On the Radar: Axis Security takes a different approach to zero-trust access

Application Access Cloud is agentless and delivered as a service

Publication Date: 06 May 2020 | Product code: INT005-000119

Rik Turner

Summary

Catalyst

Axis Security has developed a cloud-based platform to deliver secure remote access, based on a Zero Trust approach, to so-called private apps, which include custom applications that a company has developed itself that it is running on its premises or in the cloud, such as legacy apps. The use cases it is targeting are B2B (partners, supply chain, and contractors, as well as M&A), but the technology also lends itself to B2E remote access scenarios, including VPN expansion/replacement scenarios.

Key messages

- Axis delivers secure remote access to private applications with a cloud-based platform delivered as a service, requiring no agents on end users' devices.
- Access is granted to a specific app rather than to an entire corporate infrastructure, putting Axis in the Zero Trust community.
- Axis currently supports on-premises applications and ones residing in infrastructure- and platform-as-a-service (IaaS and PaaS) cloud services.
- The company sees access to private apps as the most critical, differentiated, and most urgently required service, but also has plans to expand its support for software-as-a-service (SaaS) apps, which is currently limited.

Omdia view

The VPN market is huge, with estimates varying from $20bn to $35bn, depending on how it is defined. Because VPN technology is struggling to meet the need for access to cloud-based applications, there is an opportunity for vendors like Axis to take market share with secure and easy-to-use alternatives.

Recommendations for enterprises

Why put Axis Security on your radar?

Axis Security's agentless approach to remote access is compellingly straightforward because it does not involve deploying software to every end-user device. This also makes it easier to accommodate customer-owned devices. In addition, the agnostic approach to the underlying network leaves customers free to make minimal changes in order to start using App Access Cloud.

Highlights

The shortcomings of virtual private network (VPN) technology for remote access have become increasingly clear in recent years, particularly as more and more enterprise applications migrate to the cloud. In addition, the sudden impact of stay-at-home orders across the globe in response to the

coronavirus pandemic has only cast additional light on this scenario, as millions more knowledge workers have sought secure remote access to the systems and applications they need to do their jobs from home.

Omdia has charted the evolution of VPN alternatives that have emerged, such as software-defined perimeter (SDP) and identity-aware proxy (IAP), grouping them under the heading of zero-trust access (ZTA) technologies.

Axis Security's offering would also fall under this category, but its approach differs from both SDP and IAP.

First, it is agentless, whereas most vendors in the other two ZTA sub-groups rely on an agent on the end-user's device to provide data on the user and device, as well as to make the access request.

Second, it is delivered in SaaS mode and sits in both the control and data planes. This is different from the SDP architecture, whereby the SDP controller sits only in the control plane, and makes the Axis service look more like an IAP.

However, unlike IAP offerings, Axis does not run its own network, enabling customers to run the traffic however and wherever they like, provided it traverses the App Access Platform. The Platform itself runs in AWS, but is agnostic regarding which cloud a customer's app may reside in. If it is in Azure or GCP, for example, the request to access it merely needs to go through Axis on AWS and can then be routed to the appropriate cloud once authorized, a process which is transparent to the end user.

Axis enables zero-trust application access to applications with its technology, which differentiates it from the more widely used zero-trust network access (ZTNA) acronym. Omdia does not use ZTNA because it considers the term incorrect (accessing a network is not the purpose of these new technologies).

With Axis Security's App Access Platform in operation, a customer's employee requests access from their device (laptop, tablet, or smartphone) to a back-end application. The request goes to the Axis Cloud, which queries an identity provider such as Active Directory or Okta, as well as taking into account information:

- from a geolocation service
- from any mobile device management (MDM) system the customer is running
- about the IP address
- about the time that the request is being made
- about previous access from that device.

Based on all this data, the system evaluates the user and device, deciding whether to grant access to the application, and if it does, the session is set up with another piece of software called the Axis Connector sitting in front of the app (in a data center or in the relevant cloud).

