JELLYVISION ENABLES SECURE ACCESS ACROSS HYBRID ENVIRONMENTS

Seamless access across multi-cloud and on-premises environments simplifies security administration and increases employee productivity.

Background

Jellyvision is committed to reinventing how employees choose and use benefits. Their sophisticated technology delights and guides employees to make better benefits decisions — leading them and their employers to a more prosperous future. Headquartered in Chicago, IL, Jellyvision has about 300 employees, as well as third-party contractors, working in the office and remotely.

Challenges and Requirements

Jellyvision had an end-of-life hardware VPN solution that was difficult to manage. It required restarting, was unable to limit access to specific resources and delivered a poor end user experience. Jellyvision, a remote-first company, needed an alternative to restrictive and vulnerable VPNs and wanted to replace a suboptimal service with a solution that:

- Delivers account separation for security controls for employees and third-party contractors to on-premises and cloud resources such as AWS
- Unifies policy framework and consistent end user experience for hybrid and multi-cloud environments
- Improves end user experience including reduced log-in time, decreased latency and overall ease of use
- Is flexible and future-proof to meet constantly changing compliance requirements
- Offers easy installation, configuration and deployment, configure and deploy with minimal administration

Recognizing the limitations of traditional solutions and the merits of Zero Trust security, Jellyvision elected to implement a Zero Trust Network Access (ZTNA) solution.

Requirements

Appgate was the first vendor to catch the company's attention. After evaluating other providers, Jellyvision choose Appgate SDP, an industry-leading ZTNA solution, because it delivers superior benefits in the areas of security, administrative workload and end user experience including:

- Easy admin set up so users can access everything they need no matter what network or account a resource is on, and each user has a one-to-one network segment not limited to a single resource or account
- Precise, fine-grained access control and unique multi-tunneling capability keeps developers productive by eliminating disruptive account switching required by traditional VPNs
- End users enjoy faster log-in times, reduced latency and an improved experience
- Single packet authorization (SPA) helps reduce security incidents by hiding infrastructure from unauthorized access
- Reduced regulatory compliance costs and time by reducing scope and audit complexity

INDUSTRY
SaaS

USE CASES
Employee VPN replacement
Third-party access
Secure DevOps
On-premises access

CHALLENGES
Multiple AWS accounts
Distributed teams
Compliance support

BENEFITS
Quick, easy solution deployment
Simple to configure policies, conditions and entitlements for all users, devices and workloads
Precise, fine-grained access control
Makes network invisible with single packet authorization (SPA)
Transparent user experience

"When we saw the Appgate SDP demo, we were very surprised at what it could do. The least privilege access and entitlements were exactly what we needed, and the SPA feature caught our attention because it provided an extra level of security. It was easy to set up, and Appgate was there to help. The leadership team and users praised how seamless it is to use."

Damian Zavala, lead systems engineer, Jellyvision

About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Learn more at appgate.com