White Paper

axis security

Enabling a SASE Approach to Private Application Access and Security

Learn how Axis Security's Application Access Cloud enhances Secure Access Service Edge (SASE)

Executive summary

Enterprises have many private applications. These vary from well-known big brand accounting applications to industry-specific applications, such as those for logistics and input sourcing. While many parts of enterprises have undergone digital transformation, the delivery and security of private applications to demanding business users have lagged. Fundamentally, they still rely on legacy security and access methods. While some of these applications, along with their security controls, are migrating to the cloud, they are taking with them a legacy mindset resulting in the same underlying security issues. This "cloudified' legacy approach has failed to deliver the business agility expected, causing an unnecessary complexity and cost burden.

Axis Security's Application Access Cloud™ delivers private applications to anyone, anywhere over any network connection. It uniquely delivers the architectural approach of Gartner's secure access service edge (SASE) by consolidating many access and security capabilities into the underlying service delivered as a communication platform. Application Access Cloud™ reduces complexity and cost, enables new business scenarios, improves and centralizes security, simplifies end-user access, and increases the effectiveness of network and security staff.

In terms of security, with built-in prevention, detection, and response, Application Access Cloud also aligns well with the Continuous Adaptive Risk and Trust (CARTA) strategic approach from Gartner for a security architecture. It also expands to the CARTA identity and access management model by providing adaptive access and continuous user access management.

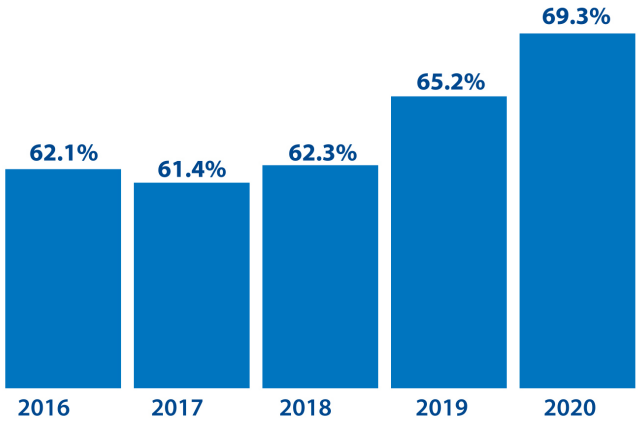
By enhancing SASE and adhering to CARTA, Application Access Cloud brings true digital transformation and business agility to private applications. Even more, it does so while reducing IT complexity and increasing security and business agility.

Introduction

Digital transformation is dramatically improving business economics. But at the same time, it is negatively impacting IT with complexity from legacy technologies that are applied to new cloud-centric IT (or mobile workforce). As enterprises become more reliant on mobile workers with flexible work arrangements, they are demanding consumer-like access that is simple, fast, and safe for all applications. To support this shift, IT departments need to change their systems and processes significantly and pay particular attention to the security of the applications and the underlying infrastructure.

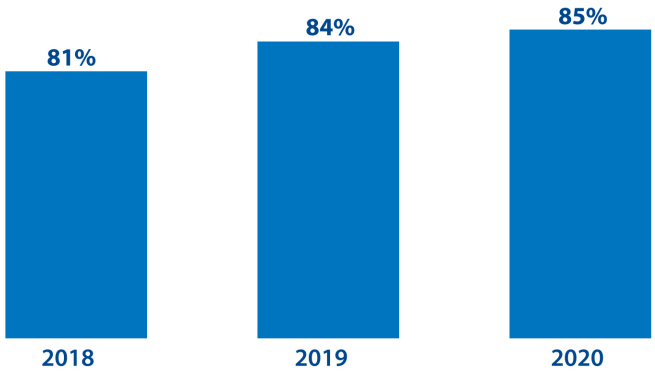
At a time when the most significant barrier to effective defense is a lack of skilled personnel, new solutions must be easy to use and take considerably less employee time maintaining them when compared to the legacy systems they are replacing. New solutions must incorporate continuous visibility to ensure that the right end-users have the right access at the right time and provide real-time session monitoring to be able to respond quickly to any bad behavior or risk. Finally, they must improve the security posture of the enterprise and the potentially vulnerable resources they are exposing in the effort to help end-users and the business.

