

CASE STUDY

High Tech SaaS Provider Migrates to Zero Trust Secure Cloud Access in 24 hours

Customer Background

Our customer is a SaaS-based Meetings, Incentives, Conventions and Exhibitions (MICE) aggregator that connects group travel organizers with hoteliers worldwide. With a pan-global network of 200,000 hotel partners, their cloud platform offers solutions to group travel organizers and travel and hospitality providers.

The company has an all-cloud infrastructure with developers working remotely, on-premises and geographically distributed within and outside the continental US. Their insurance underwriters asked them to meet specific compliance requirements with multi-factor authentication (MFA) to ensure authenticated access to anyone logging in to their development platform. However, their VPN solution at the time did not support either 2FA or MFA.

The last two years have seen the single most significant shift to remote work. IT environments had to evolve quickly to accommodate changes in working habits and customer behavior.

There is another parallel shift underway. According to [McKinsey](#), \$8 out of over \$10 of IT hosting will go to the cloud by 2024.

The combination of these trends requires a replacement of networking centric security with cloud-centric solutions. The untrusted nature of networks and proliferation of devices requires that organizations adopt a zero-trust approach. And when it comes to zero trust, identity and access management are just starting points for any company. Companies recognize that modern zero trust solutions must enable remote work and agility without impairing security. Our client is one such company.

“Compliance is a check box. But, privacy, security and compliance must work in tandem to help manage risk. We started the journey with Appaegis to get visibility for compliance. We ended up with a solution that delivers compliance, provides zero-trust remote access to our cloud infrastructure and integrates MFA.”

- CISO

A Transformational Switch to a New Normal

With their Dev-heavy workforce, protected access to critical cloud infrastructure was imperative.

The cloud access security solution they chose needed to help them achieve Zero Trust with:

1. An identity-based perimeter that restricts access for all users, applications and cloud infrastructures.

Zero-trust security principles with continuous monitoring of identify changes and visibility to ensure always-on verification. All users are authenticated and authorized before being allowed to access a resource.

2. Complete visibility into user activity, focusing on permission visibility and data-aware access to meet compliance requirements.

Zero trust solution to allow brokered gateway access and deliver performance, TCO and scalability.

3. Enforce strict security by integrating with internal services to include essential management services.

The client wanted to prevent risky behaviour such as using shared passwords. They also had VPNs and infrastructure that they had invested in for their campus and on-premise teams and wanted something that would easily sit on top of their current security stack.

4. Minimize the usability impact on development engineers.

They were mindful that adoption resistance by even one user could create easily exploitable security gaps with any solution they implemented. Therefore, they wanted to ensure they signed up for one everyone on the team found easy to use.

With Appaegis Access Fabric, Zero Trust Isn't a Tool; It's a Strategy

More than 80% of all attacks involve credential theft or misuse in the network. Appaegis Access Fabric is helping companies recognize this risk and eliminate security challenges using zero trust principles. As its basic principle says, zero trust means no device, interaction, or endpoint is trusted until otherwise verified.

