"In summary, they're a great partner, very active both on the business development side, as well as the support and product side."

– James Brooks
Sr. Product Manager
Dell SecureWorks

WhatWorks in Intrusion Prevention and Detection: Innovating and Evolving at a Manager Security Services Provider

About Dell SecureWorks

Dell Inc. (NASDAQ: DELL) listens to customers and delivers innovative technology and services that give them the power to do more. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs. For more information, visit www.secureworks.com.

About the User

Mark Wood, Director of Product Management, Dell SecureWorks
Mark Wood has more than 25 years of experience in the technology industry in product management and engineering. Prior to Dell SecureWorks, Mark held a variety of roles at Cloud Sherpas, nCircle, Internet Security Systems (ISS), and AT&T Bell Laboratories.

Details

Customer Name: Dell SecureWorks
Industry: MSSP
Location: Atlanta, GA (Global Headquarters)

Challenges

- Enhancing protection of IT assets
- Reduction of overall security costs singly and with partners

Objectives

- Broaden base of product offerings
- Retain scalability in growing partnerships

Deployment

- FortiAnalyzer
- FortiGate
- FortiManager
- FortiWeb

Mark holds a Bachelor of Science degree in computer science from Duke University and a Master of Science degree in computer science from Georgia Institute of Technology.

SANS Summary

Managed Security Services provider Dell SecureWorks wanted to broaden its base of product offerings by including Fortinet solutions. The Fortinet firewalls and other products are scalable and cost-effective. Good customer service and a willingness to innovate and evolve products based on requests were added bonuses.

Interview

Q: As an MSSP, what was going on with your clients that prompted you to bring Fortinet into the mix of products you manage?
A: Many of our clients were impressed with the performance and features available on Fortinet appliances and either wanted to start their initial deployment of FortiGate products or expand their existing FortiGate installations.

Q: When did you add the Fortinet products?
A: We added support for Fortinet products to our portfolio of services in the first half of 2010.

Q: Do you know why the Fortinet products were chosen?
A: Fortinet is strong in the UTM space and is gaining speed on the enterprise side. They are a great partner to work with from a business development perspective and support. They continue to innovate and deliver a solid UTM product.

Q: Typically, there are two reasons why MSSPs would support a product: one is if the customer base wants them to manage and monitor a particular brand of firewall, the other is that the MSSP wants to offer and recommend a specific product that they will monitor and manage for a client. Which one drove Dell SecureWorks to support Fortinet?
A: As an MSSP, we are technology agnostic. When a product gains traction in the market, our customers will generally ask us to support. That's when we decide to engage with a technology partner.

Q: Do you have any idea of the managed service offering Dell SecureWorks is currently doing where the FortiGate products are out there, some idea of some of the larger scale customers, quantity of devices, FortiGate devices?
A: We manage hundreds of Fortinet devices and the number grows every year. We typically manage five to 15 FortiGate devices per customer, which may just be a subset of the all their devices. For example, a customer may want Dell SecureWorks to manage FortiGate devices that need a sophisticated rule so they can benefit from our expertise and in-depth knowledge on the FortiGate products.

Q: Which FortiGate products are you managing the most?
A: For Dell SecureWorks, it's a mix of small-to-upper range of devices. Enterprises use all device sizes to protect their micro/small offices and central headquarters. Smaller organizations leverage primarily the small to medium sized devices based on their own specific needs.

Q: Can you expand on managing the FortiGate next generation firewall-type capabilities for your enterprise customers?
A: There's been a shortage of talent in the security industry for some time. When customers need to grow their business, and their networks, they need security expertise and may not be able to hire appropriately. Rather than having to find an employee who has specific expertise for every next generation device and feature, a managed security services partner like Dell SecureWorks can that care of that for them.

Q: Since FortiGate tends to have UTM-type capabilities across products, what are the most frequently used functions on the FortiGate products that the customers are asking you to manage?
A: IPS and the firewall. The more advanced application control features are a driver for our services. As an example, customers don't necessarily want to block everyone from going to a site such as Facebook, but

they may want to limit only their marketing department to have access. That granular level of control is probably the fastest growing segment. Also, requests for features like Web or URL filtering and integrated anti-virus is also on the rise.

