growing adoption of multi-cloud and hybrid IT infrastructure is significantly expanding the attack surface.
- Cloud and Hybrid IT environment is leading to growing security risks, internal threats, external malware, and compliance requirements.

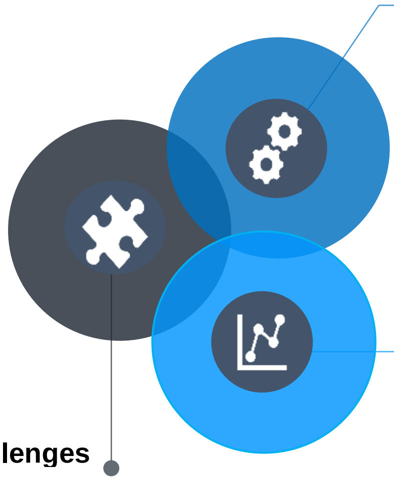
Challenges → **Market Developments** → **Trends & Outlook**

Source: Quadrant Knowledge Solutions

Presence of Multiple Standalone Security Tools are Not Effective in Addressing Modern, Complex Threat Landscape

In the age of digital transformation and evolving threat landscape, large enterprise organizations with the presence of multiple standalone security tools are facing challenges in defending against advanced threats. Application deployment in the hybrid IT, on-premise and multi-cloud environment within the organizations are significantly adding to application security, data security, and privacy challenges. Organizations are dealing with multiple security tools to address security-related concerns for different environments. Applying the existing data center policies for IaaS and SaaS situations is resulting in limiting network visibility, leading to multiple security gaps and vulnerabilities, and causing unpleasant user experience. Cybercriminals are continuously looking to exploit security gaps and vulnerabilities to launch numerous cyber-attacks. Thereby, organizations are continually looking at implementing a robust, integrated security strategy. A robust SDP solution provides a framework to implement enterprise-wide integrated security strategies to protect applications and resources deployed across the complex IT infrastructure environment. SDP integrates discrete architectural elements like user-aware applications, client-aware devices and network-aware gateways, and works effortlessly in hybrid IT and multi-cloud environments.

Presence of Multiple Standalone Security Tools are not Effective in Addressing Modern, Complex Threat Landscape



Market Developments

- Cybercriminals are continuously looking to exploit security gaps and vulnerabilities to launch multiple cyber-attacks.
- Organizations are continuously looking at implementing a robust, integrated security strategy.
- SDP solution provides a framework to implement enterprise-wide integrated security strategies to protect applications and resources deployed across the complex IT infrastructure environment.

Trends

- Organizations are increasingly evaluating SDP technologies and its value proposition of integrating discrete architectural elements, like user-aware applications, client-aware devices and network-aware gateways and to ensure robust security and user experience in a multi-cloud, hybrid environment.
- SDP solutions are increasingly becoming a part of an enterprise integrated security strategy.

Challenges

- Application deployment in the hybrid IT, on-premise and multi-cloud environment within the organizations are significantly adding to application security, data security, and privacy challenges.

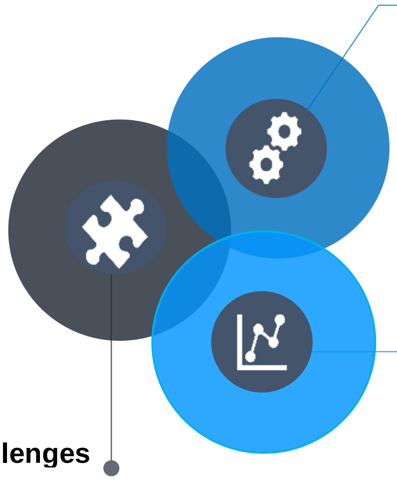
Challenges → **Market Developments** → **Trends & Outlook**

Source: Quadrant Knowledge Solutions

SDP Solution Effectively Provides Application and Data Security with No Physical or Virtual Boundaries

With organizations going global and operating from multiple locations worldwide, applications and resources need to be accessible from anywhere. While global organization are becoming boundaryless, they are facing the challenge of data security as resources can operate anywhere, and they need to be accessible from everywhere. With an increasing number of contractors, suppliers and vendors accessing the company's resources, securing third-party access are becoming increasingly important. SDP solution provides fine-grained and contextual access policy allowing secure connection based on who can connect from what devices and to which resources. SDP gateway ensures that data and applications are secured regardless of where it is stored.