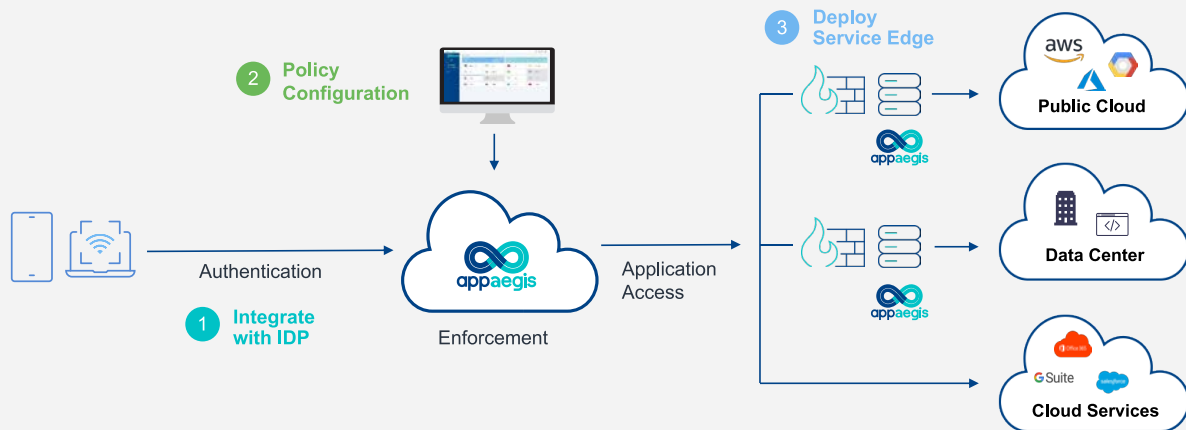
Once introduced to Appaegis, the customer quickly realized our solution had the potential to solve their core problem of compliance while augmenting their existing security solutions.

And that it was a simple plug and play principle that wouldn't need any additional coding to connect Appaegis Access Fabric to their existing solution. For them, our solution elegantly underscores the agile essence of the cloud.

Amongst all the solutions they researched, Appaegis' offering was the only one that could solve their problems today with the current capabilities and not forecasted benefits. Appaegis met every one of their needs upfront - so much so that they could sign up and start using our solution immediately. In addition, they found Appaegis' simplicity of setup and the intuitiveness in the use and management to be game-changing.

They could roll out Appaegis to all the users within their development organization with minimal training. While Appaegis offers extensive customer training and support, since platform rollout is hugely intuitive, our clients managed it themselves in two 30-minute sessions. Appaegis is so easy to use; it eliminates any friction in adoption.

Beyond Breach Prevention. Appaegis Access Fabric is So Much More than a Zero-Trust Brokered Gateway.



What started as a check box for compliance has grown into an implementation that effectively enhances security. Key among these are:

- 1**
The ability to control access to cloud resources from any device at anytime from anywhere
- 2**
The ability to manage who has access to what data and what they can do with the data
- 3**
Provide the ability to record sessions and replay them for troubleshooting or root cause analysis

An unanticipated yet welcome benefit of the session recording capability allows the company to use the recordings to train their engineering teams. As a result, these recordings have become essential for guidance and direction on best practices. In addition, the robust security offered by Appaegis combined with show-and-tell has helped create a culture where developers feel like they have all the agency to make mistakes without fear of breaking the platform.

The investment in Appaegis has created a shift in mindset. Appaegis delivers:

- Secure access to the client's cloud platform
- Provides a platform to implement a second factor of authentication
- Offers education and guidance in a non-punitive setting that supports growth and builds capability

And of course, they are also planning on using session recordings as evidence for their annual SOC compliances.

Appaegis Access Fabric offers five key benefits to any organization:



Complete control over cloud access:

Agentless access and real-time policy enforcement from any device to any platform and application



Data security: Context-based access and at-source data retention



Visibility and monitoring: With context and insights



Malware protection: With no lateral spread and reduced attack surface



Seamless onboarding: Frictionless adoption from rapid app deployment, training and user implementation in under 30 minutes.

Conclusion

Our platform offers out of the box MFA and SSO integration with agentless identity-aware access. Appaegis IAC also has built-in integration with networking and application services. And our APIs allow easy integration into existing workflow and security solutions.

The price of convenience should never be security. And with Appaegis IAC, that is a trade-off you never have to make. And the customer was able to meet the requirements to get cybersecurity insurance.

Appaegis secures cloud infrastructure access where it matters. We use an enterprise access browser to observe every interaction between users and the cloud. This provides complete visibility into access to applications and control over what data users can access. We are redefining the standard for secure access to cloud infrastructure.

Connect with us

555 Bryant St. Suite 220 Palo Alto, CA 94301
+1 669 699 1122 · info@appaegis.com

