Publication date:
12 Nov 2020
Author:
Rik Turner
Principal Analyst

On the Radar: PortSys offers a zero-trust access platform

Brought to you by Informa Tech

Table of Contents:

Summary

Catalyst

PortSys has developed zero-trust access (ZTA) technology, a term applied to products that have emerged in recent years as a more efficient and secure alternative to virtual private networks (VPNs), for remote access to applications. Its product consolidates access to local and cloud-based resources including web applications, legacy applications, software as a service (SaaS), infrastructure as a service (IaaS), SSH, and other forms of access into a single solution.

Omdia view

VPN technology and other remote access technologies such as the Remote Desktop Protocol (RDP) were creaking under the strain of cloud computing even before the coronavirus pandemic, which suddenly threw into sharp relief the need for more efficient remote access technology. ZTA addresses this need and PortSys is positioned to gain market share with its Total Access Control (TAC) product.

Why put PortSys TAC on your radar?

TAC offers simple deployment and supports a peaceful coexistence with and gradual switchover from VPNs. TAC is agentless, so it can support even non-corporate devices, and addresses access requirements to on-premises applications, as well as to those in IaaS, PaaS, and SaaS environments. Furthermore, PortSys does not charge extra for 24x7 support or disaster recovery, making it a serious contender for any remote (or local) access technology refresh a company is considering.

Market context

Zero trust is an approach to how security is implemented, along the lines of “trust no-one and nothing, (no systems), limit access as far as possible, and continuously verify”. The term is applied to a range of security platforms, including remote access, privileged access management (where “least privilege” is effectively a zero-trust approach), and cloud permissions management (CPM).

For remote access, some analyst firms refer to zero trust network access, but Omdia agrees with PortSys that the access requirement relates primarily to applications regardless of where they reside and the networks that must be traversed to get to them. Like PortSys, Omdia therefore uses the ZTA acronym.

VPN technology evolved to provide remote access for users who needed to get to applications residing in their company's corporate data center. To do this, software clients on their laptops connected to concentrators in the data center, with an encrypted tunnel set up between the two. The user could then access the application in the back end. However, as enterprise applications migrate to the cloud, the shortcomings of VPNs are becoming increasingly apparent.

First, they are inefficient because they require traffic between the end user's device and the app to "trombone" through the corporate data center, which can add latency and degrade the user experience.

Second, from a security perspective, VPNs are overly permissive. They grant blanket access to an entire corporate network rather than a specific application, so if an attacker can get in by using one, they can plant code to spy for privileged credentials, steal them, and then install ransomware or access the corporate "crown jewels."

Over the last few years, new approaches have come to market to address this, delivering remote access to applications without the need for a concentrator and restricting access specifically to one application, or at most a specific group of applications per session. Omdia groups these approaches under the collective title of ZTA, a category into which the PortSys technology fits.

The two flavors of ZTA: SDP and IAP

ZTA vendors fall broadly into two categories. First are those that offer software defined perimeter (SDP) technology as specified by the Cloud Security Alliance (CSA). This approach deploys an SDP controller (usually although not necessarily in the cloud) and often deploys software agents on end users' devices. An agent asks the controller for access to an application or set of applications, and if the request is granted, the controller instructs an SDP Gateway, which ideally resides directly in front of the application (in a data center or a cloud environment) to set up two encrypted tunnels, one between the user and the gateway, the other between the gateway and the app. Crucially, the controller sits in the control plane but not in the data plane, while the gateway operates in pass-through mode on the data plane, therefore adding no latency.

The other group offer identity-aware proxy (IAP) technology, where a proxy sits in both the control and data plane. Given that such a "bump-in-the-wire" approach has the potential to add latency, IAP is always offered as a service, with the provider also operating the network, to mitigate any latency with traffic shaping.

Product/service overview

The zero-trust technique called micro-segmentation is a cornerstone for what TAC does, which is to enable organizations to put customized security policies in place for access to each resource (local or in the cloud) to more effectively control access to each of these resources. It reduces the ability for lateral movement within an organization's infrastructure to other applications, whether local or in the cloud, if someone gains access with compromised credentials and applies for access requests originating from both inside and outside the organization.

Users access an application via TAC by going to a URL provided by their company, where they input their credentials, and multi-factor authentication (MFA) is also an option here. The system factors in device information such as the OS patch level, whether it has antivirus running, and geolocation when deciding whether to grant access. The appliance that houses the “brains” of the system also comes with a database of IP addresses to further inform the decision.

Once authenticated, the user is directed to the specific resource. They can also be sent to a portal with multiple applications/resources and single sign-on (SSO) if they regularly require access to a group of applications. The company can also set a timeout for access.

PortSys sees the ZTA market as characterized by three distinct approaches.

First are the **identity-focused** players, a category that includes the cloud access security broker (CASB) vendors now adding access control to their arsenal, along with companies coming from an MFA background. PortSys characterizes the general approach here as interjecting passwords in different places throughout the access process but feels it is limited in its scope.

Second are those adopting a **data-focused** approach (the objective is primarily to control access to the data itself), putting the likes of Broadcom’s Symantec business unit and Akamai in this class. PortSys sees this approach as difficult to implement because all a company’s data assets must first be identified and classified, and an entire new layer of infrastructure must be potentially inserted. This approach is also limited because is still possible for an attacker to do a lot of damage even if they have been blocked from accessing any data.

