CASE STUDY

Electronic Health Records Hosting Provider Uses Fortinet to Boost Performance and Reliability While Cutting Costs

Regional hospitals with limited resources often want to focus the resources they have on patient care rather than technology management, and Tegria helps them do just that. Tegria offers healthcare providers access to leading technology platforms without the hassle of deploying, integrating, or operating those systems. The company's cloud hosting business specializes in providing remote access to the MEDITECH electronic health records (EHR) system.

"We host the EHR system for hospitals across the United States," explains Jeff Taylor, supervisor of network engineering for Tegria cloud hosting. "We have three data centers spread across the country that host MEDITECH."

Keeping the MEDITECH environment secure is business-critical for Tegria. Customers do not typically focus on cybersecurity when selecting a service provider, but a significant breach or loss of customer data would be catastrophic.

"Most hospitals make decisions about hosting engagements based primarily on uptime and cost," Taylor says. "But our track record of never having any of our environments affected by ransomware, even when our customers have been hit, is definitely a selling point for Tegria."

Iterative Journey Toward Efficient Hosting

The Tegria hosting infrastructure has been through a few iterations in the quest to provide the performance, reliability, and security customers need. Isolating customer environments within the data centers has long been a key security objective. Initially, the company hosted different hospitals' MEDITECH systems on the same hardware without much separation between customer environments. Then, Taylor's team built out virtual domains (VDOMs) within the FortiGate Next-Generation Firewalls (NGFWs) in each Tegria data center. This approach provided better separation of customer networks, but it was not as efficient or effective as the team wanted.

"The FortiGates have performed really well for the past six years," Taylor reports. "They have done a very good job of keeping our environment protected, and they have been reliable." Still, the cumbersome day-to-day management led Taylor's team to look for another solution. They decided to rearchitect their environment and use virtual firewalls to build a fully separate MEDITECH environment for each hospital.

"At the time, if we had to do a firmware update, we had to coordinate with every customer on that piece of hardware," Taylor says. "But customer-specific virtual firewalls would enable us to manage updates one customer at a time. If one customer had an issue, we could update everybody else and get back to them

Tegria

"The VM solution enables us to scale our costs to meet customer needs. Rather than buy an appliance that is big enough to handle the traffic growth we expect, we can just buy VMs as needed."

Jeff Taylor
Supervisor of Network Engineering,
Tegria Cloud Hosting

Details

Customer: Tegria

Industry: Healthcare

Location: Madison, Wisconsin

Business Impact

- Streamlined failover so customers do not even notice issues with circuits
- Faster resolution of connectivity issues with customer circuits
- Improved disaster recovery through easy restores to a remote data center

whenever they were ready. We knew that would give us a lot more flexibility in managing the environment."

As Tegria planned its new architecture, Fortinet was the obvious choice for the virtual firewalls "because of our success in the past with the physical FortiGates," Taylor says. "The track record and familiarity were there. Because the virtual FortiGates are the same vendor and same basic product as our physical firewalls, they are more efficient for our staff to manage. Those were strong reasons not to shop around."

FortiGate Virtual NGFWs Give Each Customer a Private Cloud

Over the course of a couple of years, the hosting provider moved customers' MEDITECH instances into virtual environments, each protected with a high-availability (HA) pair of FortiGate virtual NGFWs. "Essentially, each customer has its own private cloud," Taylor says. "The networks we use for hosted services live on the virtual firewalls. That has simplified our configuration, in addition to improving customer isolation."

Most of Tegria's 40+ customer instances of MEDITECH have multiple virtual local area networks (VLANs) coming into their virtual NGFWs. In addition to the MEDITECH internal network, Tegria provides "a DMZ [demilitarized zone], where the hospital's external-facing, internet-connected applications live," Taylor says. "We also provide a shared-services DMZ that contains certain utility servers for monitoring, backups, and patching connections. And then we have a connection for services that are shared among multiple customers, which also comes into the virtual FortiGates."

The customers' FortiGate firewalls include the FortiGuard AI-Powered Security Services Unified Threat Protection (UTP) Bundle, and they leverage the package's antivirus, URL filtering, and application control capabilities. "Our configuration is pretty cookie-cutter for the hospitals," Taylor says. "It gets deployed automatically. And we tell them: This is your own environment, and your traffic is the only traffic that is going to get through your firewalls."

A Big Win with SD-WAN

Customers have connectivity options, but most are standardized on one dedicated multiprotocol label switching (MPLS) circuit and one dedicated broadband circuit. Within each customer site, Tegria installs and manages an HA pair of physical FortiGate NGFWs, which use Fortinet Secure SD-WAN to manage the connections back to the Tegria data center.

"We are using SD-WAN to balance and failover traffic between the MPLS circuit and internet backup," Taylor says. "But the SD-WAN gives us the flexibility to have two separate internet circuits, without the MPLS, if the customer wants. Fortinet Secure SD-WAN does not care what medium it is routing traffic across. We give it the interfaces, and it figures out the best path."

Fortinet Secure SD-WAN has also proven more stable than the dynamic routing Tegria used previously for customer connectivity. "If a circuit is bouncing up and down, with dynamic routing, that link goes up and down and up and down unless you manually intervene," Taylor points out. "When we would have that flapping interface in our legacy environment, we would hear about it from customers. With SD-WAN, we can tell the FortiGate that a circuit must be solid for 60 seconds before it goes back into service. The fact that no one is complaining anymore is remarkable."