Percentage of Organizations Indicating Compromise is More Likely to Occur Than Not in the Next 12 Months



Source: 2020 Cyberthreat Defense Report, CyberEdge Group

Percentage of Organizations Experiencing a Shortfall of Skilled IT Security Personnel



Source: 2020 Cyberthreat Defense Report, CyberEdge Group

In the 2020 Cyberthreat Defense Report, published by CyberEdge Group – given the underlying legacy security issues and pressures on staff – it is no surprise to see that 69.3% of organizations expect that a successful cyberattack will compromise them in the coming year. That is an increase of almost eight percentage points from 2017.

One area that has fallen behind and has not fully realized the promise of digital transformation is the organization's private applications. This paper will show how adopting Axis Security's Application Access Cloud will bring digital transformation to private applications and deliver business agility that will give organizations a competitive edge and help keep businesses safe from bad actors.

> Some of the acquisitions are very small mom-and-pop operations with zero security capabilities. (These are) highly dirty networks that we had to assume to already be compromised. This rapidly became one of our most prevalent use cases."
>
> **Curtis Simpson**
> **Former Global CISO of Sysco**

Digital transformation accelerates business but challenges security

When implemented well, digital transformation comes with several benefits that increase an enterprise's agility and competitiveness in the market. For example, moving to cloud computing and making better use of mobile and freelance workers can reduce costs and increase efficiencies. Enabling access and collaboration leads quickly to safe and more efficient organizational integration following mergers and acquisitions. Companies that have implemented digital transformation for their private applications should benefit from flexible and easy access. At the same time, they should gain an enhanced security posture from capabilities such as continuous session monitoring and policy-based access controls.

Digitizing areas of business fundamentally changes how businesses operate and significantly enhances the way they deliver value to their customers and partners by encouraging cooperation both within the company and with external partners. This increasing agility opens the door to innovation but also increases the risk of a security breach.

Business applications locked down with restricted access now must be opened up, not only to employees but also to contractors and other third parties, such as partners and customers. The number and diversity of endpoints are increasing, driven by bring-your-own-device (BYOD) policies, the Internet of things (IoT), and broader third-party access. Not only are businesses requiring more general access to their private applications, but they are also moving those applications away from legacy data centers and into the cloud. This move to the cloud, along with the increasing number of remote and third-party devices needing application access, is forcing the security perimeter around end-users to change. The well-defined perimeter with a hard edge protected by devices such as firewalls has become elastic and porous. In this environment, legacy security controls are struggling to provide the required flexibility and protection.

Providing broader access and moving to the cloud increases business agility and delivers significant cost savings. However, if you still take a legacy approach to security, this move can have dire consequences, as demonstrated by the infamous Target breach in 2013.

Carrying on a legacy approach to security also slows down business since the risk of a violation is often met with restricting access, forcing the user to follow a lengthy process to gain the required access. Old methods, such as VPNs, provide minimal visibility into who is accessing what and have high maintenance costs that worsen the staffing shortages.

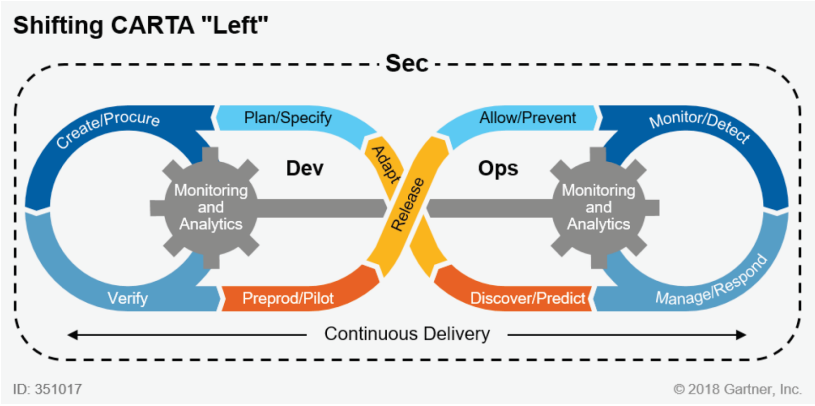
Digital transformation security needs a new approach

A cyberattack can temporarily paralyze a large enterprise, but smaller enterprises may never recover. Enabling mobile, remote, and third-party access to applications cannot be at the expense of security, and yet security should not be so overbearing that it slows down the business. Legacy network access and network security architectures were designed for a headquarter-centric age of computing that is fast disappearing. Their reliance on labor-intensive appliances – physical or virtual – is no longer efficient or effective in meeting the best practices of security today. Such an approach is becoming increasingly inefficient, costly, and risky.

