CASE STUDY

US Signal, primed to scale, safeguards sensitive information

US Signal, a leading provider of data center and cloud services, partners with Palo Alto Networks to rapidly deploy virtual firewalls for cloud customers and streamline its own security oversight.

paloalto® NETWORKS

IN BRIEF

Customer

US Signal Company, L.L.C.

Industry

Telecommunications and technology

Country

United States of America

Products and Services

Data center technology, cloud solutions, and managed services to businesses.

Organization Size

1-500

Website

www.ussignal.com

Challenges

- Operating multiple platforms from different vendors increases the likelihood of human error, which can lead to data breaches.
- Customers are confused about too many product choices.

Requirements

- Best-in-class security, scalability, ease of automation, and real-time updates are among critical product features.
- Must operate in a VMware vSphere ESXi™ environment.

Solution

US Signal evaluates all the major players and chooses Palo Alto Networks Next-Generation Virtual Firewalls as the top solution across all identified requirements.

Protecting against cyberthreats

Security is top of mind for US Signal, a leading provider of data center and cloud services. With eight data centers in the Midwest, the company hosts cloud solutions, provides colocation space, and delivers best-of-breed security services powered by its own secure, robust fiber network.

Customers in health care, banking, and other industries rely on US Signal's HIPAA- and PCI-compliant infrastructure to keep information safe. They consider US Signal an extension of their own IT security teams and trust the company to protect their businesses from cyberthreats, ransomware, and online attacks.

In 2020, US Signal decided to expand its cloud footprint and data protection capabilities to additional data centers. The company had seen 300 percent growth in its data center business over the previous five years. It sought to meet increasing demand for its services from customers during a period when many businesses were migrating to the cloud to support remote work.

Challenge

CRITICAL NEED FOR A CENTRALIZED SYSTEM TO SECURE INFRASTRUCTURE

At the time, US Signal was operating multiple firewall platforms from several vendors. As part of its expansion, it wanted to consolidate platforms and work with a single vendor. Doing so would mean its engineers wouldn't need to learn the ins and outs of multiple systems and would gain a centralized perspective of the company's own security infrastructure.

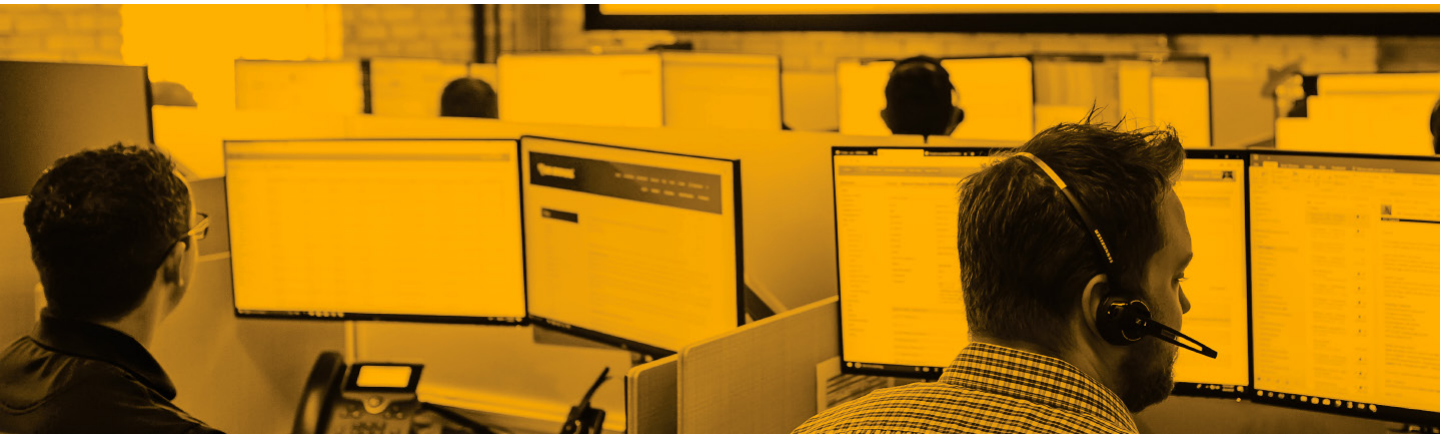
"Especially with everything in the news, and even going back as far as we all can remember, we can't afford to have any infiltration of any kind into our infrastructure that could put anyone's data at risk," says Derrin Rummelt, US Signal's Executive Vice President, Cloud Engineering.

