

Utility Overhauls Network Defenses to Boost Control and Visibility

Jones-Onslow Electric Membership Corporation upgraded network with advanced security features.

EXECUTIVE SUMMARY
<p>JONES-ONSLow ELECTRIC MEMBERSHIP CORPORATION</p> <ul style="list-style-type: none"> • Industry: Utility • Location: Jacksonville, North Carolina • Number of Employees: 167
<p>CHALLENGE</p> <ul style="list-style-type: none"> • Protect network against malicious threats • Implement tighter controls over third-party vendor access • Streamline labor-intensive malware defense processes • Address PCI Compliance more efficiently
<p>SOLUTION</p> <ul style="list-style-type: none"> • Upgraded network defenses with firewall, virtual private network, access control, intrusion prevention, and security monitoring solutions.
<p>RESULTS</p> <ul style="list-style-type: none"> • Reduced malware and spyware • Greater visibility into and control over third-party network users • Eliminated time-consuming manual processes • Improved PCI Compliance efficiencies

Challenge

Jones-Onslow Electric Membership Corporation (JOEMC) is a member-owned electric utility cooperative with a vital technology infrastructure. The cooperative’s network supports a variety of critical applications, including an IP contact center, customer support and financial applications, and an outage management system that alerts JOEMC employees to service problems. All of these systems are essential to providing the electric service on which 60,000 JOEMC customers depend every day, and those customers demand the utmost reliability and security. However, one of the biggest challenges for JOEMC is supporting all applications and customers with just a four-person IT staff.

“Because we are a small department, we are always looking for solutions that can keep the network secure, but that do not require extensive support from our team,” says Carrie Peters, vice president of IT/IS, JOEMC.

To meet these requirements, JOEMC works with a variety of third-party vendors that provide technology, financial, and business services vital to the daily operation of the co-op. All vendors require access to the JOEMC network, ranging from periodic on-site visits to VPN links supporting managed services that must remain open at all times. Despite the number of outside parties that require access to the network, JOEMC lacked sophisticated tools to monitor and control vendor access. The safeguards that were in place (such as checking vendor PCs for viruses and malware before allowing them to connect to the co-op’s network) were also labor intensive and time consuming.

“I don’t think we have touched a computer because of spyware or malware since we went live with Cisco Security Agent.”

—Carrie Peters, Vice President of IT/IS

“We used a CD that ran multiple antivirus applications to scan vendors’ machines,” says Jay Carraway, senior network administrator, JOEMC. “But, we had to update the antivirus definitions and create a new disk every day. Between that process and manually scanning vendor machines, we could literally waste entire mornings.”

Despite having firewall and other network security products in place, viruses and malware could still attack employee PCs, and JOEMC’s small IT staff struggled to keep up.

“We would get complaints about pop-ups or systems running slow, and someone on our staff would have to literally sit in front of the machine to clean it,” says Peters. “You don’t have to have but a couple instances of that to know that time could be spent productively elsewhere.”

Since JOEMC handles customer credit card information daily, the organization also had to meet strict Payment Card Industry (PCI) security requirements. That meant developing a much more detailed view of what was happening on the network at all times, and implementing tighter controls over the transmission of customer financial information, neither of which could be accomplished easily with the existing network security infrastructure. JOEMC’s IT staff also struggled to keep up with PCI reporting requirements.

“For the PCI reporting process, we had to sift through syslog data from all of our network devices and parse it ourselves,” says Carraway. “It was cumbersome, labor intensive, and very time consuming.”

Ultimately, JOEMC needed more visibility into and control over the network and new mechanisms to automate manual tasks. The time had come to revamp the network security infrastructure.

Solution

JOEMC had used Cisco® routing, switching, and IP communications solutions for many years, but its previous-generation Cisco security solutions could not provide all the capabilities that the co-op now required. The organization needed state-of-the-art firewall and VPN solutions, a more sophisticated access control system, tools to lock down employee PCs and protect against malware attacks, and a comprehensive security monitoring solution. After evaluating options from multiple vendors, JOEMC leaders chose Cisco to support the entire network security overhaul. The organization appreciated the scalability and rich feature set of the Cisco solutions, but JOEMC’s past experience with Cisco played an important role in the decision as well.

“We worked with Cisco previously when we deployed unified communications, and if we ever had a problem, Cisco always came through,” says Carraway. “We could pick up the phone, and Cisco was here on-site with their very experienced engineers to help us solve a problem. We’re a relatively small business, but Cisco never pushed us aside. They have gone well beyond any other company that I’ve dealt with to make us happy.”

To assist with the network security upgrade, JOEMC turned to the co-op’s managed services provider, Priveon, a Cisco Premier Partner with extensive Cisco security expertise.

“For an implementation on this scale to succeed, you need a partner who knows the products that you are deploying and who understands your business and your priorities,” says Peters. “That’s what Priveon brought to this process.”

At the network perimeter, JOEMC replaced its older Cisco PIX® firewall and VPN concentrator solutions with Cisco ASA 5500 Series Adaptive Security Appliances. The appliances provide robust firewall protection and allow the co-op to carefully monitor traffic leaving the environment, as well

as potential threats trying to get in. With integrated IP Security (IPsec) and Secure Sockets Layer (SSL) VPN capabilities, the solution allowed JOEMC to replace two devices with one, simplifying network maintenance and reducing power consumption.

