Ovum
TMT intelligence | informa

On the Radar: Pulse Secure delivers zero trust secure access

Manages connectivity protection, visibility, and threat response across mobile, network, and cloud

Publication Date: 15 Feb 2019 | Product code: INT003-000324

Andrew Kellett

Summary

Catalyst

Pulse Secure is an information security specialist. It focuses on zero trust secure access for people, devices, things, and services. Since being spun out of Juniper in 2014, the company has made considerable investments in its product lines, capabilities, and usability.

Pulse Secure Access Suite is the company's cornerstone product set. It provides IT access security for global enterprises across a wide range of industry verticals and a hybrid mix of operational platforms.

The value of the Pulse Secure Access Suite comes from its ability to deliver protected connectivity, operational intelligence, and threat response across mobile, network, and multicloud environments, where it focuses on providing ease of use for administrators and transparency for end users.

Key messages

- Pulse Secure helps enterprises deliver multicloud, 360-degree user and endpoint visibility, protected access to applications and information, granular security controls, and high availability for on-premises or cloud environments including public, private, and software-as-a-service (SaaS).
- Dual-mode secure access facilities offer integrated perimeter-based VPN and software-defined perimeter (SDP) architectures. Ecosystem integration provides flexible access provisioning, security posture protection, and low total cost of ownership.
- Secure access orchestration and reduced complexity is achieved using a centralized management system, a unified appliance platform, broad endpoint client coverage, standards-based infrastructure, and cloud interoperability facilities.
- Organizations with a piecemeal approach to secure access can incur complications and limitations from multiple access security systems, including visibility, usability, policy, enforcement, and coverage gaps. An integrated approach, such as Pulse Secure, can help overcome these obstacles.
- Integrated suites for SMEs, large enterprises, and service providers address secure mobility, endpoint visibility and compliance, single sign-on (SSO) and multicloud access protection, automated workload balancing, and Internet of Things (IoT) security.
- Technology investments and development efforts have propelled Pulse Secure beyond its remote access SSL VPN origins to offer an enterprise-grade secure access platform for hybrid IT.

Ovum view

Since 2014, Pulse Secure has moved far beyond its remote access origins, and it now offers a comprehensive and flexible enterprise secure access proposition. The company has enhanced and expanded its product line to support an extensive range of endpoint, mobile, network, cloud, and IoT environments and their respective access control ecosystems. With its latest platform release

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

(October 2018) and SDP-enabled Pulse Secure Access Suite, the company can support enterprises looking for a one-stop approach to secure access.

Recommendations for enterprises

Why put Pulse Secure Access Suite on your radar?

Pulse Secure Access Suite enables enterprise clients to benefit from zero trust secure access. It offers users simple and safe access to company resources, as well as providing administrators with the visibility, flexible control, and threat response facilities they need. IT security managers can centrally manage access controls alongside user and device policy compliance for applications, data, and services that are delivered on-premises or in the cloud. Delivery supports both perimeter-based VPN and SDP architectures.

Other important drivers for Pulse Secure Access Suite adoption include

- digital transformation issues that are pushing IT to support an ever-expanding variety of devices, applications, and data protection requirements, as well as the growing use of flexible work practices that help organizations boost employee productivity
- mobile workforce demand combined with the consumerization of IT that introduces mobile access challenges and data privacy risks
- the need to optimize IT application delivery extending existing data center resources and applications to private and public cloud and SaaS, which introduces visibility, access control, and segmentation challenges
- the adoption of the zero trust mode to extend user and device authentication prior to granting access, including interest in SDP for direct entity to web application access
- evolving malware, IoT security, and data privacy risks that are further complicated by endpoint compliance deficiencies
- the amalgamation of secure access technologies (e.g., firewall, UTM, secure gateways, VPN, SDP, CASB, ADC, and MDM) that can improve security operations and user productivity.

Pulse Secure Access Suite provides a unified, open, flexible, and scalable solution to address these issues.

Highlights

Pulse Secure Access Suite supports the protected-access requirements of small, midsize, and large enterprise organizations. It is an inclusive and integrated platform that provides zero trust, policy-based secure access services to any corporate resource/application or third-party services from authorized users, devices, and systems.

