CASE STUDY

Verge Health

Healthcare Risk Management Provider Secures Its SaaS Environment on AWS With Next-Generation Security Platform

VERGE™
HEALTH

> "As risk management experts handling very sensitive protected health information in a public cloud, it is incumbent upon us to provide the highest levels of security for our customers. 'Good enough' is not sufficient; we have to exceed their expectations, and with Palo Alto Networks, we are doing that."

James Lawson | Chief Solutions Officer | *Verge Health*

Industry

Healthcare

Challenge

Prevent cyberthreats from compromising PHI handled by a governance, risk and compliance application hosted on AWS.

Solution

Palo Alto Networks Next-Generation Security Platform deployed on AWS with Cloudticity integration to enable high availability.

Subscriptions

Threat Prevention, URL Filtering (PAN-DB), GlobalProtect, WildFire, Premium Support

Appliances

VM-300

Results

- Revealed threats from foreign states never before recognized
- Decreased traffic 29 percent by blocking specified regions of the world
- Reduced unnecessary connected sessions by 30 percent
- Reduced platform failover from up to 60 seconds to less than one second
- Strengthened endpoint security for staff accessing the SaaS network

Background

Founded in 2001, **Verge Health** is a leading provider of governance, risk and compliance solutions for healthcare. Verge Health's software solutions enable healthcare organizations to proactively protect and defend patients, caregivers, and frontline staff against errors, adverse events, and policy violations. With over 900 facilities and 500,000 active users, the company's Converge Platform provides hospital organizations with a cross-functional, proactive surveillance tool enabling optimal quality and safety results.

Story Summary

Verge Health™ provides healthcare organizations with a systematic approach to managing governance, risk and compliance through a SaaS-based offering hosted by AWS®. Because the company handles sensitive protected health information (PHI), it requires the highest level of network security to prevent cyberattacks from compromising its SaaS environment.

By deploying the Palo Alto Networks® Next-Generation Security Platform on AWS, Verge Health is able to intelligently prevent global bad actors from breaching its network, as well as stop cybercriminals attempting access through corporate endpoints using stolen credentials. The company also leverages a unique high availability capability in which Cloudticity™ integrates Palo Alto Networks Next-Generation Security Platform with AWS availability zones to ensure instant failover in the event of a site outage. This assures Verge Health and its customers that sensitive data and vital risk management services are safe, compliant and available 24/7.

Protecting Private Health Information in the Cloud

Protected Health Information (PHI) has become one of the most sought-after targets for cybercriminals to steal using a wide range of sophisticated and persistent schemes. Healthcare organizations that do not properly manage their risk could face dire consequences, including loss of reputation, regulatory fines and the enormous cost of information recovery. But Verge Health, a leading risk management solution provider, is out to make sure that doesn't happen.

Verge Health serves more than 900 health systems and hospitals with its Converge Platform™, a SaaS (software as a service) offering that provides a systematic approach to managing healthcare governance, risk and compliance (GRC). Verge Health runs its SaaS environment on AWS to optimize scale, flexibility and economics. Given the sensitivity of information Verge Health handles, cybersecurity is a top priority. For that, the company relies on Palo Alto Networks Next-Generation Security Platform.

Vivek Desai, Verge Health's Director of Information Security, explains: "We need to protect both our internal corporate data and our clients' PHI to ensure HIPAA compliance and minimize

"The visibility and control we get from the Palo Alto Networks platform gives both our internal team as well as our customers the comfort that Verge Health is using real intelligence to do everything possible to reduce risk and prevent targeted attacks from compromising our SaaS network."

Vivek Desai | Director of Information Security | *Verge Health*

their risk of exposure. Targeted malware and phishing attacks have really ramped up in 2017, so we apply a defense in depth strategy to keep those threats from breaching our corporate network and sidestepping into our SaaS network. Our first layer of defense is the Palo Alto Networks platform."

James Lawson, Chief Solutions Officer with Verge Health, adds: "Practically every day you hear about another hospital system or vendor that's been attacked. As risk management experts handling very sensitive protected health information in a public cloud, it is incumbent upon us to provide the highest levels of security for our customers. 'Good enough' is not sufficient; we have to exceed their expectations, and with Palo Alto Networks, we are doing that."

