

Building Supplier Gains New Visibility into Network Environment

With hundreds of network devices deployed across thousands of miles, Pacific Coast Companies turned to Cisco for real-time security insight.

EXECUTIVE SUMMARY
<p>PACIFIC COAST COMPANIES, INC.</p> <ul style="list-style-type: none"> • Building Materials Manufacturing & Distribution • Rancho Cordova, California, United States • 3000 employees
<p>BUSINESS CHALLENGE</p> <ul style="list-style-type: none"> • Protect mission-critical supply chain applications from downtime due to network attacks • Guard against rogue devices across large, dispersed network environment • Improve visibility into network security state
<p>NETWORK SOLUTION</p> <ul style="list-style-type: none"> • Overhauled network defenses with Cisco security and network monitoring solutions
<p>BUSINESS RESULTS</p> <ul style="list-style-type: none"> • Immediately identified previously unknown threats • Allowed IT team to quickly block any rogue device • Will deliver full ROI in one year

Challenge

Pacific Coast Companies provides IT and administrative services for the Pacific Coast Building Products family of companies, one of the largest suppliers of building materials and supplies in the United States. The IT team supports more than 80 facilities across the western United States, Canada, and Hawaii, including manufacturing sites that manufacture building materials, dozens of large supply yards and warehouses, and a transportation and logistics organization.

Pacific Coast’s business model is based on providing essential building materials to customers exactly when they need them to meet aggressive building and construction schedules. To support this “just-in-time” model, the company relies on customer service, supply chain, and logistics applications. These tools help Pacific Coast operate efficiently and provide better service to customers, but they also could potentially leave the company vulnerable to a

network attack. A security breach that shuts down an important distribution site or supply chain application, for example, could result in huge financial losses, both to Pacific Coast and its customers. The Pacific Coast network also supports large banking and financial transactions every day, which could present an attractive target to criminals.

Pacific Coast Companies has long employed network security technologies to protect against threats, but the scope of the operation presented significant challenges.

“Our facilities can be enormous, literally miles of warehouse under one roof, with 15 to 20 access switches throughout the property,” says Matt J. Okuma, enterprise architect with Pacific Coast Companies. “It’s very hard to control what is physically plugged into our network. We’ve had instances in the past where rogue access points ended up bringing down parts of our network. Guarding against those kinds of intrusions is our biggest concern.”

Over time, the Pacific Coast network had become so extensive that the company was devoting a full-time IT analyst solely to reviewing device logs to monitor for intrusions. In an attempt to employ a more efficient solution, the company had decided to outsource its intrusion prevention system (IPS) services to a third party. The service included a managed IPS appliance that the Pacific

Coast IT team could not access and continuous monitoring of the company's two firewalls. Unfortunately, the experience proved less than satisfactory.

"It was a very costly service, and we found that we weren't really getting anything out of it," says Okuma. "They were supposed to review all of our firewall logs and correlate issues for us, but the analysis that we received was very generic. Even if they found a problem, they couldn't tell us exactly where it was coming from. There was no way to tell if threats were getting through. It just wasn't cutting it."

"We had spent a long time trying to achieve that kind of visibility with our previous IPS service. But in less than half a day of deploying the Cisco IPS and MARS solutions, we were gaining extremely valuable insights."

—Matt J. Okuma, Enterprise Architect, Pacific Coast Companies

Solution

Pacific Coast Companies had long relied on Cisco® networking and unified communications solutions to support its just-in-time operation. When the time came to renew the outsourced IPS contract, the company turned to Cisco for an alternative solution.

"We run a very lean IT operation, so I'm always trying to reduce complexity in our environment," says Okuma. "As soon as you start introducing products from multiple vendors, you create more complexity, and more time and resources that need to be devoted to making sure everything works together. We have a major investment in Cisco technology, and we rely on Cisco to design unified, interoperable solutions for us."

Okuma's personal experience with Cisco support also played a role in the decision.

"When we had issues with the third-party IPS solution, we didn't get the kind of service that we were used to receiving from Cisco TAC [Technical Assistance Center]," says Okuma. "We have a very good rapport with Cisco. Knowing that the support will be there if we need it was very important."

