



CASE STUDY

Innovating with a “cloud everything” strategy requires a cloud-driven security platform

Sumitovant Biopharma digitally innovates with the Network Security Platform from Palo Alto Networks.



IN BRIEF

Customer	Industries	Country
Sumitovant Biopharma	Pharmaceutical and Life Sciences	United States
Products and services	Organization size	Website
Biopharmaceutical therapies	1,200	www.sumitovant.com

Challenge	Requirements	Solution
<ul style="list-style-type: none">+ Building a network and security infrastructure from the ground up+ Connecting remote workforce during the pandemic+ Enabling efficient innovation	<ul style="list-style-type: none">+ Reduce risks to a global infrastructure+ Provide consistent security across a multicloud (AWS, Azure, and GCP) environment+ Maximize resources through ease of management on-prem to cloud+ Audit-proof security compliance	Selecting the Palo Alto Networks cloud-delivered networking and security platform to provide Zero Trust protection and access for its workforce, Sumitovant Biopharma deploys Prisma® Access, Next-Generation Firewalls (Software Firewalls [VM-Series virtual firewall and future Cloud Firewalls], PA-220, PA-440, PA-820, and PA-3410), GlobalProtect™, and Panorama™.

Sumitovant Biopharma is a patient-first, technology-driven biopharmaceutical company that's accelerating the development and commercialization of novel therapies for patients with rare conditions and other serious diseases. Through the company's proprietary computing and data platforms, scientific expertise, and diverse portfolio, Sumitovant has supported development of multiple FDA-approved products and a robust pipeline of early- through late-stage investigational assets addressing unmet need in pediatrics, urology, oncology, women's health, specialty respiratory and infectious diseases. Sumitovant is a wholly owned subsidiary of Sumitomo Pharma. (Sumitovant has combined with Sumitomo Pharma's other U.S. subsidiaries and is now Sumitomo Pharma America.)

The company has embraced digital transformation to achieve its goals of getting research-supported drugs to market faster and improving patient lives. Sumitovant's IT team had a vision to enable the company's researchers, data scientists, and sales and manufacturing teams to be as nimble as possible. While building out the company's network infrastructure from the ground up, the IT team sought a partner to help bring its vision to fruition.

"One of our biggest goals is innovation," says Trevor Cardwell, Senior Cloud and Network Architect at Sumitovant. "We want to come up with creative ways for people to be efficient and innovate without exposing ourselves to risk, which is not always easy."

“One of our biggest goals is innovation. We want to come up with creative ways for people to be efficient and innovative without exposing ourselves to risk, which is not always easy.”

— Trevor Cardwell, Senior Cloud and Network Architect, Sumitovant Biopharma

CHALLENGE

Unique strategy meets access and pandemic challenges

Sumitovant's "cloud everything" strategy is driven by Head of Enterprise Technology Jeff Miller and is central to the company's goal of allowing more rapid innovation for internal teams. By building the company infrastructure on multicloud environments and SaaS applications and eliminating physical servers, the company is more flexible. This allows it to add new products to its pipeline and get them to market faster.

Shortly after the company started doing business, the pandemic hit, and its employees shifted to remote work. The IT team needed to quickly put in place a plan to enable a remote workforce without any downtime or risk to data security.

Sumitovant initially provisioned remote workers to connect to the network using a VPN. While that worked reasonably well, the IT team concluded that a more modern connectivity strategy would further the company's goals. Sumitovant sought best-in-class, cloud-delivered networking and security to provide users immediate, uninterrupted access and lead the company into the future.

REQUIREMENTS

Protecting a global infrastructure

The company required a solution that could support its global infrastructure without security gaps and needed to build out end-to-end network security with limited resources.

Getting employees online as fast as possible was paramount when the company first formed, during the pandemic, and later as the company onboarded additional teams during mergers and consolidations.

Any security solution selected needed to provide consistent security and visibility across all major clouds—Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform. Once the multicloud security infrastructure was built, it needed to be easy for the small IT team to manage.