Some enterprises are currently piloting or selectively implementing SDP for their cloud-based apps and environments as a complement to conventional perimeter-based controls. This will not negate SSL VPN use but, on the contrary, often requires managing two systems. By offering both VPN and SSL in one platform, organizations gain greater operational, security, and cost efficiencies.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Sold separately or as a bundle, the Pulse Secure Access Suite provides next-generation SSL VPN and SDP facilities for protected remote, on-premises, mobile, and cloud security; authentication and SSO; endpoint visibility and compliance; network profiling and network access control (NAC); and virtual application delivery controller (vADC) technologies.

The product-level building blocks of the platform include Pulse Connect Secure, Pulse SDP, Pulse Workspace, Pulse Profiler, Pulse Policy Secure, and a virtual application delivery controller, Pulse Secure vADC. Pulse SDP is only available as part of the company's Secure Access Advanced and Enterprise edition suites. These components are complemented by the Pulse unified client, the Pulse unified appliance, and Pulse One Manager for single-pane-of-glass visibility, policy, and appliance administration. The products are also available through cloud service providers, including Microsoft, Google, Amazon, and Rackspace, as well as some regional managed service providers.

The complete product portfolio is described in detail in Table 1.

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Table 1: Pulse Secure Access Suite

Product portfolio	Description
Pulse Secure Access Suite An integrated set of products that are value-packaged for SME to large enterprise, enabling the selection and deployment of Essential, Advanced, or Enterprise editions.	Essential edition offers SSL VPN, native mobile VPN and mobile device management (MDM) container, centralized administration, and cloud visibility. Advanced edition adds network profiling, SSO, and cloud-based administration, and Enterprise edition adds NAC enforcement. Advanced and Enterprise editions offer optional SDP access security facilities.
Pulse Connect Secure A feature-rich SSL VPN and SDP gateway solution that provides safe user connectivity, regardless of the device being used, to any corporate resource, including cloud applications and corporate data centers.	Facilities include strong authentication, host checking, granular policies, virtual desktop and browser access, and MDM integration. Pulse Client (agent and agentless) supports VPN and SDP facilities for user and device authentication and security state verification. Supports always-on, on-demand, and application-activated VPN tunneling and SDP gateway facilities with multifactor and certificate authentication, SSO, and SAML features. Cloud security facilities enable seamless and compliant access to SaaS applications such as Office365 and Salesforce.com.
Pulse Workspace Offers a mobile application and device management capability for business and private use, enabling enterprises and their users to benefit from securely delivered corporate and third-party apps and data to personal devices.	Mobile VPN facilities can work with existing MDM solutions. Mobile container facilities secure apps and data on each device to separate personal and professional environments, balancing user experience, security, and personal device privacy. The technology is deployed with low IT administrative overheads and supports GDPR levels of data and privacy protection.
Pulse Policy Secure Is NAC 3.0 technology insofar as it provides visibility, policy-based controls, and phased enforcement for user and device access. It delivers the "who, what, when, where, and how" controls needed when users and devices connect to a company's network.	NAC features include agent and agentless endpoint visibility, guest management, BYOD onboarding, granular compliance policies, logging and reporting, and migration capabilities (e.g., 802.1X port-level and L2-L4 enforcement). Vendor-agnostic facilities provide interoperability with popular network and wireless switches, next-generation firewalls (NGFWs), security information and event management (SIEM) systems, and enterprise mobility management (EMM) tools. Predefined and custom-built policies are supported using a variety of facilities that include host checking for endpoint tracking, anomaly detection, automated and user-directed remediation, network quarantine and blocking, IoT device classification, and security.
Pulse Profiler A network profiling product that supports endpoint discovery, classification, and device monitoring for devices connected to enterprise networks. It can be purchased as a standalone product or as part of Pulse Policy Secure (NAC).	Pulse Profiler offers comprehensive user, endpoint, and IoT visibility; inventory; and behavior monitoring, as well as the compliance reporting needed to make informed, policy-based decisions about issues and threats. It makes use of built-in RADIUS server facilities and can be implemented across distributed networks. To incorporate remote user and device visibility requires the use of optional Collector technology, which is embedded in Pulse Connect Secure (VPN).