The Pacific Coast IT team launched a proof-of-concept analysis of a Cisco security solution based on the Cisco ASA 5500 Series IPS Solution and the Cisco Security Monitoring, Analysis, & Response (MARS) system. The Cisco ASA 5500 Series would provide perimeter defense, along with integrated inline IPS to guard against intrusions and other network threats. Cisco Security MARS would collect and correlate information from the security appliances, as well as from Cisco switches across the environment. Okuma hoped the solution would give his team a real-time picture of the entire network environment, and allow them to rapidly isolate suspicious activity. It didn't take long to see results.

"The first day of the proof-of-concept, we found a host within the IT department that was infected with malware," says Okuma. "We were able to identify it and stop it immediately. We had spent a long time trying to achieve that kind of visibility with the previous IPS service. But in less than half a day of deploying the Cisco IPS and MARS solutions, we were gaining extremely valuable insights."

Pacific Coast Companies decided to let the outsourced IPS contract expire. They upgraded the company's existing Cisco PIX® firewalls to Cisco ASA appliances with IPS modules and fully deployed Cisco Security MARS in the production environment.

In addition to firewall and IPS capabilities, the Cisco ASA appliances provide integrated virtual private network (VPN) functionality, allowing Pacific Coast Companies to support critical VPN links to key partners with a single device, instead of using dedicated VPN appliances. The migration from the previous solutions to the Cisco ASA 5500 Series was a relatively quick, painless process.

“I was very impressed when I migrated the site-to-site VPN tunnels with some of our vendors to the Cisco ASA appliances,” says Ken Joseph, the Pacific Coast Companies network engineer responsible for managing the company’s firewalls. “I was anticipating having to do a lot of troubleshooting on the production network, but once we cut over to the new devices, the tunnels came up flawlessly.”

Results

Since deploying the Cisco IPS solution and Cisco Security MARS, Okuma has gained extraordinary visibility into the Pacific Coast Companies environment. He is confident that the organization is more secure than ever before, and that his team can now quickly identify and respond to any threat.

“With the previous security solution, we were always relying on the service provider to protect us, hoping that they were watching our network carefully,” says Okuma. “Now, if there is a problem, I receive an alert from the Cisco Security MARS, and I can log in and see everything for myself. If there is a network slowdown somewhere, I don’t have to call that site to try to figure out what’s happening. I can see the potential threat or attack path and drill down to investigate issues as they are unfolding.”

PRODUCT LIST
<p>Routing and Switching</p> <ul style="list-style-type: none"> • Cisco Catalyst® 3560 and 3750 Series Switches • Cisco 2800 ISR Routers
<p>Security and VPN</p> <ul style="list-style-type: none"> • Cisco ASA 5510 Series with AIP-SSM-10 Modules • Cisco Security Monitoring, Analysis & Response System
<p>Unified Communications</p> <ul style="list-style-type: none"> • Cisco Unified Communications Manager • Cisco Unity® • Cisco Unified IP Phones 7900 Series

The Cisco security solution also helps safeguard Pacific Coast Companies against infections from rogue devices at its many business sites. “We have all of our switches logging into the Cisco Security MARS, and it gives us a much better sense of what’s happening at those remote locations now,” says Okuma. “If someone tries to plug a device into a switch, I have fine-tuned the system to immediately disable that port.”

The Cisco solution has also benefited Pacific Coast Companies’ bottom line. The entire solution was deployed for the same cost as the company was previously paying annually for its IPS contract, providing a full return on investment in just one year.

The greatest benefit of the new security solutions, however, is simply the knowledge that Pacific Coast’s mission-critical, just-in-time business operations are protected. “I couldn’t begin to put a dollar value on having the kind of control that we have now, but it’s a huge advantage,” says Okuma.

Next Steps

The Pacific Coast Companies IT team is now working to incorporate every network device and server at every location into the new Cisco security solution. Whereas the previous IPS service monitored just two firewalls, the Cisco solution will ultimately monitor hundreds of devices across the entire environment.

For More Information

To find out more about Cisco security solutions, visit <http://www.cisco.com/go/security>.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0812R)

Printed in USA

C36-518928-00 01/09