Access is granted only to the application to which it has been requested. This approach differs radically from overly permissive conventional VPN technology, and for this reason the technology can be considered a zero-trust offering. In addition, the evaluation is ongoing (not just at the start of the session) so that access can be terminated if conditions change.

As a further layer of security, any content that the user seeks to post to the application, such as customer information, is subjected to disassembled and reassembled in the Axis Cloud where the

Platform resides, using a content disarm and reconstruction (CDR) approach to remove any malicious code lurking within it, such as the DejaBlue bug, which exploits a vulnerability in Microsoft's RDP protocol. There is also the potential for it be recorded for auditing and forensic purposes.

Background

Axis Security was founded in 2018 by CEO Dor Knafo and CTO Gil Azrielant. Both spent time in the Israeli Defense Forces' Unit 8200 for cyberwarfare. Knafo went on to be a senior security researcher at Fireglass (a browser isolation vendor acquired by Symantec), then held the same post at Symantec after the acquisition. Meanwhile, Azrielant was a co-founder and the CTO of Cool Cousin, a travel tech firm.

The vendor has raised a total of $17m in venture funding, most recently announcing a $14m Series A round when it emerged from stealth in March 2020. The round was led by Ten Eleven Ventures, with further participation of seed funding investor Cyberstarts.

Current position

Axis Security began a beta testing program for App Access Platform with a handful of enterprise customers in August 2019, and by the time it emerged from stealth in March 2020, the technology was in production in a customer base that it says is "in the tens", with particular strength in sectors such as hospitality, aviation, and healthcare.

Several vendors in ZTA, and particularly ones with no legacy VPN business, tout their technology's ability to replace VPNs altogether for their customers' remote access needs. Axis adopts a more cautious approach, targeting large enterprises with specific use cases, typically those that require fast deployment, strong application/access security controls, and clientless access, namely:

- Remote access for non-employees such as people working for partners or companies in their supply chain, as well as short-term contractors requiring access to applications but not going onto the customer's Active Directory as permanent staff.
- Merger and acquisition scenarios, where a customer has made an acquisition and needs to grant a new set of employees access to its enterprise applications quickly, before all the work of merging the two entities' directories has been carried out.

Neither use case is suited to conventional VPN technology, so Axis can enter an account and coexist peacefully alongside it. This can enable quicker customer wins for Axis, but once installed in the account, the vendor will hope that by showing itself to be secure and easy, both to deploy and to use, the App Access Cloud will persuade customers to extend its use for their entire remote access requirements.

Axis points out that, because it is in the cloud, its platform has the potential to do even more analysis. An example the company cites is behavioral analysis, which could further enhance decision-making.

The offering will become still more compelling when Axis expands its support beyond on-premises apps to those that its customers are running in infrastructure- or platform-as-a-service (IaaS and PaaS) cloud environments. If it can also serve access to SaaS applications such as Salesforce, Office 365, and Box, Axis will be able to claim coverage of all application access requirements, as well as centralized management, policy, and visibility.

In terms of its competitive environment, Axis says the vendor it sees most often is Zscaler with its ZPA offering, but there are several other players, including Perimeter 81, which uses the zero-trust application access term for one of its services. However, it operates its own network.

Data sheet

Key facts

Table 1: Data sheet: Axis Security

Product name	Application Access Cloud	**Product classification**	zero-trust access
Version number	n/a (SaaS product, no public version numbers)	**Release date**	GA March 2020
Industries covered	all (horizontal solution)	**Geographies covered**	North America
Relevant company sizes	enterprise	**Licensing options**	annual subscription, user-based
URL	www.axissecurity.com	**Routes to market**	direct, channel/VAR, MSSP
Company headquarters	San Mateo, CA, US	**Number of employees**	25

Source: Omdia

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

Further reading

Omdia Market Radar: Zero-Trust Access, INT005-000094 (March 2020)

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

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

CONTACT US

omdia.com

askananalyst@omdia.com