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

Pulse Secure vADC Designed to make applications run faster, more reliably, and more securely. It is positioned as a complete software-defined ADC that can be deployed at scale to free up applications from the constraints of hardware-based load balancers.	Pulse Secure vADC delivers high performance and availability for application delivery within the data center and multicloud environments including Amazon AWS, Microsoft Azure, and Google Cloud. Proprietary Optimal Gateway Selector technology with the Pulse Virtual Traffic Manager (VTM) allows real-time, high-performance routing to the geographically nearest gateway. Facilities include the Pulse VTM, Pulse Services Director, and built-in web application firewall. Application load intelligence and resource usage analytics are available to expedite service optimization and troubleshooting.
Pulse One Manager Enables IT administrators to utilize a single, centralized console for the management of multiple Pulse Secure products across operating environments. It offers end-to-end user and device visibility for controlling enterprise access to data center and cloud-based systems.	Pulse One Manager ties together the administrative components needed to deploy and maintain Pulse Secure systems, manage multilevel policies, and gain unified intelligence and orchestration. In SDP mode, it acts as the SDP Controller to initiate host user and device authentication and security state verification, to manage role and resource access policies and stateful access requests, and to authorize protected access between SDP-enabled clients and SDP-enabled gateways. It can be deployed as an on-premises appliance, a virtual appliance, or SaaS.

Source:

Background

Pulse Secure was created from a technology spin-off from Juniper Networks in 2014. The secure access technology involved had a rich legacy of innovation dating back to 2004, giving the new company a strong opening position on which to build. Pulse Secure, privately owned by Siris Capital, 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 senior vice president and general manager for the Enterprise and Service Provider Division at Citrix. Before that, he held management positions at Polycom, Motorola, 3Com, and US Robotics.

Since the company's formation in 2014, Siris Capital has continued to invest in strengthening Pulse Secure with the acquisition of complementary technologies such as MobileSpaces in 2014 and the vADC business from Brocade Communications in July 2017.

Current position

Pulse Secure is a strong, global organization with around 750 employees across support, sales, and R&D, and over 3,000 partners. It secures more than 18 million endpoints and has over 20,000 customers across most industry verticals, including 80% of the Fortune 500. The company has a proven track record of providing robust support for its products and services, having successfully sold a mix of integrated security products and suites to small and midsize enterprises as well as large, global organizations.

Today, businesses are in the midst of often difficult-to-deliver digital transformation challenges. To achieve these objectives, they require worker flexibility and greater accessibility to information. At the same time, IT and security teams must deliver safe access that addresses the conflicting demands of workforce mobility, IT consumerization, cloud migration, and privacy compliance. It is these

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

fundamental business and operational requirements that have made enterprise secure access products, such as Pulse Secure Access Suite, more relevant.

Pulse Secure will continue to build on its remote, cloud, and network access control heritage. It has already strengthened its portfolio of products and services through innovation and acquisition and is continuing to extend its relevance to the business and user protection requirements of its wide-ranging install base. The introduction of dual-mode VPN and SDP architectures within the same Pulse Secure platform strengthens operational and economic advantages to current and prospective customers.

Pulse Secure is upbeat about the future business relevance of its security products and services. Annual revenue figures are growing at double-digit rates. Demand for its technology is increasing as the business mix of on-premises and hybrid cloud adoption continues across all sectors, and as advanced malware and IoT threats continue to grow. Equally, Pulse Secure also sees further levels of interest as organizations adopt new flexible work styles alongside the need for more stringent data privacy and protection mandates.

Data sheet

Key facts

Table 2: Data sheet: Pulse Secure

Product name	Pulse Secure Access Suite, Pulse Connect Secure, Pulse SDP, Pulse Workspace, Pulse Policy Secure, Pulse Profiler, Pulse vADC, Pulse One Manager	**Product classification**	Enterprise secure access
Version number	9.0 rev.3	**Release date**	October 2018
Industries covered	All	**Geographies covered**	All
Relevant company sizes	Small, midsize, and large	**Licensing options**	Perpetual, subscription, named user, and concurrent user
URL	www.pulsesecure.net	**Routes to market**	Channel distribution
Company headquarters	San Jose, California, US	**Number of employees**	750

Source: Ovum

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. Although On the Radar vendors may not be ready for prime time,

© Ovum. All rights reserved. Unauthorized reproduction prohibited.

they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

2019 Trends to Watch: Cybersecurity, INT003-000295 (October 2018)

Ovum Decision Matrix: Selecting an Endpoint Protection Solution, 2017-18, INT003-000019 (December 2017)

Author

Andrew Kellett, Ovum Associate

Maxine Holt, Research Director, IT Infrastructure

maxine.holt@ovum.com

Ovum Consulting

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

Copyright notice and disclaimer

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

Ovum
TMT intelligence | informa

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Boston
Chicago
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
Paris
San Francisco
Sao Paulo
Shanghai
Singapore
Sydney
Tokyo