IT SOLUTIONS PROVIDER STOPS MASSIVE RANSOMWARE ATTACK WITH NEXT-GENERATION FIREWALL

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

– *Chief Technology Officer, cloud hosting and services company*

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 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 recalled 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 2-day period and some of the end-users were blocked for as long as five days."

FORTINET TO THE RESCUE

Luckily one if its employees brought in a FortiGate Firewall 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 was able to deliver the necessary intrusion protection, anti-virus and web-content filtering capabilities that we urgently needed to secure our entire network and regain control," the CTO recounted.

DETAILS

CUSTOMER: Cloud hosting and services company

INDUSTRY: Information Technology

LOCATION: USA

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

SOLUTIONS

- FortiGate
- FortiAnalyzer
- FortiManager
- FortiDDoS
- FortiADC

The company immediately engaged with Fortinet and purchased a Fortinet FortiGate 1500D Enterprise Firewall, along with FortiAnalyzer, to replace the incumbent firewall that had failed the company.

"Despite having a very complex environment, we made the switch to the FortiGate 1500D in 30 minutes; it was amazingly straightforward," enthused the CTO. "We didn't have to re-architect any aspect of our environment."

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

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 noted, "It pinpointed the exact origin of the attacks."

BROADENING PROTECTION

"Today – leveraging the Fortinet Security Fabric – the company has implemented FortiManager to enable single-pane control across all the Fortinet devices throughout the infrastructure. FortiADC was added to streamline the delivery of secure applications delivery and FortiDDoS 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 stated.

The chief executive officer, summarized, "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."

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

112114-A-0-EN September 5, 2017 10:46 AM
Macintosh HD:Users:mbunnell:Desktop:CS-IT-Ransomware:cs-IT-ransomware