FORTINET

CASE STUDY

FortiGuard Incident Response Helps Large Planned Community Recover from Ransomware

When seniors in Southern California want their retirement years to be active and full, they move to Laguna Woods Village. The condominium-planned community is home to about 18,000 residents ages 55 and up. Laguna Woods Village offers something for everyone, from golf courses and swimming pools to horseback riding, archery, and bridge.

"Our community has myriad ways to keep busy in retirement," explains Chuck Holland, CIO of Village Management Services (VMS), the organization responsible for all the community's services and common areas. "Our clubhouses host a wide array of clubs and activities, including everything from painting, weaving, pottery, and woodworking to classes from local college professors. Many people get inspired later in life to discover new talents they did not realize they had."

VMS enables residents to focus on such pursuits by taking on many of the day-to-day responsibilities of property ownership. "We handle all the maintenance, take care of the common areas, and provide recreational activities, transportation systems, security, cable TV, and internet services," Holland says. "We are responsible for about 2,500 structures, as well as one of the largest privately owned fiber optic networks in Southern California."

Keeping Seniors Secure

Cybersecurity has always been important to VMS management because protecting residents is crucial to the Laguna Woods Village brand. Still, in the mid-2010s, as Holland pushed to modernize the organization's technology infrastructure, he sometimes found himself bumping against budget restrictions and other concerns.

"It was always my intent to lift and shift our data center into the cloud," he says. "But we had limited resources for technology investments, and some decision-makers felt that keeping everything on-premises gave the IT team more control over resident safety."

In 2016, VMS engaged Irvine, California–based AirGap Labs to assist with networking and security. AirGap provides advisory and managed services in networking, security, and cloud transformation. "We are an engineering-first company that helps customers develop solutions to their technology problems in a vendor-agnostic way," says Milton Yeo, principal consultant with AirGap Labs. The firm is a Fortinet Engage Preferred Services Partner. "We entered this partnership because Fortinet has an end-to-end suite of products on the security side that works well for many of our clients."

Laguna Woods Village®

"I am so thankful that Fortinet and AirGap Labs are out there fighting the good fight against the bad actors. We have great security partners, and we are looking forward to expanding our security footprint as new Fortinet solutions become available."

Chuck Holland
CIO
Village Management Services (VMS), Laguna Woods Village

Details

Customer: Village Management Services (VMS), Laguna Woods Village

Industry: Construction/Real Estate

Headquarters: Laguna Woods, California

Business Impact

- Rapid response to major security incident locked down attacker's access within 24 hours
- Efficient and effective development of new, modern security infrastructure

AirGap Labs started working with VMS by rolling out FortiGate Next-Generation Firewalls (NGFWs), FortiSwitch secure Ethernet switches, and FortiAP access points in certain areas of the VMS network. “We liked that Fortinet provided a complete solution with single-pane-of-glass visibility to our infrastructure,” Holland says. Still, progress toward standardizing on Fortinet was slow until VMS experienced its security worst-case scenario in October 2020.

The Worst Case Strikes

“Coming off a wonderful weekend with my family, I got a phone call at 5 o’clock on Monday morning that we had been hit with a ransomware attack,” Holland remembers. “In the past, we had experienced isolated attacks on individual parts of the network. But these bad actors were sophisticated. They had penetrated our network weeks earlier through an email attachment, then sniffed out all our important assets before executing the malware. They shut down every system we had on-site.”

As soon as VMS discovered the problem, Holland and AirGap Labs engaged FortiGuard Incident Response (IR) Services to understand what had happened and how to prevent similar attacks in the future. “My colleagues and I were in over our heads,” Holland says. “We needed to stop the bleeding and then start recovering the VMS environment as soon as possible. Thankfully, we had Fortinet to walk us through the process.”

AirGap Labs coordinated the on-site response, working with the FortiGuard Incident Response team, the FBI, the U.S. Department of Homeland Security, and the Orange County Cybersecurity Awareness group. “We felt a sense of relief and confidence that we had the right people and the right resources to get our community back up and running,” Holland reports.

