On the Radar: Pulse Secure delivers zero-trust secure access service

Publication Date: 08 Sep 2020 | Product code: INT005-000158

Rik Turner

Summary

Catalyst

Pulse Secure is an information security vendor with a focus on secure remote access for people, devices, things, and services. The Pulse Secure Access Suite is its flagship offering in this area and is targeted at global enterprises with a hybrid mix of multi-cloud and data center environments.

Pulse Secure Access Suite delivers protected connectivity, operational intelligence, and threat response across mobile, network, and multi-cloud environments, where it focuses on providing ease of use for administrators and transparency for end users. With the launch of Pulse Zero Trust Access (PZTA), the company adds software-defined perimeter (SDP) functionality delivered as a service and hybrid IT deployment flexibility, targeted at organizations with cloud-only infrastructure, those migrating applications to the cloud, and managed service providers (MSPs) that can operate PZTA in their or their customer's cloud.

Omdia view

The market for remote access technology was huge even before the COVID-19 pandemic massively increased demand. As an established player in the SSL VPN market, Pulse Secure can help its more than 24,000 enterprise customers and MSP partners with additional options, particularly those with multi-cloud applications, to adopt a zero-trust approach to granting access to them. Moreover, PZTA is a service platform, and paving the way for a broader secure access service edge (SASE) play is part of the company's longer-term strategy.

Why put Pulse ZTA on your radar?

Pulse Secure has been in the secure access business for nearly two decades, with extensive experience and a huge customer base in SSL VPN, as well as in mobile security and contiguous markets such as network access control (NAC) and application delivery controller (ADC). It brings these capabilities to bear in the emerging new paradigm of zero-trust access (ZTA), enabling existing customers to diversify beyond VPNs as needed and in as gradual a fashion as they require, while addressing the needs of new customers with an infrastructure that can be entirely in the cloud or as hybrid as needed. By adding the PZTA service offering to its portfolio, Pulse Secure provides organizations with the ability to consolidate disparate secure access tools to gain efficiencies and security efficacy.

Market context

With applications moving into the cloud and employees needing to work from anywhere (the latter, a trend clearly heightened by the COVID-19 pandemic), there is renewed interest in secure access technology. While SSL VPNs are a large and well-established market, and one that continues to grow, not least in the current crisis, new ways to deliver remote access to enterprise users have arisen over the last few years. They offer both a perimeter-less architecture that does not rely on users connecting to an SSL VPN concentrator in the corporate data center, and a more granular security

posture, adhering to the zero-trust model that is gaining currency in cybersecurity. For this reason, Omdia groups these new approaches under the zero-trust access (ZTA) banner.

Zero trust is a stance on cyber that is often summarized as "never trust, always verify," i.e., assume that nobody and nothing (e.g., users, devices, applications, or networks) is trustworthy, such that even after they are authenticated and authorized, and access has been granted, it should

- be exclusively to the application(s) the user/system requires to perform a specific task, rather than broad access to corporate resources
- be able to apply adaptive access control by continuously monitoring for any deviations from user/device security posture or normal behavior, indicating non-compliance, potential account compromise, or insider threat

ZTA is the application of zero-trust principles specifically to secure access. Omdia has written extensively about this emerging field, focusing on two ZTA approaches in some depth, namely software-defined perimeter (SDP) and identity-aware proxy (IAP). We group both under the umbrella heading of ZTA.

Without going into a huge amount of technical detail, the basic architectural difference is that, while SDP works via a controller, which sits in the control plane between user and application, and a gateway sitting in the data plane between the two, IAP performs the control function and establishes the connection via a proxy sitting in both the control and data planes. As an additional "bump in the wire" between user and application, therefore, there is the potential for the IAP to introduce latency in the communication, particularly for applications sitting on a customer's premises. For this reason, IAP providers always operate the actual network over which the connection is made, enabling them to perform traffic shaping and other optimization activities.

SDP, by contrast, introduces no additional latency and is usually sold as software that a customer or service provider deploys on whatever network they choose, and as a result, it can be a licensed software sale, whereas IAP is always a service and, as such, requires the customer's traffic to traverse the IAP provider's cloud or content network.

Pulse ZTA (PZTA) is unusual in that it applies the SDP architecture of separate control and data planes, yet is offered as a service where the PZTA Controller is managed by Pulse in the cloud, with the clients and gateways deployed by the customer. The PZTA service is charged on a per-user, per-year basis. Omdia has stated in previous reports that it expects to see cloud-delivered services enjoy greater market success than customer-managed software deployments, given both the simplicity of adoption for a cloud-based service and the growing acceptance of the "as-a-service" delivery model for technology generally, and security technology in particular. The latter trend underpins the emergence of multiple SASE offerings in the market this year, all of them with ZTA as one of their core components.

Product/service overview

Pulse Secure delivers PZTA in accordance with the SDP architecture as specified by a dedicated working group within the Cloud Security Alliance (CSA). This entails client software on the end user's devices (typically a laptop or mobile computer) requesting access to a controller (i.e., the control

plane) and, if successful, gaining access via encrypted tunnels through a gateway (i.e., the data plane).

It provides this as a service, with the controller currently running over Microsoft's Azure cloud infrastructure, though it plans to expand to other cloud service providers over time. The customers themselves deploy gateways wherever their applications reside (i.e., in any cloud or data center). The service is licensed by named users and not by the number of applications or gateways, which should simplify customer purchasing, deployment, and the expansion of its use within the account.

All user and application data is encrypted within the data plane for purposes of data sovereignty. Importantly, the service requires no changes to the resources being accessed, whether they be on the customer's premises or in the cloud. The PZTA Controller leverages built-in optimal gateway selection (OGS) that ensures user experience and data compliance.