Third is the group PortSys itself is in, which it defines as the **access-focused** approach. It has the advantage of enabling a phased migration to zero trust, coexisting with legacy remote access technology, for instance, rather than requiring an overnight switch.

PortSys sees the SDP flavor of ZTA technology as a hybrid between the data- and access-focused approaches and believes it is potentially challenging to implement, depending on the complexity of the infrastructure. It believes its own technology is a less invasive version of SDP, although given TAC’s position in both the control and data planes between the end user and the application, Omdia would consider it an IAP approach.

Company information

Background

PortSys was founded in 2008 by CEO Michael Oldham, who had previously been a global program director at Network Engines, a development, manufacturing, and distribution partner for storage and security software and equipment providers that was subsequently acquired by Unicom.

The company’s initial business model was to work with HP and Microsoft on the development of security appliances, such as Microsoft’s Threat Management Gateway and Unified Access Gateway. However, when those vendors’ product strategies shifted elsewhere, PortSys refocused and developed what is today its flagship offering, the TAC platform, which was launched in 2015.

TAC was clearly a replacement for the UAG product, and PortSys migrated customers across to this platform in the succeeding years, offering 24x7 support as default in order to differentiate its offering.

PortSys remains completely privately held with no venture capital funding.

Current position

TAC's technology can be installed either with an endpoint agent or agentless, depending on an organization's specific requirements, and with a physical or virtual appliance, with the latter optionally cloud-based. TAC sits between the end users and the applications they seek to access, whether the apps are on a company's premises or in the cloud. Users request access on a portal, where their employer publishes all the applications and sets up the permissions for each individual and/or functional group of employees.

The employer sets up the requirements for accessing each application/resource in terms of who has access and the security requirements, such as GeoIP address, device type, security status of the device, and OS. These requirements must be met before a user is granted access to the resource. This allows for a dynamic and flexible portal that is "self-defining" based on the full context of the user at that time. The portal dynamically displays only the resources that user can access under their current circumstances. TAC's SSO then provides access to the resources. The end user does not have to know where the resource resides (locally or in the cloud).

PortSys charges for TAC on a per-user annual subscription basis, with no extra cost for disaster recovery and no limits on bandwidth, throughput, or number of connections. It does not have a managed service offering, and instead relies on MSP partners for this.

In terms of the market landscape for TAC, PortSys sees Okta, Pulse Secure, Citrix, and F5 in competitive situations, all of which are considerably larger vendors with deeper pockets to fund their marketing efforts. There are also many other heavyweights that have entered the market over the last couple of years, making it a highly competitive environment.

To position itself competitively against such players, PortSys bundles 24x7 support and does not charge extras for disaster recovery. It also believes that TAC's ease of implementation and ability to support a gradual migration from legacy technologies to the ZTA approach are significant differentiators.

Key facts

Table 1: Data sheet: PortSys

Product name	Total Access Control	**Product classification**	Access control, zero trust, cybersecurity
Version number	20.10.20.12	**Release date**	November 2020
Industries covered	All	**Geographies covered**	North America, Europe, Middle East, Africa
Relevant company sizes	All	**Licensing options**	Per-user license subscription
URL	https://portsys.com/	**Routes to market**	Direct and channel

Company headquarters	Marlborough, MA, US	**Number of employees**	n/a

Source: Omdia

Analyst comment

The ZTA market had already been developing for a few years prior to 2020 when the COVID-19 pandemic raised the profile of secure remote access technology beyond anyone's expectations. These technologies arose initially as a more efficient way to deliver access to applications in the cloud, but the sudden need to scale remote access to entire workforces instead of the 12–15% of remote workers that most companies were reporting pre-pandemic has put the emphasis on cost and scalability of ZTA for end users.

There is no shortage of ZTA vendors in the market. These range from large enterprises with broad portfolios, such as Akamai, Cloudflare, and Palo Alto Networks, all of which are in the IAP group, to smaller specialists such as Appgate and Safe-T, both of which offer SDP, and of course PortSys. In addition, most of the IAP vendors are now bundling their services into a still broader category, namely secure access service edge (SASE), which are services that straddle security and networking.

As a specialist vendor and a privately held company, PortSys's challenge is first and foremost to raise its profile in what is now a very busy market. Even before it can establish its technical credentials, it must register as a contender in the minds of potential customers.

In this context, it is at a disadvantage, particularly when compared with the industry heavyweights in the market that bring huge marketing budgets to the table when enterprises are hungry for information about how they can complement or even ultimately replace their VPN estate. PortSys notes, however, that it continues to do business with "significant customers who are absolutely loyal to TAC." And some organizations would consider its position as a smaller, potentially nimbler vendor as an advantage over more monolithic market leaders.

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 (ZTA) (February 2020)

Omdia Market Radar: Zero-Trust Access (May 2020)

"Security access service edge is not a new cybersecurity market segment" (June 2020)

Author

Rik Turner, Principal Analyst, Cybersecurity

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

Copyright © 2020 Omdia. All rights reserved. Reprinted with permission from Omdia. Content reproduced or redistributed with Omdia permission must display Omdia legal notices and attributions of authorship. The Omdia reports, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact. The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result. Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials. To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech 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