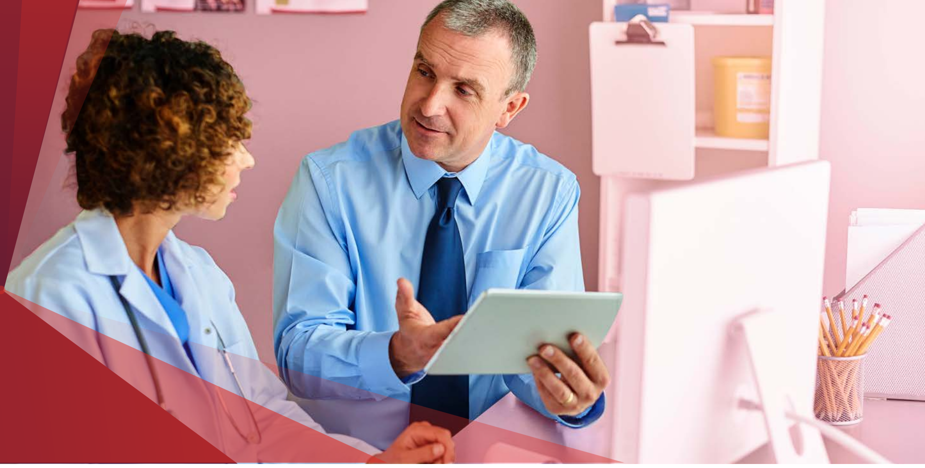
FORTINET



CASE STUDY

Healthcare Company Finds Comfort in Enterprise-level Network Security

SEASONS HOSPICE & PALLIATIVE CARE

As Seasons Healthcare Management expanded its geographic reach, the provider of end-of-life healthcare services needed a streamlined approach to securing its network. It turned to Fortinet, largely because of the tight integration and efficient management across the solutions in the Fortinet Security Fabric. Seasons now uses a FortiGate next-generation firewall (NGFW) and FortiAP access point in each of its locations across the United States. Its centralized network operations center (NOC) manages the network infrastructure from a single pane of glass, reducing resource consumption and saving money. Most important, the Fortinet solutions enhance the security of the company's network, helping Seasons protect its vulnerable patient population.

Protecting Patient Health and Data

For the past 23 years, Rosemont, Illinois-based Seasons Healthcare Management has supported patients at the end of life. "Our company has grown organically and our patient care has evolved over the years," explains Sonu Singh, vice president of IT and national security officer. The company originally formed to provide hospice care. Since then, it has expanded to also provide psycho-social support services, including music therapy and pet therapy. "We do all we can to make our patients' end-of-life moments comfortable and to support their loved ones on this very tough journey."

Seasons staff care for patients in nursing homes or in their family homes. In doing so, they leverage a range of sensitive information about patients' needs, medical history, and care options. Protecting this data is crucial. "For patients at the end stage of their lives, trust is vital in their relationships with their caregivers," Singh explains. "If their data were stolen, they would have no energy or resources to remedy the situation. Our promise to our patients is not just to provide care, but also to properly safeguard the information they are confiding in us."

In addition, the organization must comply with the Health Insurance Portability and Accountability Act (HIPAA) and state data security requirements. "If we were to lose patient data, we might face a multimillion-dollar fine or even lose our license," Singh says. "Security for our data and systems is imperative to our business."

"Maintaining our promise that patients can trust us with their data has supported our ability to grow rapidly over the past 10 years."

– Sonu Singh, VP, IT, and National Security Officer, Seasons Healthcare Management

Details

Customer: Seasons Healthcare Management

Industry: Healthcare

Location: Rosemont, Illinois

Business Impact

- Enhanced the Seasons brand by building trust with vulnerable patients
- Facilitated rapid expansion over 10 years
- Streamlined security management throughout IT network
- Reduced spending on network management resources

A Security Solution To Support Healthy Growth

For its first decade, the company was small and localized, and its digital security consisted of routing all network traffic through the data center's perimeter firewalls. However, it soon began expanding geographically to serve patients throughout the United States. The need for a new approach to information security became clear. "We would open an office in Boston, and then an office in California shortly afterward," Singh says. "We were struggling to manage security across those distances."

Singh evaluated the company's networking options. For performance and cost reasons, he did not want to route all internet traffic from every location through the data center, but every location required enterprise-level security. Fortinet offered a solution, which customers today will recognize as Fortinet software-defined wide-area networking (SD-WAN).

