Case Study

Leading Polish Medical Center Revitalizes Cybersecurity Through Hillstone Solutions

Hillstone next generation firewalls (NGFW), breach detection system (BDS) and network intrusion prevention system (NIPS) provide the security needed to protect client data and medical infrastructure.

Customer Profile

Customer

Dolnośląskie Centrum Rehabilitacji i Ortopedii (DCRO)

Sector

Healthcare

Location

Southwest Poland

Size

Regional medical center with 6 departments, 2 specialty clinics, 3 diagnostic labs

Challenges

Upgrade and refresh security infrastructure to ensure the safety of critical data and protect both the perimeter and internal network from attacks and malicious actors.

Requirements

- Protect patient and other critical data against theft and extraction
- Defend the perimeter and control data flows
- Safeguard the internal network against both internal and external attacks
- Secure connections to remote offices and clinics

Result

Hillstone's future-ready NGFW and BDS NDR solution provide advanced threat detection and protection across the network, with in-depth visibility, monitoring, and analysis

The Challenge

Modernizing Cybersecurity Infrastructure

Originally founded in 1902 as a hospital for patients with tuberculosis, this regional facility was reinvented 1977 to its current mission, now known as the Dolnośląskie Centrum Rehabilitacji i Ortopedii (DCRO). In addition to providing surgical and rehabilitation services for trauma and orthopedic patients, DCRO provides cardiac and neurological rehab and other assistance.

As a healthcare provider, the data security and confidentiality of patients, human resources, and accounting data – and the network as a whole – was of utmost importance to DCRO. The facility is subject Europe's GDPR regulations, which extends far beyond the requirements of the United States' HIPAA regulations. Failure to meet the GDPR requirements can result in expensive penalties.

The existing security infrastructure, however, was aging and focused primarily on perimeter protection. The DCRO IT team determined that it was time not just for a refresh, but for a complete rethinking and strategy for a more comprehensive cybersecurity architecture.

The team considered solutions from four vendors: the existing NGFW provider and three competing solutions. Specifications and capabilities were carefully compared, and proofs of concept were conducted to determine the breadth of security coverage, flexibility, ease of use, and other factors.

The Solution

Comprehensive Protection from Edge to Core

Ultimately, the DCRO team chose Hillstone's A-Series next-gen firewalls coupled with Hillstone's AI-driven network detection and response (NDR) solution. These solutions combine to deliver deep and comprehensive protection against even the most insidious and dangerous threats while remaining easy to use, easy to manage, and under budget.

A-Series NGFWs offer high-security performance, broad-based threat prevention and detection, and intelligent policy definition and operation. The foundation for the A-Series NGFW is an all-new hardware platform that provides market-leading application-layer performance to meet the demands of today's threat landscape. Automated and efficient smart policy capabilities span the entire policy lifecycle – including deployment, management, optimization and operation – to simplify security operations.

In addition, the A-Series NGFW is future-ready to meet changing needs in the years ahead. Local storage for logs and other data can be expanded, for example, and a user-friendly interface allows integration of third-party products for additional security features if needed.

A-Series NGFWs are deployed in a high-availability pair to provide continuous operation even during disruptive events. In addition, the A-Series provides SSL VPN for secure connectivity for remote employees, doctors' offices, clinics, and other facilities.

Overall, the team found the NGFW to be far more flexible and performant than the previous devices, with more functionality and ease of management. The existing firewall policies were easily migrated to the new NGFW via a rewrite policy.

Hillstone's NIPS provides advanced network intrusion detection and prevention features that analyze, detect, and block advanced threats in real-time. Based on AI and machine learning algorithms, NIPS provides intelligent, layered cybersecurity that operates with the Hillstone A-Series to block potential threats.

Hillstone's BDS extends the hospital's security deep within the network, where it intelligently detects and mitigates multi-stage, multi-layer threats like ransomware and botnets. BDS utilizes machine learning, advanced analytics, and rules-based identification to continuously detect and act upon suspicious or anomalous activities inside the network infrastructure.

Both BDS and NIPS interoperate with the NGFW in one platform, providing intelligence that allows automatic fine-tuning of policies and protective measures to respond to the threat landscape both accurately and rapidly. In addition, the intelligence gained from all three solutions allows the DCRO IT team to monitor for and respond to threats manually as needed.

After deployment, Hillstone solutions detected several vulnerabilities within the network, allowing the IT team to quickly remediate them. In addition, Hillstone solutions identified a number of older, insecure software versions on network elements that were then upgraded by their respective vendors.

Hillstone's solutions are a part of the company's integrative cyber security strategy for digital transformation, which brings coverage, control, and consolidation for comprehensive cyber security. It eliminates gaps in protection that can put an enterprise at risk, while dramatically reducing layers of complexity and cost.

> **"The Hillstone solution allows us to think calmly about the further development of our company by effectively securing our patients' data."**
>
> Waldemar Wiśniewski
> **Head of the IT Department for DCRO**

The Conclusion

A Revitalized, Comprehensive Security Solution

The new, integrated Hillstone solution has completely overhauled and refreshed DCRO's security infrastructure, providing comprehensive security from edge to core. The solutions work together to quickly block potential threats, and expand visibility and control, allowing staff to easily visualize and analyze their security posture.

Patient records and other sensitive information are secured and compliant with GDPR regulations, and DCRO can also monitor and manage the security of their clients' networks – reducing cost and increasing efficiency.

"Thanks to the Hillstone technology, our security measures have finally entered the 21st century and ensure that data security is at a very high level," said Waldemar Wiśniewski, head of the IT department for DCRO. "The Hillstone solution allows us to think calmly about the further development of our company by effectively securing our patients' data."

About Hillstone Networks

Hillstone Networks is a leader in cybersecurity, delivering both depth and breadth of protection to companies of all sizes, from edge to cloud, and across any workload. Hillstone Networks' Integrative Cyber Security approach brings coverage, control, and consolidation to more than 26,000 enterprises worldwide.

Hillstone Networks is uniquely positioned with a platform that's future-proof to enable digital transformation and business continuity. For more information and to find your Integrative Cybersecurity solution, please visit www.hillstonenet.com

Learn more about Hillstone products mentioned in this case study

Hillstone Next Generation Firewall (NGFW)

Hillstone Breach Detection System (BDS)

Hillstone Security Management (HSM) ⇨

Read about Hillstone solutions

Cloud Workload Protection (CWPP) ⇨

Extended Detection & Response (XDR) ⇨

Zero-Trust Network Access (ZTNA) ⇨

Secure SD-WAN ⇨

Micro-segmentation ⇨

Network Detection & Response (NDR) ⇨

Gartner
Peer Insights
Customers'
Choice 2023
™

Hillstone
NETWORKS