SOLUTION

An integrated security platform is the answer

The Network Security Platform from Palo Alto Networks was the clear front-runner at each stage of Sumitovant's journey to becoming a cloud-first, cloud everything company. Sumitovant considered several other vendors, but competitive products couldn't match the Palo Alto Networks portfolio when it came to ease of management and product integration. Partnering with Palo Alto Networks allowed the IT team to manage and secure the entire enterprise network, a project that would have otherwise required many more engineers.

Cardwell first experienced Palo Alto Networks Next-Generation Firewalls (NGFW) when he was with Roivant Sciences, and he was impressed. "I remember the first time I touched a Palo Alto Networks Next-Generation Firewall," he says. "It was the best firewall I'd ever encountered. It was amazing. I loved it." Miller, who chose the NGFWs for Roivant Sciences, and Caldwell decided they would continue that model as they built the infrastructure for Sumitovant. They selected Palo Alto Networks NGFWs to safeguard the new company with on-premises hardware solutions, then virtual solutions, ultimately leveraging more Palo Alto Networks products.

"I initially decided to bring Palo Alto Networks in because I wanted to go with the industry leader," Miller says.



Panorama's single pane of glass is super valuable. Spending a lot of time switching between consoles wastes time. We have a lot on our plate. Being able to go to one place in Palo Alto Networks Panorama and find the information we need adds a lot of value.

– Tracy Cohen, Senior Information Security Engineer, Sumitovant Biopharma

The right solution is a game changer

When Sumitovant was founded, it didn't have a dedicated office with network gear. Palo Alto Networks Next-Generation Firewalls and GlobalProtect network security client allowed the IT team to get remote users online securely. Once the company set up its office, most employees worked on-premises. During the pandemic, though, the team began exploring other options to connect workers as they worked from home.

In 2021, the IT team selected Prisma Access to replace its VPN and provide least privilege secure connectivity for the organization's remote workforce while offering a better and consistent employee experience. "From the second we provisioned Prisma Access, it was a game changer for us," Cardwell says. "It literally brought everybody online instantly and provided consistent employee experiences wherever they connected remotely. Palo Alto Networks tools definitely helped us improve our efficiencies."

Comprehensive management saves time and resources

Panorama allows the IT team to manage network security while centrally providing single-pane-of-glass visibility into traffic. "Panorama's single pane of glass is super valuable," says Tracy Cohen, Senior Information Security Engineer at Sumitovant. "Spending a lot of time switching between consoles wastes time. We have a lot on our plate. Being able to go to one place in Palo Alto Networks Panorama and find the information we need adds a lot of value."

A single global policy makes allowing or denying access simple and consistent for all offices while freeing up IT resources for other priorities. "The Network Security Platform allows us to focus on what's really important, which is moving into the future with modern technologies and not managing mundane day-to-day security tasks that should be automated," Cardwell says.

Simple deployment and prompt support

Deploying the Palo Alto Networks enterprise Network Security Platform was straightforward, thanks to clear documentation. "Palo Alto Networks Prisma Access is one of the easiest security products I've ever set up," Cardwell confirms.

The IT team quickly learned how to use the products. Cohen recalls managing the Next-Generation Firewalls and setting up Panorama before Cardwell started at Sumitovant. "I had an easy time learning the Network Security Platform from Palo Alto Networks and figuring out how things worked," she recalls. "I appreciated that because it isn't always the case when you're talking about firewalls and VPNs."

When the team had questions, they got answers from Palo Alto Networks Trustwave Technical Assistance Center (TAC) support technicians in about an hour. Ongoing support from Palo Alto Networks has ensured almost four years of trouble-free security for Sumitovant.

"The only time I ever had an issue was when I was on a mountain skiing, and I got a phone call that our backend VPN connection went down," Cardwell says. "The steps were so simple, from memory alone, I could walk my colleague through how to use it. They had never before logged into a Network Security Platform from Palo Alto Networks. Within 15 minutes, it was fixed."