The architectural approach of Gartner's cloud-delivered secure access service edge (SASE) model consolidates network and security services to increase the speed and agility of business while simplifying and reducing the complexity of security and access. It calls for the dynamic application of policy-based secure access regardless of the location, network, or device. The perimeter is dynamically created, and any connections to an enterprise's private applications are closely watched.

Continuous visibility into end-users, systems, activities, payloads, and the network is the core of Gartner's adaptive security architecture named CARTA. CARTA stands for continuous adaptive risk and trust assessment. This approach moves away from a security model that is heavily dependent on preventing access and attacks to one that, while still keeping in place prevention technology, focuses more on an agile system that is continuously monitoring and detecting activity. This model will assess and prioritize risk so that proper responses can contain breaches and limit the lateral movement of attacks.

Identity and access management must use the CARTA approach to respond to damaging changes in an end-user session after access is granted. Continuous monitoring and assessment of an end-user session are imperative to reduce applications or related data risks. Unfortunately, even some of the newer technologies stop monitoring an end-user once they have passed the criteria for gaining access to an application or the network. With what Gartner refers to as a "left shift," a CARTA approach must be applied to applications in development and those in production.



Source: Gartner (April 2018)

The Axis Security Application Access Cloud implements the consolidation of network and security services of the SASE model, as well as providing a CARTA style architecture that applies to applications both in development and in production.

Challenges to legacy security of application access

Application Access Cloud is a better, more secure method for private access, replacing solutions such as the legacy VPN or the newer client-initiated zero-trust network access solutions.

While VPNs have evolved over the years, and security has improved, the underlying issues remain. Any solution that gives access to the corporate network is inherently dangerous, and it supplies a large attack surface for a security hacker. Once in the corporate network, lateral movement by the attacker can cause enormous damage to a business, as witnessed in the aforementioned Target breach that started with access to the HVAC system and ended up with 41 million customer payment card accounts being affected. VPNs also require complex sets of network and port-level access control lists and firewall policies where the slightest of misconfigurations can have dire consequences.

Along with the security issues, VPNs are very labor-intensive to set up and keep operational. As hardware appliances, they require considerable maintenance. This complexity does not just make VPNs costly, it also slows down the business while trust models are designed and implemented. That same hardware and user-based licensing are challenging to scale under sudden demand. Recent events have exposed the complexity, scalability, and flexibility limitations of VPNs, which could have existential repercussions on business.

To overcome the security, cost, and usability issues associated with VPNs, client-initiated zero-trust network access (ZTNA) solutions provide a different approach. You install a client on the end device that, once authenticated, connects to the applications through a gateway. While this is a step forward, it still does not work well in an enterprise with BYOD policies or where third-party access is needed. There is also low visibility into the application-level and limited application isolation. Further, the costs associated with managing and implementing "client-initiated ZTNA" can be high, especially in a business environment that is continually changing. ZTNA is often scalable, but it merely recreates the security, monitoring, and access limitations of the physical networks and VPNs they attempt to replace.

A better way forward: Application Access Cloud

The Axis Security Application Access Cloud builds on a zero-trust approach in a way that end-users gain access to applications from virtually any Internet-enabled device without ever needing to connect to the corporate network. By removing direct corporate network access, secure, tightly managed private application access is delivered to anyone, anywhere, on any device in minutes without the associated dangers that legacy approaches have. There are no network or network access changes needed. As an application-level solution, Application Access Cloud removes the need for hard-to-manage VPNs or costly hardware appliances, releasing finances and labor.

Axis Security's Application Access Cloud secures end-user access to private applications without ever connecting end-users to the corporate network or even to the applications themselves. The result is amazingly simple access that is more secure than ever with continuous visibility and control over end-user activity. Following the Gartner SASE model and CARTA imperatives, Application Access Cloud delivers many business and security advantages that enable enterprises to digitally transform all their private applications while further enabling their businesses with increased agility.

