

## Cisco Helps Vignette Maximize the Efficiency of its Security Architecture

### Background

Based in Austin, Texas, Vignette Corporation is a growing technology company that provides comprehensive applications to give customers the ability to deliver enterprise Web applications that integrate information, composite applications, and business processes to effectively meet business objectives. Vignette's solutions allow organizations to reduce costs, improve productivity, and increase customer satisfaction through the effective delivery of highly personalized and targeted enterprise information. Businesses of any size can more effectively manage their IT infrastructures, enterprise information, and customer interactions through Vignette's broad line of application services, suites, and product modules.

With close to 900 employees and offices all across the globe, a robust and secure network is integral to the efficient operation of Vignette's business. When Senior Network Engineer Selim Nart started working for Vignette more than two years ago, the company wanted to simplify its network to more easily protect it. Vignette's IT Operations team redesigned the network, taking a modular approach based on the SAFE Blueprint from Cisco®. According to Nart, "This gave us control over most viruses, network management, deployment, and growth. For example, if we have to move a particular group, we can disconnect that group's module and move that network somewhere else without interruption of service to any other groups."





## Protecting the Network

With a newly designed network structure in place, the Vignette IT Operations team was available to concentrate on the crucial task of securing the network. Due to budget limitations, Vignette had to implement security solutions in stages. The company began with Cisco PIX<sup>®</sup> security appliances for external firewalling, placing three different sets of Cisco PIX security appliances at the headquarters: one for network access to the outside, one for e-commerce, and one to control the product demonstration environment. Next, Vignette deployed Cisco VPN 3000 Series concentrators to support the most advanced encryption and authentication techniques ensuring that remote workers and offices could securely connect to the central office.

Once the IT Operations team had implemented the new VPN concentrators and Cisco PIX security appliances, they focused on what they considered to be a vital component of any comprehensive security architecture: intrusion protection. They looked carefully at several vendors' Intrusion Detection System (IDS) offerings, and chose Cisco IDS solutions. "Cisco IDS solutions were very easy to implement and fit right into our network design," says Nart. "Another major reason we picked Cisco is for the support structure. We have Cisco staff supporting us up in the United Kingdom and Sydney, Australia. Rather than relying on U.S. employees for support and waking them up at night, we can contact local representatives. It helps us a lot."

Vignette installed one Cisco IDS 4210 Sensor to monitor the demo environment and two Cisco Catalyst<sup>®</sup> 6500 Series IDS services modules (IDSMs) in a backbone Cisco Catalyst 6500 Series switch. One of the modules is active and one serves as backup to maintain fully redundant intrusion protection. The IDSM receives copies of packets directly from the switch backplane and provides full-featured intrusion protection services within the switch. Like the Cisco IDS 4210 Sensor, the IDSM inspects traffic traversing the network, identifies unauthorized or malicious activity, such as hacker attacks, worms, or denial-of-service (DoS) attacks, and terminates this illegitimate traffic to suppress or contain threats. "The IDS appliance and modules are very flexible and easy to deploy," says Nart.

## The IDS Challenge

Although the Vignette IT staff was impressed by the amount of activity thwarted by its newly implemented intrusion protection solutions, the team was having difficulty keeping up with the sheer volume of alarms. "We were receiving about 90,000 alarms per month," Nart recalls. "We did not have the personnel to handle it. Our network is so adaptive, it keeps changing so much, so we do not have the resources to continually configure and write filters to help qualify our alarms."

## The Solution: Cisco Threat Response Technology

In light of the company's need to better organize and filter IDS alarms, Vignette was pleased to discover Cisco Threat Response software, which virtually eliminates false alarms and automatically determines which threats need immediate attention to avoid costly intrusions. "Basically, Cisco Threat Response software virtually replicates a network security engineer," Nart explains. "The software creates a sort of artificial intelligence that is about 25 times faster than a regular engineer who receives alarms, investigates the alarms, and then reports on the severity of the alarms and whether or not we should pay attention to them."

## The Result: Reduced Costs, Increased Efficiency

Nart calculated that with Cisco Threat Response software Vignette saw a 95 percent reduction in alarms—more than 85,000 false alarms were eliminated in one month alone. The new software also substantially reduced the total cost of ownership for the company's intrusion protection solutions because Vignette did not have to hire additional engineers to monitor alarms. At the same time, the Vignette IT Operations team could now focus on valid alarms and prevent costly intrusions from affecting the company's business operations. "With every alarm we block, we increase our uptime and increase our business to our customers," Nart explains. "And we can now create reports every month for upper management regarding how many alarms we have received and how many we have blocked. This helps us to quantify our work as an IT department and it helps us to be viewed as a business unit value."

Vignette did not have to expend a lot of time or resources to reap the benefits of Cisco Threat Response software. "Even though the technology is complex, the software design is very simple to manage and understand," says Nart. "Cisco Threat Response software is

easy to use for our engineers here and is really doing what it's supposed to do—managing alarms for us. It gives us the sense of security that someone is monitoring our alarms around the clock."

## Conclusion

Vignette has so finely tuned and maximized the efficiency of its security solutions that it now has more than ample time to concentrate on the rapid growth of the business. The company is currently expanding the network to support new offices, and Vignette administrators are considering implementing several additional Cisco PIX security appliances and Cisco IDS 4200 Series sensor appliances, including Cisco Threat Response software, at the company's new locations. The Vignette IT Operations team is also working on deploying a secured wireless network and IP telephony, based on SAFE blueprints from Cisco. Nart is confident that his security architecture is serving the company as a tool to protect business productivity without over-taxing his IT department. In fact, he's come to rely so heavily on the newly deployed security systems that he says working without them "would be like operating in a sandstorm."



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the  
**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Catalyst, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.  
(0304R) ETMG 203170—RD 09/03