axis security

Case Study

A Global Vacations Company Protects Their Data (and Their Leisure Time) with App Access Cloud

How a global vacations company traveled away from VPNs and landed a simpler way to access private apps

Two million members. Seventy resorts. Countless hotels and condos. A public entity since 2011, this vacations company call themselves the world's leading "pure play" public timeshare company.

With a vast network of teams and partners around the world dedicated to maximizing their customers' valuable leisure time, this organization is well aware of the potential security issues that could come from over-exposing networks, customer data and vulnerable legacy applications for relatively untrusted users. That's why they've chosen Axis Security to create a Software Defined Perimeter based on a zero trust access posture.

> "Our huge portfolio of legacy enterprise applications is probably the most unique thing about our business. Every one of our call center agents and hundreds of thousands of sales people all need to interact with these legacy apps."
>
> **Head of Information Security (CISO)**

Providing third party access with lower risk

Between their on- and off-premises sales processes and a two-million-member exchange network, the organization faces considerable enterprise complexity with hundreds of custom-built, often legacy, internal applications used to enable partners and customers.

But different employees have different data needs, so the CISO's team set out to structure application access, enabling partners with different levels of access without exposing them to the network, which would dramatically increase risks.

In order to enable partners and still keep applications secure, the CISO sought tighter security that could establish a Software Defined Perimeter, an architectural approach that lays a foundation for implementing a zero trust access posture.

More Flexibility, Less VPN

The existing vacations company VPN and network had become too costly to license and upgrade, and too complex to implement and maintain properly given the business-level demands on it. They weren't flexible or dynamic enough to integrate with multiple business partners or support new sale centers. The CISO recalls, "It caused IT to act slower because we didn't have the flexibility that we needed." Business agility was limited by IT.

As a result, their legacy systems actually increased the risk of security breaches – especially when it came to enabling partners. The team viewed VPN as a "dumb" connection that couldn't deliver improved security capabilities. The CISO needed a solution where they could have these capabilities built in as needed and not through unscalable hardware.

He and his team were also hoping to enable micro-segmentation "isolation": A security solution that addressed client devices (which he assumed were compromised) and placed them on different networks away from servers, databases, and other key internal assets external users never needed to touch.

One of the more urgent needs involved security around remote testing, for which the vacations company employed two security solutions.

> I wanted something with a robust infrastructure, something that could give us threat detection, misuse detection, data loss prevention, different types of security controls, etc."

Head of Information Security (CISO)

> One was to put (the test environment) on the Internet and do IP whitelisting. It's technically feasible, but involves a lot of people and it was very fragile and broke a lot, was complex to maintain and manage, and just a really bad way to do it in general.
>
> Our other option was to try to come up with some kludgy VPN that would work on non-company-owned assets, on mobile phones, on laptops of different platforms. But the VPN prevented it from acting like a native experience."

Head of Information Security (CISO)

> “There was a strong willingness from the Axis team to help us solve our problems and solve new use cases. It’s been a very collaborative, positive experience. That meant a lot to us.”
>
> **Head of Information Security (CISO)**

How Partnership Adds Value

Searching for the solution took some time. They looked at Zscaler’s private access solution and a few other vendors. Most vendors failed because their products weren’t mature enough, focusing mostly on Web traffic, and/or were unable to achieve a zero-trust posture. Most just weren’t ready or architected for their needs.

In one such use case, Axis worked with the vacations company’s security architecture and applications teams, to immediately relieve key pain points around providing secure remote access to developers who were testing an app. Axis enabled them to make the app Internet-facing earlier in the life cycle, without exposing the application to the Internet test environment. In another use case, Axis enabled the vacations company’s team to take an older, out-of-date application and quickly make it securely available without the use of a VPN.

> We were already testing Axis, so we applied it and it quickly solved the problem VERY fast. Axis found a better way and delivered it successfully to the application teams."
>
> (Axis was) very responsive and willing to listen to our use cases and develop the product and make it work. We wouldn't get that sort of response from a bigger, more legacy solution."
>
> **Head of Information Security (CISO)**

It Just Works

Short-term successes included the replacement of reverse proxy solutions like IBM's WebSEAL and Microsoft's Forefront Threat Management Gateway – legacy solutions that didn't have broad usage in the organization to begin with. The CISO also hopes to see Axis replace VPN and Virtual Desktop solutions altogether in the next 3-5 years, which could save them time and money while reducing IT complexity.

Axis provided solutions for problems beyond the initial scope – specifically with remote testing. Apps teams would publish lower end test environments to the Internet for testing, even though some of the company's lower environments were already exposed. It's a risky scenario, because these environments are still in development; they contain some data, so they're not fully sanitized, and therefore ripe for discovery and exploitation.

The quick win instantly reinforced Axis' reputation and technical credibility and encouraged Ludlow and team to move forward to implement a zero-trust access system for their partner ecosystem.

The global vacations company continues to find new uses for Axis, now that they can securely "publish" their applications to the Internet – Internal finance applications, additional test environments, even some core business apps – while reducing risks.

Ready to improve security and save money?

Learn more at:
axissecurity.com