Business advantages of Application Access Cloud

Using VPNs, agents, or appliances adds a layer of complexity that slows business down. Application Access Cloud speeds up business as it provides simple, smooth access to applications that are seamless to the end-user with no client-side software to install. This solution delivers a better end-user experience that facilitates the adoption of new applications by end-users, and it accelerates the onboarding of new staff and third parties, such as suppliers. When it comes to mergers and acquisitions, not only is onboarding faster, but it is also more secure since there is no corporate network access allowed. Application Access Cloud's shielding of the corporate network reduces risk when third parties are accessing applications through their unmanaged devices, which may well be compromised. No corporate network access with no direct application connection means there is no need for new end-users to wait for their devices to be sanitized and secured before they are allowed to access the applications.

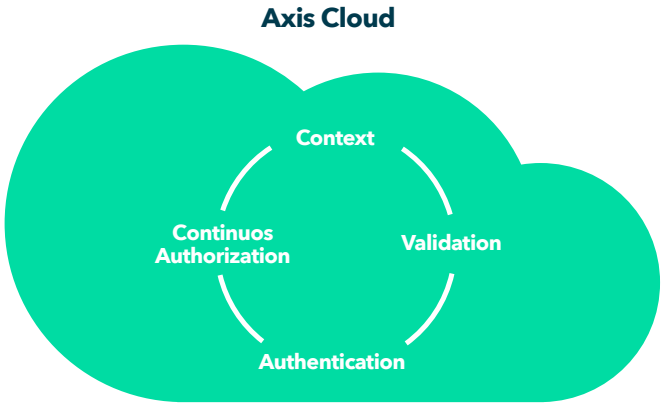
When designing and developing new applications using Application Access Cloud, security and secure access are built into the environment. This built-in security allows for the applications to be created, updated, and tested, speeding up the development and test cycle to bring faster business benefits.

There are also cost and staff savings. Application Access Cloud can be deployed in minutes, not weeks, and has no physical or virtual appliances to manage. You can now apply the enormous amount of time spent in configuring and managing legacy appliances to other areas of IT that can accelerate business. By freeing up security staff from the mundane labor-intensive tasks of managing legacy hardware, it helps alleviate IT security staff shortages. Additionally, it provides time for security professionals to focus on more critical aspects of modern cybersecurity.

Security advantages of Application Access Cloud

Serious breaches can occur when your corporate network is infiltrated. Leveraging Isolation Access Technology™, the Application Access Cloud enables the separation of private applications from the corporate network, virtually eliminating the application attack surface and preventing bad actors from gaining a foothold in the corporate network. The continuous monitoring of authenticated end-users after they have gained access to an application is required in the second imperative of CARTA but is lacking in most solutions today. Adaptive Access Technology™ from Axis Security continuously collects and analyzes real-time behavior for each end-user session. Through this analysis of end-user activity, it can adjust the security policy and user access in real-time.

The Axis Cloud is also able to add additional layers of control to an application. For example, it can stop downloads of files in high-risk end-user scenarios or initiate the visual recording of a remote desktop session.



Keeping bad actors out of the corporate network is essential, so never allowing end-user devices to attach to the corporate network through legacy VPNs significantly mitigates attacks stemming from end-user devices. Many breaches result from configuration errors, especially as networks and network security, get more complicated. By reducing or removing the use of VPNs altogether, the configuration risks and issues around the levels of privileged network access are eliminated.

Conclusion – Rethink your secure access service edge for private applications

For the modern enterprise, continued and widened access to private applications yields significant business operations benefits. Yet with these benefits and the move to the cloud comes a higher degree of risk due to the weakness of disparate legacy network security systems.

The direction is clear – the Gartner SASE model calls for a ground-up approach that integrates network and security functions, and the CARTA imperatives require continuous monitoring of the entire end-user session to respond to changes and unexpected behavior. To this end, the Axis Security Application Access Cloud delivers a whole new approach that makes private application access amazingly simple. It securely connects end-users to private applications while avoiding the unnecessary complexity of legacy VPNs, agents, or appliances that carry high cost and risk overheads.

Axis Security enables organizations to gain the agility and flexibility needed to succeed today and well into the digital future.

To see the amazing simplicity and power of Application Access Cloud, request a demonstration by visiting www.axissecurity.com

axis security

Axis Security
3 East Third Ave, Suite 203,
San Mateo, CA 94401

Phone: +1-650-850-8991
Email: info@axissecurity.com