SDP Solution Effectively Provides Application and Data Security with No Physical or Virtual Boundaries



Market Developments

- With organizations operating from multiple locations, applications and data need to be accessible from anywhere
- Organizations are increasingly adopting cloud to reduce cost, mitigate risk and achieve scalability
- With an increasing number of contractors, suppliers and vendors accessing the company’s resources, securing third-party access are becoming increasingly important.

Trends

- SDP solutions provide fine-grained and contextual access policy, thus allowing safe connection based on who can connect from what devices and to which resources.
- SDP gateway ensures data and applications are secure regardless of where it is stored

Challenges

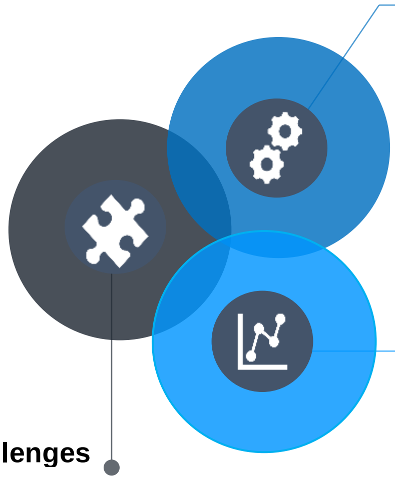
- The Global organization knows no physical boundary and face the challenge of data security as resources are stored in and accessed from multiple locations
- Organizations need to secure their applications and data everywhere- be it on-premise, public or private cloud.

Challenges → **Market Developments** → **Trends & Outlook**

Source: Quadrant Knowledge Solutions

Global Regulations and Compliance Requirements are Increasingly Becoming Complex

Global Regulations and Compliance Requirements are Increasingly Becoming Complex



Market Developments

- The global regulatory compliance requirements and scrutiny of auditors continue to become stringent.
- The emergence of strict data privacy regulation driven by GDPR, CCPA, and others are causing businesses to adopt advanced security and compliance solution.
- Organizations are continually looking at adopting an advanced security solution to improve their defense strategies and compliance with stringent regulatory requirements.

Trends

- SDP solutions are expected to find widespread adoption in the next three to five years to improve organization's overall security strategies and compliance requirements.
- SDP solutions improves compliance data collection, reporting and auditing by centrally controlling secure connections between users and resources, and capturing related access activity to sensitive information.

Challenges

- Numerous compliance frameworks, such as NIST, FISMA, HIPAA, PCI-DSS, and others, are significantly impacting the overall enterprise security strategies across industry verticals and geographical regions.
- A non-compliance can result in a higher risk of information theft, fines, liabilities, negative publicity, and more.

Challenges → Market Developments → Trends & Outlook

Source: Quadrant Knowledge Solutions

Numerous compliance frameworks, such as NIST, FISMA, HIPAA, PCI-DSS, and others, are significantly impacting the overall enterprise security strategies across industry verticals and geographical regions. While compliance with global, country and industry regulations can help improve an organization's security posture, non-compliance can result in a higher risk of information theft, fines, liabilities, negative publicity, and more.

Additionally, EU's General Data Protection Regulation (GDPR) ushered in a global standard in data privacy with extensive specifications and potential penalties. GDPR not only kept the businesses busy restructuring their policies to comply, but also started a wave of privacy regulation across the globe. In line with GDPR, California has introduced its data privacy law- CCPA (California Consumer Privacy Act). CCPA holds businesses in California accountable for how they collect, share and secure personal consumer data. Additionally, 11 states of the US passed legislation to strengthen their data privacy laws. Other countries like Australia and Canada also followed suit in updating their consumer data privacy laws. Going forward, businesses should expect more of the same as the rest of the world also gears up in response to increasing public pressure against data breaches and exfiltration.

SDP solution can significantly help organizations ensure adherence to ever-changing industry and regulatory compliance specifications. SDP solutions improves compliance data collection, reporting and auditing by centrally controlling secure connections between users and resources, and capturing related access activity to sensitive information.