One client for VPN and ZTA

The client software for PZTA is the same client that delivers the vendor's traditional VPN and NAC capabilities, without the need for a software upgrade to get ZTA functionality. This enables the company to offer those customers a diversification of their remote access options at the speed that suits them, while at the same time targeting potential new customers outside its VPN installed base.

PZTA not only provides connectivity once the user has been authenticated and authorized, but also monitors their activity during the session and gives the customer a continually updated risk score for each individual user (in keeping with the "always verify" mantra of zero trust), based on its built-in behavioral analysis capability. The rationale here is one of adaptive assessment, with the continuous monitoring enabling customers to detect anomalous behaviors, indicating that credentials may have been stolen, for instance, and to mount a timely response. As for authentication methods, the system supports built-in and third-party multi-factor authentication (MFA) integrations, as well as single sign-on (SSO) via standards-based approaches such as the Security Assertion Markup Language (SAML).

PZTA can work with a range of applications, including HTTP and TCP/UDP-based ones, and a variety of connectivity types, including layer-3 and layer-4 segmented access.

The service is licensed by named users and not by the number of applications or gateways, which should simplify customer purchasing, deployment, and the expansion of its use within the account.

Company information

Background

Pulse Secure was created from a technology spin-off from Juniper Networks in 2014. The company came into existence as an established player in remote access technology, a market in which it had been active since 2004, giving a large customer base and a solid opening position on which to build. It currently has some 24,000 enterprise and service provider customers using tools, suites, and now a cloud-delivered service across a portfolio that includes VPN, SDP, NAC, virtual application delivery controller (vADC), and mobile device management (MDM) technology.

Privately owned by Siris Capital, Pulse Secure is headquartered in San Jose, CA, with offices in Europe and Asia. The company is led by security industry veteran and CEO Sudhakar Ramakrishna. Ramakrishna was previously SVP and general manager for the Enterprise and Service Provider Division at Citrix, and before that, held management positions at Polycom, Motorola, 3Com, and US Robotics.

Since the company emerged as a standalone venture, Siris Capital has sought to strengthen Pulse Secure with the acquisition of complementary technologies such as MobileSpaces (MDM for BYOD/non-managed devices) in 2014, and the vADC business from Brocade Communications in July 2017.

Current position

With an installed base of over 24,000 enterprise customers and 21 million users for its secure access technology, Pulse Secure has clearly had to factor in the coexistence of VPN and ZTA within those accounts, making PZTA an upsell opportunity rather than a “rip-and-replace” choice.

The vendor offers its portfolio as the Pulse Secure Access Suite, comprising the following:

- SSL VPN with endpoint compliance and cloud access (Pulse Connect Secure)
- Mobile device management with VPN and container (Pulse Workspace)
- Virtual Application Delivery Controller with cloud-based load balancing, optimal gateway selection, and web application firewall (Pulse vADC)
- Network Profiler and NAC (Pulse Policy Secure)
- A central management platform with a user and entity behavioral analysis (UEBA) capability (Pulse One)

The company offers three integrated product bundles under the Pulse Access Suite Plus moniker, Essentials Plus, Advanced Plus, and Enterprise Plus, with each suite combining various components. Annual subscription pricing for the Essentials Plus Suite starts at around $80 per concurrent user, with volume and multiyear discounting available. PZTA is sold separately and can coexist with the individual products and suites. PZTA annual subscription starts at $15 per named user per month, also with volume and multiyear discounting available.

Future plans

Pulse Secure has plans to expand the PZTA offering, offering a virtual PZTA Controller that customers will be able to deploy on their own cloud or on their premises and enabling NAC management through the PZTA Controller.

Key facts

Table 1: Data sheet: Pulse Secure

Product/Service name	Pulse Zero Trust Access (PZTA)	**Product classification**	Secure remote access technology based on an SDP architecture
Version number	20.7	**Release date**	July 2020
Industries covered	All	**Geographies covered**	All
Relevant company sizes	Enterprise and midsize	**Licensing options**	Annual subscription based on number of named users
URL	https://www.pulsesecure.net/	**Routes to market**	Direct and channel
Company headquarters	San Jose, California, US	**Number of employees**	650+

Source: Omdia

Analyst comment

Pulse Secure comes to ZTA with a large installed base in VPN, so upsell is clearly a major opportunity for this established vendor, as well as potential new accounts. However, the competitive landscape in ZTA is expanding apace, with dedicated players jostling with broader portfolio vendors, all of them hoping to attract the attention of enterprises faced with a sudden expansion of their remote access requirements on account of COVID-19.

Significantly, ZTA is also being rolled up into even more extensive offerings in the form of the SASE services now being launched by any number of security vendors great and small, with networking and security elements converging and being marketed as cloud-delivered services. Typical SASE components are

- An IP network, with points of presence (PoPs) around the globe
- SD-WAN networking or other tunneling capabilities for branch office connectivity
- Network security functions such as firewall, secure web gateway (SWG), cloud access security broker (CASB), content filtering, and so on
- ZTA for remote users, with the option for those in branch offices to also use it

SASE is clearly gaining a head of steam in the current market, and one of Pulse Secure's challenges will be to raise its profile against some of the heavyweights offering SASE and the deep pockets they bring to their marketing efforts. Omdia sees the potential for the secure remote access specialist to partner with vendors that have other parts of the SASE toolkit, such as firewall, secure access gateway, CASB, or SD-WAN providers, for a combined offering into this market segment.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Fundamentals of Zero-Trust Access, INT005-000090 (February 2020)

Author

Rik Turner, Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation Policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com