End-to-End Security Available 24/7

Verge Health deployed Palo Alto Networks VM-Series on AWS, which complements AWS security with unique application-level traffic control. Palo Alto Networks Next-Generation Security Platform is enabled with Threat Prevention, URL Filtering, and WildFire™ cloud-based threat analysis service, enabling Verge Health to block known and unknown cyberthreats across its SaaS environment. The company also uses GlobalProtect™ network security for endpoints as an integral part of its security posture, providing a globally secured entry point for staff logging in to the SaaS network.

Tom Fink, Vice President of Technology Services at Verge Health, comments: "We wanted a solution that could best meet our dynamic growth, and provide assurance that we can proactively monitor threats as they show up in an easy and efficient way. Palo Alto Networks checks all those boxes."

The company's critical SaaS environment also demands high availability to ensure 24/7 cybersecurity on AWS. Verge Health takes advantage of a high availability capability provided by Palo Alto Networks and Cloudticity that integrates the Palo Alto Networks platform with AWS Lambda scripting service. This unique solution achieves virtually instant failover of security monitoring and control across AWS availability zones in the event of a site outage. With Cloudticity integration, Palo Alto Networks platform services fail over seamlessly, compared to taking nearly 60 seconds using a traditional failover strategy.

"Cloudticity brought in a high degree of expertise in the Palo Alto Networks platform, as well as best practices on AWS," says Desai. "They were instrumental in marrying our GRC platform with AWS and driving our entire security posture, including HIPAA compliance."

Stops Global Bad Actors in Their Tracks

Since adopting the Palo Alto Networks platform, Verge Health has gained much deeper visibility into traffic spanning its SaaS network on AWS. What's more, the company can now act on complex threat vectors proactively – something it couldn't do before.

Desai comments: "When we put the Palo Alto Networks platform in place, we started seeing lots of threats coming from foreign states that we have no business in. So there was no reason for them to be accessing our sites. Using the geo-blocking feature on the Palo Alto Networks platform, we prevent traffic from specific regions of the world from having contact with our SaaS application and systematically remove the threat of global bad actors."

As a result, Verge Health has reduced traffic from inappropriate sources by 29 percent and reduced connected sessions on its SaaS application by 30 percent.

"These kinds of very specific metrics are illustrative of what we can do with the Palo Alto Networks platform that were very difficult with our previous solution," notes Fink. "We can assess our environment, understand activity on our SaaS network, and take steps to move our security posture where it needs to be. Then we can measure our success over time and present that information to the board to demonstrate the value of our security investments."

Secure Access From All Endpoints

A key aspect of mitigating risk internally is ensuring that only authorized staff can access the SaaS environment. Verge Health relies on GlobalProtect to secure all login attempts by developers, operations managers and others who need to interface directly with the Converge Platform. Currently, GlobalProtect users are predominately those with corporate-issued laptops; however, Verge Health has begun testing mobile devices with plans to allow a bring-your-own-device policy.

> “We can assess our environment, understand activity on our SaaS network, and take steps to move our security posture where it needs to be. Then we can measure our success over time and present that information to the board to demonstrate the value of our security investments.”

Tom Fink | Vice President of Technology Services | *Verge Health*

The company is also now implementing host information profiles as an additional layer of security for its GlobalProtect users.

“Using our defense in depth strategy, we assume that a user’s GlobalProtect credentials could be stolen,” Desai says. “So we’re using HIPs and other pre-checks embedded natively in the Palo Alto Networks platform to force access through multiple security layers. This makes it extremely difficult and unlikely for an unauthorized individual to gain access to our SaaS network using stolen credentials.”

Fink adds: “What we like about GlobalProtect is we can enable strong security very easily. Other solutions are like learning a new language, but GlobalProtect is very intuitive. And it’s simple for the users. They don’t have to navigate through page after page to get in; they just enter their login credentials as usual. We have everything locked down in the background.”

Private Patient Records Are Safe and Compliant

Taking this comprehensive defense approach to network security, Verge Health has not only solidified confidence internally; it is also positioned to provide evidence-based assurance to its customers that their private health information is safe and compliant.

Lawson points out: “Our clients are very savvy about the steps required to secure their data. Consequently, they’re more demanding of us to have the proper controls in place before they’re willing to put their medical records and private patient information in our hands. With the Palo Alto Networks platform, we can give them the assurance they need.”

Desai concludes: “The visibility and control we get from the Palo Alto Networks platform gives both our internal team as well as our customers the comfort that Verge Health is using real intelligence to do everything possible to reduce risk and prevent targeted attacks from compromising our SaaS network.”