Q: As an MSSP, do you use FortiManager?
A: We do leverage some of the FortiManager capabilities on the device in combination with own systems. Our customers may have a FortiGate as well as other vendor firewalls or other security technologies. We have to leverage our backend systems to integrate all of those technologies into one portal where a customer can log in and see a macro view of their security network.

Q: Let's look at a typical install. You either have a new customer that's using FortiGate or you have an existing managed service customer that's going to add FortiGate products to the mix. How long does it typically take to do an install and get things up and running?
A: The entire install is usually about 30 days or less, including configuring the device, shipping it, installing the device remotely and integrating it into our operations. Lastly, we transition the process from the implementation team to the security operations center.

Q: Dell SecureWorks monitors lots of people's equipment across lots of different products. When some new threat becomes known, how do you handle pushing out updates to the FortiGate products?
A: Most updates and signatures are already done by Fortinet, and we're taking care of the patch management, the change management issues and policy changes. We're also monitoring it 24x7. Any alert or suspicious activity is correlated through our Counter-Threat Platformsm and ultimately to our SOC, our Security Operations Center. They analyze it and recommend an appropriate action.

Q: How did Dell SecureWorks work with customers using the FortiGate products to help them with advanced threats?
A: Information provided by Fortinet is automatically integrated into the device through the traditional FortiGate channels, signature updates and so forth. We ensure that the devices are updated properly from the Fortinet resources. As you know, our Counter Threat Unit (CTU) has the best researchers in the world constantly surveying the global threat landscape. If there is a specific threat we're following – we'll program our technology to be on alert for the threat actor's behavior. Our systems will alert us as threats are found during the process described earlier and are evaluated in real-time by one of our analysts in the Security Operations Center.

Q: In your SOC, do you have a test bed with the types of equipment you have under management?
A: Yes. Every patch or change is tested by a team that's dedicated to that type of activity. Patch management, certification of a new hardware platform or other similar changes are handled by a separate team. We support any new devices or push out a new patch or change unless it's gone through the certification process and we know there are no bugs or other issues.

Q: What are some of the positive features you've seen on the FortiGate products?
A: Probably the high throughput speed. Fortinet seems to handle additional features quite well. Also, they're definitely one of the leaders in virtualization, which is a very fast growing area for the industry.

Q: Is Dell SecureWorks seeing a lot more demand to monitor and manage virtual firewall instances?
A: Most definitely. Some customers may want to segment different parts of their network using a virtual firewall and one hardware platform. Others may have an internal cloud and use it to segment their customers while still leveraging the tools that we provide them. In that case, they get the value of only having to buy one appliance, but can leverage that across multiple customers.

Q: So, you'll have customers that are using one of the bigger FortiGate appliances and are virtualizing it to segment their customers and then Dell SecureWorks is doing the monitoring for them?
A: Yes. We're sort of the backend system for them. The first model I mentioned was simply the enterprise

customer who has a data center or a large corporate network and needs to provide their own segmentation.

Q: From the MSSP side, is there something you have to do differently when you're monitoring and managing a virtual FortiGate versus a dedicated box?
A: For us, it's viewed as just another firewall. On the backend, other than being flagged as a virtual firewall, everything else is treated the same.

Q: How's the support been from Fortinet in supporting Dell SecureWorks?
A: No issues. I spoke with one of our platform engineers who does a lot of the certifications and communicates a lot with the support team. They say the support is great.

Q: You mentioned FortiAnalyzer, are there any other Fortinet products that Dell SecureWorks uses or its customers use that you're monitoring?
A: We have FortiWeb, some email appliances and FortiGate appliances. If we get a request for something we don't support currently, we can turn it around pretty quickly because we have individuals internally dedicated to FortiGate.

Q: What do you think of the FortiGate products overall?
A: In summary, they're a great partner. We are pleased with our partnership from a business development perspective as well as product feature and support.

SANS Bottom Line on Fortinet products at SecureWorks:

1. Consistently good customer service, meets the evolving needs of clients;

2. Virtual firewalls scale well for most customers;

3. High level of throughput with advanced features turned on;

4. Offers granular level of control for IPS and firewalls.

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

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

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

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428