AirGap Labs immediately deployed the FortiEDR endpoint detection and response solution for its lightweight endpoint agent and complete endpoint coverage, encompassing both current and legacy operating systems and IoT devices. The FortiGuard IR team used FortiEDR and the NGFWs, along with any other current security controls the customer had, to determine exactly what had happened. Within a few hours of the attack, the team had identified the bad actor’s locations on the network and built a containment and remediation strategy with the customer. Then, they dug into how the attacker had entered the network and what post-exploitation activity had occurred and began preparing recommendations for VMS security upgrades.

At the same time, the teams were working to restore affected systems. Ultimately, VMS decided to rebuild its technology infrastructure from scratch. “We might pay the ransom to get our data back and then be hit again five minutes later,” Holland says. “So, we decided to burn everything to the ground. Every PC, every smartphone, every tablet computer, every server—we scrapped everything we had and started over.”

Lemons Produce Lemonade

The process of rebuilding was long and intense, and Holland was glad to have Fortinet and AirGap Labs by his side. VMS started by restoring its email, phones, and core financial systems. Even that took a couple of weeks. However, Holland says, “It would have taken a lot longer and cost a lot more money if we tried to do it ourselves.

“FortiGuard Incident Response and AirGap Labs were class-act professionals all the way,” he adds. “There were times when I was ready to pull my hair out, but they responded at whatever weird hours we needed them and always kept their cool.”

Business Impact (cont.)

- 24×7 monitoring and alerts enabled the team to thwart several attempted cyberattacks
- Easy-to-use systems simplify security management and training of staff members
- Improved total cost of ownership across the security infrastructure

Solutions

- FortiGate Next-Generation Firewall
- FortiSwitch
- FortiAP
- FortiSandbox
- FortiNAC
- FortiDeceptor
- FortiEDR
- FortiAuthenticator
- FortiToken
- FortiClient
- FortiMail
- FortiWeb
- FortiAnalyzer

“FortiGuard Incident Response and AirGap Labs were class-act professionals all the way. There were times when I was ready to pull my hair out, but they responded at whatever weird hours we needed them and always kept their cool.”

Chuck Holland
CIO
Village Management Services (VMS), Laguna Woods Village

Soon after the incident, Holland and senior FortiGuard IR team members met with VMS's board of directors to explain why their legacy security architecture had been breached. "We made it clear that there are a lot of different types of technologies out there, and staying ahead of threats is a cat-and-mouse game," Holland says. "We need multiple layers of protection, and we need to continue to fortify our network over time to stay ahead of the latest adversarial techniques.

"When we were compromised, it became evident that VMS security was ill-prepared," he continues. The silver lining of the ransomware attack was that security ranked higher on the organization's priority list. "Instead of being in the backseat, security has become the driving factor in everything we do with technology. The risks did not feel as real until we were attacked. Now we understand that if we do not have the appropriate front-line solutions securing our environment, we will no longer have an environment."

In addition to committing to strengthen its security architecture, VMS decided to centralize IT management and move its sensitive information to the cloud. Some workflows require on-site servers, such as those supporting the community's irrigation system. However, the company's financial and other core capabilities have moved into a cloud-based enterprise resource planning system, while other data and applications are shifting to Microsoft Azure and Amazon Web Services environments. FortiGate NGFW virtual machines (VMs) protect these assets in the cloud.

Standardized on the Security Fabric

In fact, Fortinet's presence has expanded dramatically throughout the VMS network. "Before the ransomware incident, we had a game-plan for going end to end with Fortinet, but we had not figured out how to pay for it," Holland says. "The ransomware attack provided justification for us to execute on that plan."

