Beam SUNTORY

CASE STUDY

Beam Suntory improves security and performance with Prisma SASE

Integrated security and networking prepares a global distiller for the digital future

paloalto®
NETWORKS

IN BRIEF

Customer

Beam Suntory

Industry

Consumer goods

Country

United States

Products and services

Distilled spirits

Organization size

74 locations

4,500 employees

Website

www.beamsuntory.com

Challenge

+ After an incident, security urgently needed to be upgraded
+ Legacy network components created latency and costly downtime

Requirements

+ Comprehensive security solution to address perimeter, identity, and proxies
+ SD-WAN with portal-based remote management

Solution

Prisma® SASE, including Prisma Access and Prisma SD-WAN

Beam Suntory is the world's third-largest producer of distilled alcoholic beverages. Its digital network connects 74 global locations, where over a hundred iconic brands, such as Jim Beam®, Maker's Mark®, and Courvoisier®, are produced, warehoused, and distributed; all aspects of the company's operations are managed in an ERP system from SAP.

From ordering ingredients to delivering a bottle of whiskey to a retail store, Beam Suntory's digital estate plays a vital role in the business.

In 2018, a major security incident occurred, motivating the company to take a new approach to security. Soon after, Senior Network Architect Qun Wei joined the company and was tasked with replacing an aging network architecture.

Beam Suntory launched two parallel projects in 2019: one to upgrade the company's network security infrastructure and a second to replace legacy network elements with SD-WAN.

Security concerns and downtime require an upgrade

The 2018 incident shut down Beam Suntory's back-office, leaving the company temporarily unable to operate. Beam Suntory knew it needed to improve security—and that its global footprint and complex network architecture increased the challenge of keeping the company's network and data assets secure and available.

Upon analyzing its security estate, Beam Suntory realized that many of its security capabilities were outdated, inconsistent, and lacked the scalability the company required. Legacy firewalls needed to be upgraded, the hardware-based web proxy solution wasn't meeting expectations, and the intrusion detection system (IDS)—which was only present in the data center—needed to be extended across the entire network.

At the same time, legacy components of its network architecture urgently needed to be replaced. At some 24/7 manufacturing facilities, multiprotocol label switching (MPLS) circuits caused periodic losses of connectivity, costing $80,000 per hour in interrupted productivity and requiring several hours to repair.

Remote users needed to connect through the data center to access cloud-based applications, creating latency and overburdening the network. And with a wide range of system components in locations throughout the world, Qun Wei's team struggled to provide adequate management and maintenance from the company headquarters in Chicago, IL.

An integrated approach to securing the network

With these challenges pressing concurrently, Qun Wei and his team saw an opportunity to adopt an integrated solution. Rather than patching holes, they took a proactive approach, setting requirements for the combined security and networking projects with an eye to the future.

For network security, Beam Suntory needed a solution that could scale to meet its global needs. IDS functionality had to extend from the data center to the entire network, and proxy functionality needed to be replaced.

For the SD-WAN project, Qun Wei's primary requirement was to overcome the connectivity challenges of MPLS. He was also interested in gaining portal-based, cloud-delivered management and diagnostic tools. And it was important that deployment be straightforward, since no one on his team had experience with SD-WAN.

As both projects progressed, Qun Wei and his team realized that rather than pursuing two separate projects, they could combine their security and network transformation efforts by adopting a SASE architecture. This approach could meet all of their requirements while delivering additional benefits. Eliminating their reliance on the legacy remote access virtual private network (VPN) could reduce latency and help manage data center traffic loads. And integrated, cloud-based security products could move security beyond the traditional perimeter.

Meeting combined security and networking needs

Palo Alto Networks Prisma SASE, the industry's most complete SASE solution, met all of Beam Suntory's needs by integrating Prisma Access for security and Prisma SD-WAN for network functionality. With consolidated, best-in-class security and a cloud-native secure service edge (SSE) platform, Prisma Access secured the company's network, provided proxy functionality, and extended IDS from the data center to the entire network.

"The account team showed me how we could route all our remote users through Prisma Access, so they didn't have to connect through the data center," says Qun Wei. "That helped to reduce the load on the network."

Prisma SD-WAN, the industry's only next-generation SD-WAN, was deployed in parallel to replace edge routers. Its centralized cloud management met Qun Wei's desire for remote monitoring, and its ease of deployment simplified implementation. Following a six-month pilot with Palo Alto Networks engineering support, his team has been able to smoothly manage deployment at additional locations with minimal downtime.

Building on Prisma SASE, Beam Suntory was also able to enhance its network security by deploying cloud-delivered security solutions (CDSS), including WildFire®, Advanced Threat Prevention, and Advanced URL Filtering.

> " The account team showed me how we could route all our remote users through Prisma Access, so they didn't have to connect through the data center. That helped to reduce the load on the network.
>
> **— Qun Wei, Senior Network Architect, Beam Suntory**

Greater reliability and comprehensive security

By implementing Prisma SASE, Beam Suntory has significantly improved its security posture, network reliability, and performance. It's also simplified operations, making it easy for Qun Wei's team to manage network and security components.

Through Prisma Access and Panorama, the team can control all egress traffic and define whitelists and blacklists from a single location. Automation—including the ability to create and implement network-wide policies on the fly—results in meaningful time savings. And because Palo Alto Networks updates signatures and performs other dynamic updates, the IT team is able to stay ahead of potential threats. "When log4j hit," Qun Wei offers as an example, "and I went in to block the traffic, Prisma Access had already blocked it automatically. It was pretty cool. We were ahead of the game."

Prisma SD-WAN increased network speed and reliability, overcoming connectivity issues of MPLS. It also reduced latency, improving the user experience for remote users in all geographies.

When employees had to shift to remote work during the pandemic, Prisma SASE simplified the transition. Rather than logging in through the data center, users could directly access the productivity tools they need in the cloud. And for Qun Wei and his team, the visibility the solution provided ensured security, even with sudden proliferations of remote users and surges in application traffic.

> The product saved our lives and increased both the performance and the security level.

— Qun Wei, Senior Network Architect, Beam Suntory

Palo Alto Networks makes the business future-ready

Today, Prisma SASE provides secure access for Beam Suntory's more than 4,500 users. As the implementation has progressed, the company has seen a dramatic improvement in efficiency and security across its global network. "The product saved our lives and increased both the performance and the security level," Qun Wei says. It also increased his team's confidence in the network's efficiency, reliability, and security.

Now, Qun Wei and his team are working to entirely replace MPLS with Prisma SD-WAN, increasing bandwidth and reliability at every Beam Suntory location while reducing overall costs. And to further improve security, they're planning to adopt Zero Trust Network Access (ZTNA) by fully implementing the ZTNA 2.0 capabilities of Prisma Access.

Find out more about how Palo Alto Network's best-in-class solutions can improve security and network efficiency for your organization. Additional information is here.