Real-Time Threat Prevention Lets Managed IT Services Provider Vology Thrive

Summary

Company:
Vology

Industry:
Technology

Business Challenge:
Protect corporate headquarters and branch offices from advanced threats in e-mails and websites

Technology Solution:

- Juniper Sky Advanced Threat Prevention
- SRX1500 Services Gateway
- Junos Space Security Director

Business Results:

- Enabled a proactive approach to threat detection and remediation
- Gained real-time visibility and protection against previously unseen threats
- Able to automatically detect and stop malware before damage is done

More than 1,400 organizations have relied on Vology for IT consulting and managed IT services, which include Office365, network and server monitoring, IT outsourcing, and disaster recovery. Vology monitors more than 100,000 IT devices at more than 20,000 customer locations through two network operations centers. The company has been ranked on the Inc. 5000 list of most successful private companies in America for 11 consecutive years.[1]

Business Challenge

Vology is thriving, but as the scale and sophistication of cybercrime continues to increase, the company needed to rethink its defense strategy. "We wanted the ability to see threats as they happened and act very quickly," says Matt Jolly, senior IP solutions architect at Vology. "With threats accelerating, classic reactive security technologies don't get the job done anymore."

Technology Solution

To stop highly skilled cybercriminals and evasive malware, Vology needed cybersecurity built around automated and actionable intelligence, which could be shared quickly to recognize threats.

Vology deployed Juniper Sky™ Advanced Threat Prevention along with the next-generation Juniper Networks® SRX1500 Services Gateway for advanced malware protection from the cloud. Juniper Sky constantly analyzes e-mail and Web files to detect advanced persistent threats, ransomware, and other sophisticated malware.

"After less than a day with Juniper Sky, we knew about threats that we had never seen before," Jolly says.

Juniper Sky uses a pipeline of techniques to quickly detect and prevent a cyberattack, including state-of-the-art machine learning algorithms, sandboxing to trick malware into activating and self-identifying, an antivirus engine to identify known malware, and analysis of code to spot possible dangerous fragments.

"We discovered that a few of our internal servers at the data center and several of our remote users were flagged and blocked for command-and-control, or C&C, hits," he says. "This is not uncommon, but what was interesting was the vector."

[1] "Vology Ranks Among 2016 Inc. 5000 List of Fastest-Growing Private Companies," Vology, August 22, 2016, https://www.vology.com/news/2016/08/22/vology-ranks-among-2016-inc-5000-list-of-fastest-growing-private-companies/

By looking at the incident details revealed by Juniper Sky, Jolly could see that the communication with the C&C servers was coming through the local Web browser of the infected machines. The C&C servers were waiting for responses from scripts built into webpages of several major media sites, which were inadvertently running infected ads. In some cases, Vology employees didn't even have to click on the ads; the C&C server would still contact their machines. "Juniper Sky immediately blocked the clients to protect them from further contact until we could remediate the issue," Jolly says.

Juniper Sky is integrated with Juniper Networks SRX Series Services Gateways, which are next-generation firewalls that deliver deep inspection, inline blocking, and actionable alerts. "It's good to take action right up front," says Jolly. Vology also plans to integrate the Juniper Networks Spotlight Secure Threat Intelligence Platform with Juniper Sky to cascade threat information to SRX Series firewalls for immediate action.

Vology uses Juniper Networks Junos® Space Security Director to automate security management. Security Director provides extensive policy management and control through an intuitive interface that offers enforcement across emerging and traditional threat vectors. Security Director's dashboards and reports provide insight into threats, compromised devices, and risky applications.

"After less than a day with Juniper Sky, we knew about threats that we had never seen before."

Matt Jolly, Senior IP Solutions Architect, Vology

Business Results

"What we experienced with Juniper Sky was unexpected and enlightening," Jolly says.

Juniper Software-Defined Secure Network (SDSN) enables Vology to protect its business and its customers with a more innovative approach to cybersecurity that is fast, intelligent, and automated. With advanced threat detection and prevention, Vology is better protected from cybercriminals and can take immediate action when the inevitable happens. Vology can guard its corporate offices—from its headquarters in Clearwater, Fla., to its offices in California, Texas, and Oklahoma—from the data theft, business disruption, and loss of customer trust that can happen when security breaches occur.

With Juniper Sky identifying malware in real time, and SRX Series next-generation firewalls automatically blocking threats, Vology is detecting threats in real time—and quickly remediating infections before lasting damage is done.

Juniper Sky analyzes all suspicious traffic and determines the threat severity on a scale of one to 10, prioritizing the most critical alerts for Vology's IT security operations team. That saves valuable time, so analysts aren't sifting through mountains of data to find the needle in the haystack. "Juniper Sky democratizes security," Jolly says. "You don't have to be a security expert to do the forensics and validate a threat as real."

Deploying Juniper Sky has had a profound effect on security strategy at Vology. "Our IT staff realized they needed to change their security posture to account for real-time threats," says Jolly. "They were frustrated and alarmed that they did not have a solution to the issue. Their go-to desktop- and server-based antivirus solutions didn't—and couldn't—detect the threats identified by Juniper Sky." As a result, IT created new security policies that incorporated active threat prevention into its operations, which would help keep Vology one step ahead of the cyberattackers.

"Juniper Sky democratizes security. You don't have to be a security expert to do the forensics and validate it as a real threat."

Matt Jolly, Senior IP Solutions Architect, Vology

Next Steps

"What we found with Juniper Sky highlights the necessity of having a robust edge solution that can take immediate action on actively evolving threats," Jolly says. "We learned that sites we think are trusted aren't. We learned that our IT staff must be on top of security threat and response. And we learned that active threats cannot be managed with reactive security solutions."

For More Information

To find out more about Juniper Networks products and solutions, please visit www.juniper.net.

Note: Juniper offers Juniper Sky JumpStart Services to enable the rapid adoption and use of Juniper's core software products. Upon completion of this service, you will have implemented a ready-to-use Juniper Sky solution with expert knowledge transfer, enabling your operations teams to optimize its core value. To find out more, please visit www.juniper.net/assets/uk/en/local/pdf/datasheets/1000609-en.pdf.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

3520603-002-EN May 2017