Vendor Landscape

Following are detailed profiles of the key SDP vendors with a global impact. Quadrant analyst team derived and assessed this information based on numerous interviews conducted with various SDP vendors, consultants, as well as reviewing secondary research. A detailed vendor profile and analysis, along with various competitive scenarios, is available as a custom research deliverable to our clients. Users are advised to directly speak to respective vendors for a more comprehensive understanding of their technology capabilities. Users are welcome to consult Quadrant Knowledge Solutions to support their purchase decision process regarding SDP technology and vendor selection based on findings within this research report.

Vendor	Founded	Headquartered	Product
Akamai	1998	Cambridge, MA	Intelligent Edge, Enterprise Application Access (EAA)
BlackRidge Technology	2010	Reno, Nevada	Transport Access Control
Cato Networks	2015	Tel Aviv, Israel	Cato Cloud
Cisco (Duo Beyond)	1984	San Jose, CA	Duo Beyond
Cyxtera	2017	Addison, Texas	AppGate SDP
Google	1998	Mountain View, CA	BeyondCorp, Cloud IAP
Impulse (acquired by OPSWAT)	2001	Tampa, FL	SafeConnect SDP
InstaSafe	2012	Bangalore, India	Secure Access
Meta Networks	2016	Sunnyvale, CA	Network as a Service Platform
Okta	2009	San Francisco, CA	Okta Identity Cloud
Pulse Secure	2014	San Jose, CA	Pulse Zero Trust Access (PZTA)
Perimeter81	2018	Tel Aviv, Israel	Software Defined Perimeter
Safe-T	2013	Herzliya, Israel	Secure Application Access
SAIFE	2014	Chandler, AZ	SAIFE Connect, SAIFE Continuum
Symantec	1982	Mountain View, CA	Luminate Secure Access Cloud
Unisys	1986	Pennsylvania	Stealth
Verizon	1983	Basking Ridge, NJ	Vidder Precision Access
Waverley Labs	2012	Waterford, Virginia	Panther SDP
Zentera Systems	2012	San Jose, CA	Cloud-over-IP (CoIP) Platform
Zscaler	2008	San Jose, CA	Private Access

Vendor Profile – Pulse Secure

URL: https://www.pulsesecure.net/

Pulse Secure, having spun out of Juniper Networks in 2014, is a leading provider of zero trust-based secure access solutions designed for hybrid IT that yield comprehensive visibility, protected connectivity, compliance and threat response. Pulse Secure product line consists of Pulse Zero Trust Access (PZTA), Pulse Secure Connect VPN, Pulse Policy Secure NAC, Pulse virtual Application Delivery Control (vADC), Pulse Workspace (mobile security), and the Pulse One manager.

Pulse Access Suite Plus provides modular, integrated remote, mobile, cloud and network access packages that support such Zero Trust capabilities as continuous identity and device authentication, endpoint compliance and conditional access enforcement. Pulse Zero Trust Access (PZTA) extends the vendors' secure access portfolio with SaaS offering established on the company's cloud-native, microservices-based, multi-tenant platform hosted globally in Microsoft Azure cloud (replaces its former Pulse SDP solution).

Pulse Zero Trust Access service enables easy, trusted access directly between a user's device and the application residing in multi-cloud and data center environments. PZTA follows client-initiated SDP architecture framework from Cloud Security Alliance, and delivers end-to-end visibility and analytics, automated provisioning, user, endpoint and posture verification, granular policy management, and advanced threat mitigation.

Pulse Zero Trust Access consists of PZTA Controller that is hosted and managed by Pulse, virtual Pulse ZTA Gateway that customers deploy on-premises or in the cloud, and unified Pulse Client which ensures native user experience for popular OS, such as Windows, macOS, Linux, Android and iOS. Customers can deploy as many Gateways as needed closest to their on-premises or cloud applications, all centrally managed by the Controller.

Once securely enrolled with the Controller, the Client sends authenticated identity, device and posture attributes through the control plane to the Controller, which then determines authorization for each available requested application session. Upon granting access, the Controller establishes the data plane – the trusted, encrypted channel directly between the Client and the Gateway. Neither identity nor application data is not shared with the Controller to ensure data sovereignty. Each session is continuously monitored to determine if any state change affects the access policy – ensuring conditional access. PZTA applies its built-in, geographic proximity algorithms technology to ensure optimal Gateway connectivity and Controller utilization.