Business Impact (cont.)

- Performance adequate for latency-sensitive electronic health record system
- Reduced total cost of ownership and increased business agility
- Faster threat detection and response due to improvements in network visibility
- Less staff time required for day-to-day management of customer networks
- New staff and IT professionals in other departments can get up to speed very quickly

Solutions

- FortiGate Next-Generation Firewall
- FortiGate VM
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiEDR

Services

- FortiGuard AI-Powered Security Services Unified Threat Protection Bundle

"The local logs in the GUI break out information logically and make it simple to drill down into what you need. This visibility reduces our time to detect and respond to any threats to our customers' environments."

Jeff Taylor
Supervisor of Network Engineering,
Tegria Cloud Hosting

"We have had customers failover from one circuit to the other without even noticing because of how the SD-WAN is directing traffic," he adds. "The circuit goes down, and the customer keeps working. That has been a great experience."

Streamlined Management and Improved Visibility

Taylor and his team save substantial time by managing all of Tegria's NGFWs, both physical and virtual, through a single interface. "The new architecture has simplified everything so that network changes do not take nearly as long," Taylor says. "Rather than running sub-interfaces for various customer VDOMs, we give each customer network a VLAN with its own interface. That is more logical and straightforward from a management standpoint than hopping through different VDOM sub-interfaces. It makes the VMware configuration easier, too. Instead of configuring a port group with multiple VLANs in it, we just assign a port group to each interface on the virtual FortiGate."

Plus, he adds, the ability to take snapshots before making changes on the virtual NGFWs means his team can undo changes if an issue arises. "I love the virtual FortiGate firewalls," Taylor says. "If we take snapshots and make changes that don't work, we can quickly roll them back even as we are remotely managing the data centers. That is huge."

The FortiGate graphical user interface (GUI) further simplifies day-to-day network management. "The GUI is very easy to navigate," Taylor says. "We have had some acquisitions recently, and even people coming in who do not have experience with Fortinet products can get up to speed very quickly. If you know what you want to do, it is simple to figure out how to do it in Fortinet's interface."

In addition, the FortiGate command-line interface (CLI) "is laid out to match up well with the GUI," Taylor adds. "I like that I can go into the GUI and say, 'Edit in CLI,' and get the CLI config for that specific setting. It makes automating mass configuration changes a lot easier and is really helpful day to day."

Visibility is another key benefit for firewall management. "The local logs in the GUI break out information logically and make it simple to drill down into what you need," Taylor says. "I have people on the server side who have no familiarity with Fortinet at all. They can look at those logs and see what is being blocked. This level of visibility reduces our time to detect and respond to any threats to our customers' environments, and it enables other teams outside of security to troubleshoot issues. That improves our efficiency in getting connectivity issues resolved."

Taylor can see within the FortiGate NGFW interface how effectively the Tegria infrastructure is protecting customers' environments. "We have had several instances where the FortiGates have blocked threats, and we have identified and remediated issues," he says. "The threat protection in the virtual firewalls is definitely working."

Better Reliability and Performance at a Lower Cost

Reliability and performance, two key criteria for customer satisfaction, have also been excellent with the new infrastructure. "If a customer has problems accessing their EHR system, Tegria is going to have problems," Taylor says. "Uptime is a big deal, and the FortiGates have been great. Firmware updates are a nonissue. Failover works perfectly. And the high availability of the virtual firewalls has been awesome. The virtual firewalls have been as stable as our physical FortiGate firewalls."

Moreover, in the event of a disaster, the virtual FortiGate NGFWs would enable Tegria to spin up impacted customer networks in a different data center. "Having a virtual firewall means we can pick that up and do a restore in a remote location," Taylor says. "Nothing much will be different for the customer. We may have to change a public IP address, but by and large, it will be easy."

Throughput is crucial for Tegria's networks as well. "MEDITECH is a latency-sensitive application, which is why we keep an MPLS circuit for most customers," Taylor says. "We have had to restrict bandwidth on our patching and backup server to avoid overwhelming the CPUs. But the virtual firewalls have been rock-solid and passing all our traffic, with room to spare, when we are not in the middle of updates or backups."

Surprisingly, considering the many other benefits the FortiGate virtual machines (VMs) are delivering, this infrastructure has also reduced Tegria's total cost of ownership. "The VM solution is less expensive than expanding our data center with physical firewalls and adding VDOM licenses," Taylor says. "That makes us more agile and enables us to scale our costs to meet customer needs. Rather than buy an appliance that is big enough to handle the traffic growth we expect over the next several years, we can just buy VMs as needed. That is good for the bottom line."

Now, Tegria is considering rolling out the FortiAI-powered FortiManager management solution across its environment. “So far, we are liking FortiManager a lot,” Taylor says. The company is also expanding its use of Fortinet solutions in the small regional hospitals whose internal networks Tegria manages. “We have deployed some FortiSwitch secure Ethernet switches along with FortiGates for their core network connectivity, and we are rolling out the FortiEDR endpoint detection and response solution there as well. As we have success at those hospitals, we may continue to expand our use of Fortinet solutions.”

All in all, he concludes, “Our relationship with Fortinet is a partnership. We have been very happy with all the Fortinet products we have deployed over the past several years.”

August 22, 2024 2:10 AM / 2842155-0-0-EN