

COOPER-STANDARD PROTECTS GLOBAL NETWORK AND PROVIDES SECURE ACCESS WITH BEST-IN-CLASS SECURITY SOLUTIONS

Summary

Industry: Automotive systems and component manufacturing

Challenges:

- Deliver a robust security strategy to protect global network against attacks and malicious software
- Pass security audits that demonstrate compliance with the Sarbanes-Oxley Act in preparation for going public
- Provide vendors and other third-parties with secure remote access in a cost-effective and secure manner

Selection Criteria: Security solution recommended by systems integration partner

Network Solution:

- Juniper Networks IDP200 Intrusion Detection and Prevention Appliance
- Juniper Networks SA2000 SSL VPN Appliance

Results:

- Identify and stop attacks and malicious software from both outside and inside the network
- Make passing regulatory compliance audits fast and easy by providing best-in-class security with detailed reporting
- Provide vendors with secure remote access to a global network in minutes
- Conserve bandwidth by minimizing malicious and non-business traffic

From GM Sierra extended cab trucks to Ford Fusion compacts, chances are your ride depends on Cooper-Standard Automotive Inc. components. This Michigan-based company makes body sealing systems, fluid handling systems, and noise, vibration and harshness products that are used by the world's leading automakers.

With roots in tire manufacturing, Cooper-Standard has transformed itself through a series of acquisitions, and today the company supplies one of the largest portfolios of products to the automotive industry. "Change is the key word around here," says Jeff Sonne, Manager of Network Services at Cooper-Standard Automotive.

Challenges

"We needed a proven way to guarantee we're secure," says Sonne. "We believe in a defense-in-depth strategy with total diversity." Protecting operations in 62 locations across 15 countries means enforcing a unified security approach across the company's operations in Asia, Europe and the Americas. "Our policies are the same and our security solutions are in common, regardless of location. We have a single view across the world, so we can monitor and react quickly to what's happening on our network across the globe."

Selection Criteria

Sonne was introduced to Juniper Networks security solutions through its managed security service partner, CentraComm Communications. CentraComm provides active management of Cooper-Standard's IDPs. "We considered various options, and went with CentraComm's recommendation," says Sonne. As a 20-year veteran of networking, Sonne characterizes his experience with Juniper gear as having "proven themselves as quite capable."

Solution

Cooper-Standard uses Juniper Networks® IDP200 Intrusion Detection and Prevention Appliance in its locations in the United States, China and Germany as an integral part of its defense-in-depth strategy. It also deployed the Juniper Networks SA2000 SSL VPN Appliance to provide secure remote access to key vendors.

Results

"We sleep at night knowing that we're protected with Juniper Networks," says Sonne. The Juniper Networks IDP200 Intrusion Detection and Prevention Appliance is a purpose-built intrusion detection/prevention platform that delivers day-zero protection against worms, trojans, spyware and other malware from penetrating the network and spreading from already infected users to others. Ideal for enterprises, the IDP200 supports up to 250 Mbps throughput and 70,000 sessions. Cooper-Standard uses granular security policies based on what traffic to look at, what attacks to look for in that traffic, and how to respond when an attack has been detected.



Cooper-Standard also uses the IDP200 platform to identify internal misconfigurations, rogue servers, as well as types and versions of applications and operating systems that may have been unknowingly added to the network, such as toolbars and spyware.

According to Sonne, the biggest benefit of deploying Juniper Networks security solutions is that its IT infrastructure goes beyond protection.

Cooper-Standard works closely with its managed security provider, CentraComm, which provides first-line operations and reporting for its IDP worldwide. "The reporting is phenomenal. It gives us the information we need to create policies and correct misconfigurations," says Sonne. The IDP Series has fully customizable reporting, which can be used to generate up-to-the-minute status on network activity. The robust reporting is a key feature of the Juniper Networks Network and Security Manager. CentraComm has leveraged NSM to centrally manage multiple IDP Series devices worldwide in a single interface. Ultimately, this enables CentraComm to take a holistic view of a global network and allows them to react quickly to security events blocked by the IDP Series and update other IDP devices immediately. The Juniper Networks IDP Series is also critical as part of the company's penetration testing to ensure comprehensive security. "We don't tip off CentraComm that we're going to run a penetration test against the IDPs, but they've never missed an attack."

"We sleep at night knowing that we're protected with Juniper Networks."

Jeff Sonne
Manager of Network Services, Cooper-Standard Automotive

An added benefit of the IDP Series is bandwidth savings, since malicious and non-business traffic are dropped. "We suspect that we're saving more bandwidth than meets the eye," says Sonne.

In addition to protecting the company's IT infrastructure against network attacks and malicious software, Cooper-Standard uses Juniper Networks security solutions to provide secure remote access. As a global organization, Cooper-Standard has long provided remote access to employees, customers and partners. And SSL VPNs are playing a larger role in providing that access.

Cooper-Standard employees can access email and other business applications via Java-based Web portals and by using two-factor authentication. The company connects its supply chain applications to the auto manufacturers over the ANX eBusiness Network. But for its vendor partners who don't fit those solutions, Cooper-Standard has turned to SSL VPNs to provide access quickly and securely.

"If we have a vendor that needs internal network connectivity that is not offered through our Web portal, the Juniper Networks SSL VPN is our quick solution to get them access," says Sonne. About a dozen key service partners use the Juniper Networks SA Series SSL VPN Appliances to do jobs such as remotely managing manufacturing production line equipment or to access mainframe-based applications. Sonne anticipates Cooper-Standard will be able to connect many smaller vendors this way.

"We've had this problem for a long time," says Sonne. "We used to give people full network access and hope for the best. Now they go straight through the SSL VPN. It's more secure and easier to maintain."

Sonne praises the Juniper Networks SA2000 for its management and control. "We can lock users down to their specific mission that they're supposed to be doing," says Sonne. Setting up new users takes only minutes, he says.

With the SA2000, Cooper-Standard can provide secure remote access, intranets and extranets from one platform. The SA2000 provides end-to-end layered security, including endpoint client, device, data, and server security controls. Endpoint security is best-in-class and is driven by the user group or role, as well as by network, device or session attributes. As an SSL VPN, the cost of ownership is lower than remote access solutions that require the deployment of client-side software.

The SSL VPN appliance provides Cooper-Standard with best-in-class security with operational simplicity. The success of the SA Series appliance and the Web portals for remote access has prompted the future direction of secure access toward SSL VPNs and away from direct connectivity to the corporate network, according to Sonne.

Next Steps and Lessons Learned

Cooper-Standard has reaped rich rewards from its Juniper Networks security solution with best-in-class security. "That's priceless," says Sonne. Based on proven success, Cooper-Standard will use the Juniper Networks IDP Series to protect all new regional data centers it manages. Sonne adds that the service from Juniper Networks has been awesome. "The IDP Series works and stays current. It doesn't get any better than that."

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.