With multiple platforms, mistakes may occur. "The more mistakes, the greater chance for a breach," explains Brandon Prim, US Signal Cloud Security Engineer.

The company also sought to take advantage of automation to further curtail the likelihood of human error, reduce overhead, and lift some of the burden on its engineers. Provisioning firewalls for customers was a cumbersome, time-consuming process. By leveraging automation, the team would be able to do more with less and expedite deployments.

In addition, US Signal saw an opportunity to increase services for its customers and aid in strengthening its security posture. "I think a lot of our customers feel the same way that we do. They want a one-stop shop," says Rummelt. "We frequently hear, 'I don't want to log into 12 different portals just to find out what's happening with my traffic.' By consolidating platforms, we help simplify the customer experience too."

> Especially with everything in the news, and even going back as far as we all can remember, we can't afford to have any infiltration of any kind into our infrastructure that could put anyone's data at risk.
>
> **— Derrin Rummelt, Executive Vice President, Cloud Engineering, US Signal**



Requirements

CAREFUL ASSESSMENT BECOMES CRITICAL WHEN THE STAKES ARE HIGH

US Signal evaluated all major security vendors, including global cybersecurity leader Palo Alto Networks.

To even be considered, a solution had to operate in a VMware ESXi™ for vSphere Bare Metal Hypervisor environment. Best-in-class security was a primary requirement since the chosen solution would protect both US Signal's infrastructure and its customer's. Scalability was equally critical in order to keep up with the company's appetite for expansion.

In addition, US Signal judged real-time updates as essential to equip the virtual firewalls with the latest security features and threat intelligence. Ease of automation was of tremendous importance, as the company deploys virtual firewalls for hundreds of customers. Licensing and price point were also key.

When comparing vendors, US Signal also scrutinized:

- Feature set
- Performance
- Throughput
- Centralized traffic logging
- Ease of management
- Access levels
- Advanced routing
- Safety instrumented system (SAS) logging
- Intrusion detection system (IDS) features
- Intrusion prevention system (IPS) features

Solution

HEAD-TO-TOE TESTING REVEALS UNDISPUTED FRONTRUNNER: PALO ALTO NETWORKS

Palo Alto Networks was clearly the best choice. When considered against competitors, it provided the highest-ranking solution across all the identified requirements and proved top in performance, automation, and security.

"We put all the vendor solutions through the test for everything we do and pitted them against each other," Prim says. "Palo Alto Networks brought the best solution holistically for us."

US Signal knew Palo Alto Networks' long-standing cybersecurity leadership position. Rather than resting on its laurels, Rummelt says, Palo Alto Networks worked hard to prove why it stands out. The company partnered with US Signal to put together a package of products and services that supported the business's desire to scale and roll out security enhancements to its customers.

US Signal chose Palo Alto Networks' industry-leading, Next-Generation Virtual VM-Series Firewalls to provide complete Zero Trust network security for both its internal IT infrastructure and as product offerings that US Signal deploys to customers. By taking advantage of Palo Alto Networks' automated provisioning and integration with Ansible® and Terraform orchestration products, US Signal deployed every virtual firewall with a full suite of cloud-delivered security services. These included GlobalProtect™, selected to safeguard mobile users. WildFire®, the advanced malware analysis engine that goes beyond traditional sandboxing, instantly preventing new, unknown file-based threats, was deemed a "no-brainer" that would later prove particularly valuable. These services work in harmony with Threat Prevention, Advanced URL Filtering, and DNS Security to secure traffic and prevent sophisticated known and unknown attacks.

> We put all the vendor solutions through the test for everything we do and pitted them against each other. Palo Alto Networks brought the best solution holistically for us.
>
> **— Brandon Prim, Cloud Security Engineer, US Signal**

Palo Alto Networks' support made deploying the firewalls and security services seamless and nondisruptive. The company provided a week-long training course and excellent documentation, including configuration templates to enable alignment with Zero Trust best practices. US Signal engineers were comfortable using the platform within a week and became experts within six months. Prim says having a single platform made it easy to deploy a template for firewalls with all necessary base settings. Zero Trust settings, feature options like App-ID™, and certificate rotations are all handled automatically.

Since Palo Alto Networks was the right choice for US Signal's own internal IT use, US Signal recognized Palo Alto Networks would also be a terrific solution for its customers. The Palo Alto Networks name carries clout, Rummelt says, and gives customers confidence their security needs will be well met.