To streamline vendor access while strengthening control over vendor activity on the network, the organization deployed Cisco Network Admission Control (NAC). Cisco NAC authenticates any device attempting to access the network and helps ensure that it complies with organizational security policies, such as having the most up-to-date operating systems and antivirus software, which is also a PCI requirement. Along with the Cisco ASA 5500 Series appliances, Cisco NAC also allows JOEMC to place tight restrictions over which applications and network segments third-party users can access.

JOEMC next deployed Cisco Security Agent on all employee PCs to protect against malware and strengthen protection of customer data. Cisco Security Agent goes beyond conventional malware solutions by monitoring actual operating system behavior and blocking suspicious activity, instead of simply guarding against known attack signatures. Cisco Security Agent also serves as an ideal platform for enforcing JOEMC security policies, such as preventing the installation of unauthorized software and restricting the ways employees can copy or transmit protected financial information.

“You can use Cisco Security Agent to control virtually anything you can think of on a PC,” says Carraway. “We’re using it to lock down CD-ROM drives, flash drives, you name it.”

To serve as the nerve center for the new network defenses, JOEMC deployed the Cisco Security Monitoring, Analysis, & Response System (CS-MARS). CS-MARS provides JOEMC’s staff with intelligent tools to identify, correlate, and block security threats across the entire environment and maintain a real-time view of the security state of the organization at all times.

Results

Thanks to powerful new Cisco network defenses and expert integration and support from Priveon, JOEMC has established much tighter control over the network and automated or eliminated many labor-intensive tasks. The upgraded network defenses allow JOEMC to easily comply with security regulations and have boosted the overall security of the organization.

“The combination of CS-MARS, Cisco NAC, Cisco ASA, and Cisco Security Agent has given us better visibility into our network and a better understanding of how all ports and devices are being used,” says Peters. “We’ve been able to establish a baseline for normal activity, and we can quickly identify suspicious behavior.”

The new Cisco security infrastructure helps JOEMC comply with even the strictest PCI security requirements and has dramatically improved the logging and reporting process.

“We can bring information from our routers, switches, and security solutions, as well as all of our servers, directly into CS-MARS,” says Peters. “This allows us to see how traffic is traversing our network at all times, and we can dig into that data and identify any security gaps or ports we can close. As far as reporting, it would have taken days in the past to compile the kind of information we can now generate in a few moments with CS-MARS.”

With Cisco NAC and the Cisco ASA 5500 Series appliances, JOEMC also has implemented much tighter control over vendors accessing the network, while dramatically reducing the time it takes to provide that access.

PRODUCT LIST

Routing and Switching

- Cisco Catalyst 3560 Series Switch
- Cisco Catalyst 4500 Series Switch

Security and VPN

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco Network Admission Control (NAC)
- Cisco Security Agent
- Cisco Security Monitoring, Analysis, & Reporting System (CS-MARS)
- Cisco ACE Web Application Firewall

Unified Communications

- Cisco Unified Communications Manager
- Cisco Unified IP Phones 7900 Series
- Cisco Unity
- Cisco Unified Contact Center Express

Network Management

- CiscoWorks LAN Management Solution (LMS)

“In the past, once a vendor was authenticated on our network, we didn’t have many mechanisms other than passwords to restrict where they could go,” says Carraway. “Now, we can restrict access to specific segments or IP addresses, revoke access at any time, and control the way vendors transmit information. That allows us to, for example, require vendors to use encrypted channels to comply with PCI requirements. With CS-MARS, we can also generate detailed reports on everything vendors have done in our environment.”

One of the biggest changes that JOEMC IT employees have seen since upgrading the network defenses has been a reduction in malware, and a reduction in the resources required to deal with it.

“I don’t think we have touched a computer because of spyware or malware since we went live with Cisco Security Agent,” says Peters. “In fact, we are so

comfortable with Cisco Security Agent that six months after deploying it, we removed our enterprise anti-spyware solution.”

Cisco Security Agent also provides JOEMC IT staff with new capabilities to control how vendors and employees use the organization’s PCs and restrict new software installations.

“We have it configured so that users don’t even know it’s there,” says Carraway. “A vendor will try to install something on an employee machine, and it won’t work. They’ll call us to complain that something is broken, and we think, ‘Cisco Security Agent came through again.’”

Ultimately, JOEMC’s upgraded Cisco defenses have provided a robust, versatile platform for protecting vital applications and customer information, and meeting the growing demands of customers and regulators. And, thanks to the improved visibility and automation that the solutions provide, the organization’s small IT department can provide outstanding service to its employees and customers more efficiently than ever before.

Next Steps

In the coming months, JOEMC will continue upgrading its Cisco infrastructure, focusing on the unified communications system. JOEMC is in the process of replacing its previous-generation Cisco IP communications solution with Cisco Unified Communications Manager including Cisco Unity® unified messaging, and deploying a high-availability Cisco Unified IP Contact Center to provide more efficient customer service. On the security side, JOEMC plans to deploy the Cisco ACE Web Application Firewall to protect web applications from attacks such as identity theft, data theft, application disruption, and fraud. With its unique blend of HTML and XML security, the Cisco ACE Web Application Firewall also provides a compliance solution for the PCI DSS sections 6.5 and 6.6, which mandate the implementation of a web application firewall.

For More Information

To find out more about the 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 Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, 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, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, 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. (0805R)

Printed in USA

C36-486680-00 07/08