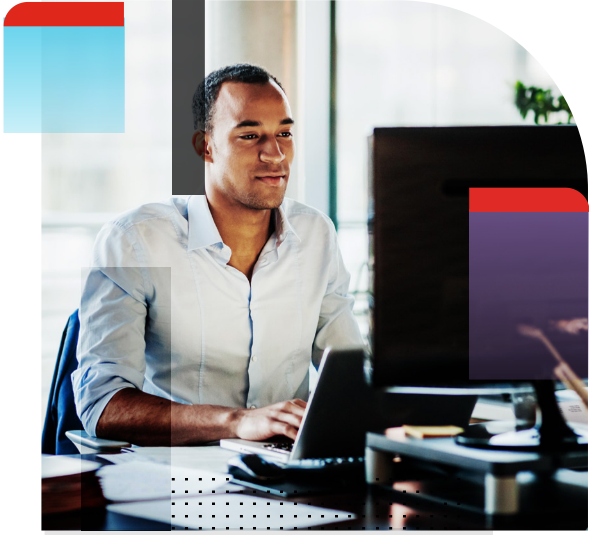
CASE STUDY

IT Solutions Provider Stops Massive Ransomware Attack with Next-generation Firewall



In just a decade, this organization has grown from a small managed application provider to a major cloud hosting and services company, offering a comprehensive selection of IT services including its own Voice-over-IP (VoIP) solution.

Falling Victim to a Breach

The company originally deployed one of the largest firewalls available from a leading network vendor to manage 30,000 email boxes and support over 50,000 websites across its infrastructure. The environment spanned 5,000 virtual machines and 300 physical servers in two data centers.

However, it wasn't enough protection: Out of the blue, the data centers were crippled by a massive ransomware attack. 4,000 access points were blocked with CryptoLocker ransomware, and horrifyingly, over 14,000 of its clients' users were locked out for three days or more.

The chief technology officer (CTO) recalls the nightmarish situation, "When the attackers breached our systems, it was devastating because they were able to gain access to my credentials. At this point, they had virtually complete control to deploy the ransomware. We received over 20,000 support calls in a two-day period, and some of the end-users were blocked for as long as five days."

Fortinet to the Rescue

Luckily, one of the company's employees brought in a FortiGate next-generation firewall (NGFW) from home to see if it could assist. While the model was designed for small businesses, the security team decided to insert the device in front of the legacy firewall. "Desperate times call for desperate measures, and this was somewhat like standing 'David' in front of 'Goliath,' but to our utter delight, the FortiGate NGFW was able to deliver the necessary intrusion protection, antivirus, and web-content filtering capabilities that we urgently needed to secure our entire network and regain control," the CTO recounts.

The company immediately engaged with Fortinet and purchased a Fortinet FortiGate enterprise NGFW, along with the FortiAnalyzer logging and reporting solution, to replace the incumbent firewall that had failed the company.

"Despite having a very complex environment, we made the switch to the FortiGate NGFW in 30 minutes; it was amazingly straightforward," enthuses the CTO. "We didn't have to rearchitect any aspect of our environment."

The security team immediately implemented the FortiGate geolocation blocking capability to reduce risk from known nation-state aggressors; multi-factor authentication for user protection; as well as antivirus functions and other defense capabilities.

"Without Fortinet, we absolutely would not be here right now. Fortinet solutions are incredible."

– Chief Technology Officer, Cloud Hosting and Services Company

Details

Customer: Cloud hosting and services company

Industry: MSSP/Service Provider

Location: Americas

Business Impact

- Immediate protection against known and unknown global threats
- Coverage of entire enterprise-scale infrastructure
- Easy to implement, with no changes to environment required
- Scalable security solutions capable of supporting dynamic business growth

Initially, the IT staff had been unable to determine where the infiltrators were coming from, but once installed, FortiAnalyzer immediately provided insight. “It was precisely what we needed,” the CTO notes. “It pinpointed the exact origin of the attacks.”

Broadening the Protection

Today, leveraging the Fortinet Security Fabric, the company has implemented the FortiManager centralized management platform to enable single-pane-of-glass control across all the Fortinet devices throughout the infrastructure. The FortiADC application delivery controller was added to streamline the delivery of secure applications, and FortiDDoS was deployed to protect against both known and unknown distributed denial-of-service (DDoS) attacks.

“Without Fortinet, we absolutely would not be here right now. Fortinet solutions are incredible. We use them throughout our security stack on a very large scale, and we also recommend them to our customers based on our first-hand excellent experience,” the CTO states.

The chief executive officer summarizes, “All told, the ransomware breach—which I think of as a terrorist attack—caused more than three million dollars of damage. It was a massive wake-up call for us that we had to find more than just a big-named security vendor; we had to source a best-in-class solution.

“For me, Fortinet stands out for having a solution set that spans every layer of the security stack; giving us confidence that we can continue to securely deliver the unrivalled levels of service and support that our clients deserve.”

Solutions

- FortiGate
- FortiAnalyzer
- FortiManager
- FortiDDoS
- FortiADC

“Despite having a very complex environment, we made the switch to the FortiGate NGFW in 30 minutes; it was amazingly straightforward. We didn’t have to re-architect any aspect of our environment.”

– Chief Technology Officer, Cloud Hosting and Services Company

www.fortinet.com

February 24, 2021 2:33 AM

D:\Fortinet\2021 Rebranded templates\Case Studies\February\IT Solutions provider\cs-it-solutions-provider-stops-massive-ransomware-attack-2242021\cs-it-solutions-provider-stops-massive-ransomware-attack-2242021

650247-0-0-EN