PZTA separates control and data planes to provides access responsiveness, nominal latency and scalability, and rendering of the Controller and Gateway invisible to only authorized entities (Dark Cloud). PZTA has extensive built-in and third-party multi-factor authentication (MFA) integrations and single sign-on (SSO) including Security Assertion Markup Language (SAML) as an Idp or SP. These defenses reduce the attack surface, prevents unauthorized access, and thwarts cyber threats like malware, identity theft, man in the middle, APTs and other attacks.

PZTA provides an extensive, interactive administrative dashboard offering rich analytics across user, device, gateway, applications and PZTA system components. This allows administrators to quickly address issues, examine all access and drill-down for more detail. PZTA allows for granular, contextual and identity-centric policies. The system also has built-in user and entity behavioral analytics (UEBA) that utilizes machine learning and risk-scoring algorithms to identify malicious, non-compliant and suspicious activity in order to facilitate threat mitigation.

Pulse ZTA takes advantage of its unified Pulse Client for popular operating systems. This Client is the same for Pulse Secure's VPN and NAC solutions, and supports policy-based, simultaneous tunneling and multi-tunneling so that users don't need to know what mode of access is being applied regardless of their location or where the application resides: on-premises, in a public cloud, private cloud or SaaS environment. The Client is configured by the administrator as always-on or invoked per application. The end user's interface is hidden until the user wants to see, via app or web portal, their available applications or conditions limiting access.

Pulse Zero Trust Access offers simple per named user subscription licensing with full gold-level technical support. Platinum support is an optional add-on. Customers do not need to determine how many Gateways and applications to account for. PZTA is available as a standalone service and, using the same Client, can co-exist with the Pulse Access Suite Plus. As such, PZTA is designed for enterprises with cloud-only environments, those operating multi-cloud and hybrid IT infrastructure, and current customers who can leverage their existing deployed Pulse Secure investment.

Analyst Perspective

Following is the analysis of the Pulse Secure capabilities in the Software Defined Perimeter (SDP) market:

- Pulse Secure is amongst the leading providers of secure access solutions with a comprehensive, modular and integrated portfolio widely deployed across an enterprise, mid-market and SMB organizations alike. The company has made significant investments to extend ease of use, visibility, deployment flexibility, scalability, interoperability and automation capabilities within its Pulse Access Suite. While many organizations use the company's standalone solutions, Pulse Access Suites continue to be the choice for mid-sized to large enterprise organizations across industries. Pulse Zero Trust Access (PZTA) SaaS further extends its secure access capabilities in accordance with Zero Trust principles.

- PZTA offers cloud-hosted, microservices-based and multi-tenant service platform that is a level ahead and replaces the vendor's previous SDP solution. Pulse ZTA delivers more simplified and scalable multi-cloud and hybrid IT access and management. As a client-initiated SDP solution, it offers deployment flexibility that supports customers and service providers seeking a SaaS solution with the Controller hosted by Pulse Secure in Azure cloud, and those that want to run the Controller in-house to make use of their own cloud and network infrastructure.

- PZTA has comparatively broader application support, including HTTP/S, TCP/UDP, RDP, SSH, Telnet, and SIP. Extensive application support, access and operational analytics, identity and device authentication, hybrid IT configuration, adaptive access control, UEBA, and threat mitigation functionality are among the key differentiators for the platform.

- Pulse ZTA can seamlessly coexist with Pulse Secure access portfolio, enabling organizations to gain more cohesive secure access control – SDP, VPN or NAC – and streamlined user experience for their remote, mobile and on-premise workforce. With its comparatively simpler named-user subscription licensing, PZTA SaaS is expected to become lucrative and preferred among organizations with cloud-only infrastructure or those migrating resources to the cloud. Clientless access is also planned.

- PZTA platform represents a significant move into cloud-delivered security for Pulse Secure. The company plans to bring its other solutions onto the platform, as well as use its integration framework (applies public protocols and APIs) to allow enterprises and MSSPs flexibility to pursue best-of-breed approaches; integrating Pulse Secure with other cloud security services (e.g. SD-WAN, CASB, EDR, SIEM).

- As per the research findings, Pulse Access Suite Plus and PZTA supports, comparatively, a broader and more diverse range of use cases and operational flexibility. As a result, Pulse Secure is distinguished among zero trust, secure access solution vendors, especially for enterprises and service providers operating hybrid IT and multi-cloud environments.