FortiGate NGFWs protect VMS's entire network perimeter and provide internal segmentation. "We have segmented based on function," Holland says. "We have a camera VLAN [virtual local area network]. We have server VLANs. Anything critical or sensitive gets a network segment. If we were to experience another attack, this architecture would keep the bad actor from moving laterally through our network." The FortiGuard Unified Threat Protection Bundle includes intrusion prevention system, web security, content security, and other capabilities for the NGFWs.

Services

- FortiGuard Incident Response Services
- FortiGuard AI-Powered Security Services
- FortiGuard Unified Threat Protection Bundle

"The simple and unified management across the Fortinet infrastructure is absolutely key. With our legacy systems, the learning curve was steep. The Fortinet applications are intuitive and modern, and they make it much easier to train staff members. Overall, the Fortinet solutions are fantastic."

Chuck Holland
CIO
Village Management Services (VMS), Laguna Woods Village

FortiWeb web application firewall defends applications and APIs running on VMs against a wide array of prospective attacks. The FortiDeceptor tool also sits at the network edge, mimicking some of VMS's outward-facing services. "By leveraging Fortinet's broad array of intelligence gathering and security mechanisms, we proactively stay ahead of malicious actors and equip VMS with the tools necessary to handle security incidents in an ever-evolving threat landscape," says AirGap Labs' Yeo.

At the endpoints, FortiClient provides virtual private network access and traditional antivirus scanning, while FortiEDR monitors every VMS endpoint looking to identify and stop breaches in real time. FortiMail scans all incoming messages to prevent the type of phishing scam that led to the ransomware debacle. And any potential threats the other Fortinet solutions detect are automatically sent to the FortiSandbox for deeper analysis in isolation from the rest of the network for protection from zero-day and unknown threats.

The FortiNAC network access control solution, FortiAuthenticator identity and access management services, and the FortiToken multifactor authentication solution manage and monitor user and device access to the network. And VMS has also fully standardized on Fortinet internally, converting all its legacy switches and wireless access points to FortiSwitch and FortiAP devices.

AirGap Labs manages the infrastructure for VMS, a role simplified by the tight integration of solutions across the Fortinet Security Fabric. FortiAnalyzer played a pivotal role in the integrated security solution by centralizing and analyzing security logs from the entire Fortinet suite. Its advanced event correlation and threat prioritization capabilities, powered by a custom playbook, significantly enhanced threat detection and response efficiency. “We worked closely with Fortinet IR and FortiEDR teams in tandem with VMS to design and implement the most optimal security architecture for their IT environment. AirGap Labs and Fortinet collaborated to develop customized playbooks that we paired with information gathered from VMS’ systems to quickly respond to all potential threats,” Yeo says.

Fortinet and AirGap Labs Fighting the Good Fight

AirGap Labs and his team “have a good handle on VMS’s security,” he says. “With AirGap Labs keeping vigil, we know that we will be notified anytime there is suspicious activity on our network. Our security systems are alerting us 24 hours a day, seven days a week, and we have thwarted several attempts by attackers to compromise our systems.”

The Fortinet solutions’ ease of use improves both teams’ efficiency in monitoring and responding to threats. “The simplicity of management across the Fortinet infrastructure is absolutely key,” Holland says. “With our legacy systems’ command line interface, the learning curve was steep. The Fortinet applications are more intuitive and modern, and they make it much easier to train staff members to support them. They are also saving us money over our legacy network and security systems. Overall, the Fortinet solutions are fantastic.”

Holland adds, “We used to always hear about security situations at other organizations, and it seemed like it could not happen to us, but it did. The cost to our organization and our community has eclipsed what it would have cost to build a stronger security infrastructure in the first place. We spent a considerable amount of dollars on recovery, which we could have avoided if we had made the modest investment in dollars each year on security.

“I am so thankful that Fortinet and AirGap Labs are out there fighting the good fight against the bad actors,” he concludes. “It takes an army of people to secure our systems. It is nice to know that we have great security partners, and we are looking forward to expanding our security footprint as new Fortinet solutions become available.”

FORTINET

www.fortinet.com

January 20, 2024 2:46 AM

2529400-0-0-EN