Benefits

AUTOMATION CUTS TIME SPENT PROVISIONING FIREWALLS BY 97%

Implementing Palo Alto Networks solutions has substantially cut the time it takes US Signal to deploy a firewall for a customer, boosting internal productivity. Automation is crucial to this process. Engineers are able to orchestrate provisioning of the virtual firewalls using Ansible and Terraform. They consider a customer's specific needs, input those specifications into the platform, and Palo Alto Networks IronSkillet configuration templates generate a base firewall with all core security settings consolidated and turned up in every instance.

"Before, we'd get a customer firewall order in and build everything by hand. We reduced the initial time to deploy by handwritten rules from about three hours to an automated 20 minutes," says Rummelt. "And a lot of that time, the engineers aren't actually interacting with the platform. They provide four variables at the beginning and they can go on to other tasks, returning to a completed base firewall. So the actual time employees spend on deploying Palo Alto firewalls with all security services enabled is five minutes. Automation takes care of the rest."

"We've received positive feedback from customers because we're able to turn around orders faster," he adds.

FEATURE-PACKED VIRTUAL FIREWALL APPEALS TO CUSTOMERS, EXPEDITES PURCHASE DECISIONS

Being able to offer a single product has also reduced the time it takes for customers to make a buying decision. In fact, the only decision customers have to make is to determine how much throughput they require through the firewall; all other protection security features are delivered automatically.

"Prior to Palo Alto Networks, we had three or even four different flavors of firewalls. That's too many options. It was too difficult for customers to understand the value of each," says Rummelt. "Now, customers ask, 'Do you have a firewall product?' And we say, 'Yes, we do. It's Palo Alto Networks.' They ask,'Well, what comes with it?' And we say, 'Everything.'"

ADVANCED CLOUD SECURITY POSITIONS COMPANY TO CONTINUE TO GENERATE CUSTOMER TRUST

Palo Alto Networks enables US Signal to be a trusted security partner for its end customers. Both US Signal and its customers are able to mitigate risk and achieve compliance as they transition to the cloud thanks to a scalable platform designed to protect critical data, workloads, and applications. Customers also benefit from US Signal's outstanding support.

With Palo Alto Networks firewalls, US Signal can better segment and isolate Zero Trust demilitarized zones (DMZs) in environments. In addition, the firewalls and Palo Alto Networks App-ID™ classification technology allow US Signal to block malicious applications, as well as IP addresses and ports. As people opt for hyper-scale cloud solutions, Office 365™, and cloud applications that run on Azure®, public IP addresses change. As these applications scale up and down, it creates security holes. By leveraging dynamic lists (text files hosted on external web servers so firewalls can enforce policy) and/or specific applications, US Signal is able to help customers not leave IP addresses and ports open if they are no longer valid.

Because of its partnership with Palo Alto Networks, US Signal is able to operate more efficiently. When it comes to protecting the company's own infrastructure, engineers can log into one place and see everything.

> Prior to Palo Alto Networks, we had three or even four different flavors of firewalls. That's too many options. It was too difficult for customers to understand the value of each.
>
> **— Derrin Rummelt, Executive Vice President, Cloud Engineering, US Signal**

VIRTUAL FIREWALLS STAND THE TEST AGAINST ZERO-DAY THREAT

US Signal has also gained increased confidence in its ability to protect itself and its customers against zero-day vulnerabilities while experiencing uninterrupted operations. When the SolarWinds hack that compromised and exposed an estimated 100 companies and a dozen government agencies occurred in 2020, US Signal witnessed WildFire's impressive response time.

"Palo Alto Networks' platform stepped up to the challenge; it had already instantly blocked the SolarWinds issue. There was nothing to worry about. The firewalls were automatically set up to receive up-to-the-minute updates," Prim says. "We put the Palo Alto platform, with all security subscriptions turned up, through numerous tests and we have yet to find a scenario where the firewall was lacking. The firewall performance speaks for itself and has proven why it is an industry leader."

UNSURPASSED SECURITY SOLUTIONS PROVIDE COMPETITIVE EDGE AND ENABLE GROWTH

The quality of service that US Signal provides through its partnership with Palo Alto Networks gives the company a competitive advantage in the data center market and is leading to increased customer satisfaction and repeat business. Implementing Palo Alto Networks' best-in-breed innovations put US Signal in a stronger position to scale and meet the security needs of its customers well into the future.

Find out more about how Palo Alto Networks best-in-class virtual firewalls and cloud-delivered security solutions can help accelerate opportunities for your organization.

paloalto NETWORKS

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