Seasons' distributed security infrastructure includes a FortiGate edge firewall at each of its locations. The edge firewalls inspect all incoming and outgoing traffic for security threats, enforce security policies, and perform all the necessary checks. To ensure appropriate quality-of-service levels for critical applications, the built-in SD-WAN function in each FortiGate NGFW performs intelligent application steering across multiple internet links. It routes internal network traffic to a private multiprotocol label switching (MPLS) connection, while sending internet traffic over a less-expensive cable internet connection. The Fortinet Secure SD-WAN solution also supports network failover and recovery should there be a disruption in any of the site's internet connections.

"The FortiGate devices were key to our strategy because they did everything we needed, in one box," Singh says. "We could not have managed different devices in every office for intrusion detection system [IDS], intrusion prevention system [IPS], application control, and load balancing—with everything configured differently. Fortinet provided consistency for our security nationwide and a single pane of glass for management by our central security team."

Solutions

- FortiGate
- FortiAP
- FortiManager
- FortiSIEM

> *"If you are not properly safeguarding yourself, you are inviting unwanted activity. To be a good member of the security community, everyone needs to do their part right. That is what Fortinet enables us to do."*
>
> – *Sonu Singh, VP, IT, and National Security Officer, Seasons Healthcare Management*

The company also rolled out FortiAP access points (APs) to provide secure wireless connectivity to each of the company's dispersed locations. Singh is satisfied with the APs, and he sees tremendous value in consolidating multiple security solutions with a single solution provider. "The fewer vendors, the less finger-pointing when there is a problem," he says. "In addition, I really like the tight integration between the FortiAP devices and the FortiGate firewalls. The FortiGate devices have a FortiAP controller built in, so we can control and configure the APs natively through the NGFWs, which streamlines management across our different locations."

Efficient, Enterprise-grade Network Protection

Since deployment of the Fortinet solutions, Seasons has expanded to encompass 19 states across the country. Each is protected by a Fortinet unified threat management (UTM) solution. "There is not a single feature in the FortiGate that we are not using," Singh says. "IDS, IPS, and application control are all crucial. The integration with the FortiGuard Labs threat intelligence service is essential, too. There have been many instances where I have read about a zero-day vulnerability and I have gone into the NGFWs to make sure we are covered, only to find that the threat is already in the signature list. In fact, over the past decade, there has not been one time that I came across published information about a threat and the signature was not recognized by the FortiGate devices."

Seasons outsources its NOC to a third party. The NOC team uses FortiManager software to monitor security policies and ensure they are applied consistently companywide. The NOC also uses FortiSIEM, the security information and event management (SIEM) solution from Fortinet. "FortiSIEM pulls in all of the security events from across the network and correlates them," Singh explains. "It provides a single pane for viewing security alerts, with less noise. We no longer have to spend resources on the basic groundwork. Now, pertinent events bubble up to the surface, and we have actionable information that can be used to triage the critical alerts."

With the Fortinet Security Fabric solution streamlining security management, Seasons has reduced the cost of its NOC services. “When we signed up with the NOC, our provider asked how many different technologies we were using,” Singh says. “Instead of having different solutions for firewall, IPS, IDS, application control, and wireless access points, we have one integrated set of technologies for them to support. They do not need staff with expertise in five different solutions. If there is an incident, the response is accelerated because the same engineer has expertise in all the Fortinet solutions. The operational efficiency this brings the NOC has also reduced our overall expenditure.”

Within the next few months, Seasons plans to further streamline its security infrastructure by shifting to FortiSwitch devices. In addition to their tight Security Fabric integration, Singh likes the way FortiSwitch devices dynamically control access to resources. “Currently, our switching fabric is a virtual local-area network [VLAN], and it provides access based on device characteristics, such as which port is connected where,” he says. “With the FortiSwitch solution, resource access is controlled dynamically through Active Directory [AD]. If users change roles in the company, their grouping in AD changes appropriately, so the FortiGate devices automatically change which network segments they have access to.”

Security That Patients Can Trust

“Without a doubt, our entire network is much more secure, thanks to the Fortinet solutions,” Singh says. “Maintaining our promise to patients, that they can trust us with their data, has supported our ability to grow rapidly over the past 10 years.”

Singh also believes the company’s strong security infrastructure has benefited the broader healthcare community. “I see doing your part in security as similar to a community watch,” he adds. “If you are not properly safeguarding yourself, you are inviting unwanted activity. There will always be attackers trying to find and exploit opportunities. If they are successful once, they will be looking for more opportunities. To be a good member of the security community, everyone needs to do their part right. That is what Fortinet enables us to do.”

www.fortinet.com