Market Recommendations

Despite the year-over-year increase in cybersecurity-related spending, security breaches and their impact on the global economy continue to outpace the investment. Conventional perimeter-based security solutions, that organizations continue to invest, are failing to protect them. The perimeter security defenses organizations depend on were designed for the networks of the 1990s, and those networks no longer exist. Simply put, legacy perimeter security defenses are being challenged — they may not fully address virtual and cloud dynamics, mobile workforce needs, and today's more sophisticated attacks. As organizations are increasingly progressing digital business strategies with a focus on providing an enhanced customer experience, supporting mobility and remote operations, and accelerating multi-cloud application and infrastructure initiatives, implementation of a robust access security strategy is essential.

Software Defined Perimeter technology is emerging as an advanced network security solution for today's complex, interconnected world. A Software Defined Perimeter isolates network services from the internet, allowing access only after successful authentication, and restricting connections to only pre-authorized services. Network assets are hidden from unauthenticated users, leaving attackers with no visible target. Software Defined Perimeter protects organizations by substantially reducing the attack surface. Followings are the key recommendations for the successful adoption of SDP solution for the zero trust network security:

Evaluate Functional Value Proposition of SDP Solutions: The various parameters of the technology excellence and product functionalities are amongst the most important consideration when evaluating and selecting an SDP solution and vendor to implement zero trust network security strategies. Organizations are advised to conduct a comprehensive evaluation of different SDP solutions and vendors before making purchasing decisions. Organizations should employ a weighted analysis of the several factors important to their specific organization, use cases, and industry-specific requirements. Requirements of key SDP solution features by an SMB user may be different from that of the enterprise user segment. Organizations should consider a well-established vendor with existing solutions for secure access along with emerging vendors with innovative technology approach. A robust SDP solution should support direct-to-app connectivity to ensure optimal application performance, extensive user, device and endpoint posture authentication & authorization, strong connectivity protection, granular policy management, scalability and interoperability.

Analyze Potential Risk: SDP solutions are placed early in the product lifecycle stage and thereby not considered a fool-proof, proven solution to address all types of enterprise requirements or defend against all types of sophisticated cyberattacks. Organizations should carefully analyze the potential risk of implementing SDP solutions for zero trust network security. Some of the possible risks associated with SDP may include the performance of the SDP controller, privileged credential abuse or bypassing of PAM controls, the ongoing market consolidation of emerging SDP vendors, and such others.

Application Support: SDP solutions should support a variety of applications including web, remote desktop protocol, HTML5, peer-to-peer, legacy data center and custom TCP/IP, SSH protocol, native VDI, VOIP, SIP and others.

Interoperability: Users should look for SDP vendors that offer extensibility and support integration with existing security policies and tools. The vendor should provide, if not at least support, integration with popular user and entity behavior analytics (UEBA), single sign-on (SSO), multi-factor authentication (MFA), endpoint protection and management tools, existing IAM and PKI infrastructure, and such others.

SDP, NGFW and VPN: Organizations looking at extending access control of users and devices are increasingly assessing their conventional NGFW and VPN solutions against SDP solutions. In many use cases, replacements of traditional NGFW and VPN solutions are possible and provide advantages to progress zero trust strategies.

NGFW is the incumbent perimeter defense that provides a necessary air gap between the Internet and intranet. As enterprises activate and scale various optional features of their NGFW including secure remote and cloud access, it will require increased NGFW capacity and introduce potential management complexities. While not comparable with best-of-breed standalone solutions, organizations should consider their requirements against added features, costs and deployment considerations.

As mentioned earlier, modern SSL-VPN operate at the application layer to provide secure remote access that align to Zero Trust principles. They offer continuous entity authentication with MFA, centralized administration, and enforcing granular, contextual access polity to specific applications and resources. It can operate in client or browser-based modes to support secure multi-cloud and data center application access with SSO. They also have enhanced usability with minimal user interaction, such as always-active tunneling.

Organizations should evaluate their specific use cases, applications, infrastructure and investment that can support SDP projects - where there are security, operational and economic advantages over VPN. Mid-tier and larger enterprises with hybrid IT infrastructures, legacy applications, and compliance requirements may need to determine the deployment and management of both SDP with VPN technologies, as well as integrated SDP and SSL-VPN offerings. Over the near-term, the majority of SDP deployments will co-exist with VPN to provide end to end access security.