BENEFITS

Reduced risk exposure drives competitiveness

Because of Palo Alto Networks innovative Network Security Platform, Sumitovant's researchers and data scientists and its sales and manufacturing teams can be creative and innovate for the biopharmaceutical industry from anywhere without exposing the company to risk. The result is that Sumitovant is more agile and competitive, accelerating its growth in drug development, science, and technology.

The company can move forward with its ambitious plans for expansion knowing its cloud everything infrastructure, from remote access to multicloud infrastructure security, is protected from sophisticated zero-day threats. When a vulnerability in the open source Apache Log4j logging service was discovered in December 2021, Palo Alto Networks immediately mitigated the problem. It automatically updated Sumitovant's Next-Generation Firewalls and blocked the cyberattacks without further intervention from the biopharma company. "The Log4j vulnerability resolution is a great metric to show that we're proactive in our security response having implemented Palo Alto Networks Next-Generation Firewalls," Cardwell says.

Sumitovant's IT team has one consistent policy in place at the global level with no policy gaps—a common cause of breaches. The team now has complete control of web traffic and has been able to deter users from visiting unsanctioned sites or applications.

Dependable and equipped to scale

Also important to the organization's leadership: Sumitovant is now equipped to scale. The IT team can bring acquired companies on faster and quickly move on to the next project. "Last year, we brought more than 400 users from one of our subsidiaries onto our network," Cardwell says. "With the Network Security Platform from Palo Alto Networks, we flipped the switch, and those new employees were securely on our network overnight. That, to me, is unheard of."

Because the Network Security Platform is dependable, Sumitovant is able to focus on its core priorities instead of worrying about a loss of downtime caused by business interruptions. The company's scientists and sales and manufacturing teams can work efficiently and be more productive. Having security products that are easy to manage and being able to get support quickly when needed allows the IT team to be nimble and accomplish more.

Strengthened compliance and regulatory benefits

Deploying the Palo Alto Networks enterprise Network Security Platform has made Sumitovant able to meet compliance requirements in a highly regulated industry. Panorama's single-pane-of-glass visibility helps prove compliance with security controls, including the Sarbanes-Oxley Act of 2002 (SOX), Japan's Financial Instruments and Exchange Law (JSOX), EU General Data Protection Regulation (GDPR), and California Privacy Act.

In addition, Sumitovant can better meet safety and quality guidelines of its pharmaceutical products, including compliance with the U.S. Food and Drug Administration's Good Manufacturing Practice (FDA GMP) regulations. Sumitovant can also show that it's meeting Identification of Medicinal Products (IDMP) standards within the International Organization for Standardization (ISO).



“ Last year, we brought more than 400 users from one of our subsidiaries onto our network. With the Network Security Platform from Palo Alto Networks, we flipped the switch, and those new employees were securely on our network overnight. That, to me, is unheard of.

— Trevor Cardwell, Senior Cloud and Network Architect, Sumitovant Biopharma

Security powers the next milestone in digital transformation

Sumitovant's partnership with Palo Alto Networks has allowed the biopharma company to focus on secure digital innovation. It can now accelerate the development of new therapies to meet unmet medical needs.

Sumitovant continues to expand its use of the Network Security Platform. The company is looking to add Palo Alto Networks Cloud Firewalls for Amazon Web Services ([Cloud NGFW for AWS](#)), available through [AWS Marketplace](#), to its security stack. It's also considering Palo Alto Networks [Enterprise Data Loss Prevention \(DLP\)](#), the industry's most comprehensive cloud-delivered service, that protects sensitive data across all networks, clouds, and users.

Sumitovant, with the help of Palo Alto Networks, is now positioned to accelerate its digital transformation and achieve its mission of improving lives for patients worldwide.

Find out more about how Palo Alto Networks' best-in-class solutions can improve networking and security for your organization. Additional information is [here](#).



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.