Case Study

Security Connected Strategy Supports Growing and Evolving Business

Eagle Rock Energy

Customer Profile
Upstream oil and gas producer with operations throughout the Southwest.

Industry
Energy/oil and gas.

IT environment
200 endpoints and 200 virtual servers spread across two data centers.

Challenge
Build a security infrastructure to meet requirements for midstream as well as upstream businesses in a SCADA environment.

McAfee solution
- McAfee® Advanced Threat Defense
- McAfee Enterprise Security Manager
- McAfee Network Security Platform
- McAfee Network Security Manager
- McAfee Web Gateway
- McAfee Email Gateway
- McAfee ePolicy Orchestrator® (McAfee ePO™) software

Based in Houston, Texas, Eagle Rock Energy Partners is an energy company focused on upstream activities, including oil and gas drilling, production, and development. Eagle Rock has working oil and gas properties and development opportunities in the midcontinent area, Permian, and southeast regions of Texas, as well as Oklahoma, Arkansas, Southern Alabama, Mississippi, and Louisiana.

Protecting the Company Brand

Led by Senior Network Engineer Anthony Hopkins, Eagle Rock's three-person network security team supports 200 users and 200 virtual servers across two major data centers in Dallas and Houston, as well as remote sites in Alabama, Oklahoma, Texas, and Arkansas. The security team's focus has changed slightly with Eagle Rock's recent divestiture of most of its midstream (gathering, processing, and pipeline) assets, which required high levels of security for supervisory control and data acquisition (SCADA) and process control network (PCN) systems at each plant. Hopkins' team is still responsible for one midstream plant, and a current project involves bringing that plant's SCADA PCN into the corporate security environment.

In addition, the team manages corporate network security and network traffic for business functions, such as accounts payable, which requires compliance with PCI security guidelines. The security engineers are also working to bring active remote drilling rigs onto the network in order to extend security to those operations.

"Our approach may have shifted away from the SCADA PCNs, but we still have the same basic security priorities—namely, maintaining control of our network and protecting it from advanced malware threats. Also, since we're bringing one of the midstream plants onto our corporate network, we're opening up to a host of new security threats," Hopkins notes. "Plant devices are exposed to a lot of risk, such as sabotage that could cause an outage or uncontrolled situation. When those controls are hooked into our infrastructure, we have a real burden to prevent a security breach that could lead to an unforeseen event. It really comes down to protecting our brand name, which could be significantly damaged by such a breach."

Previously, Eagle Rock relied on solutions from multiple vendors for SIEM, endpoint, and network security. While offering fair insight into the security posture of the network, the previous SIEM solution was neither flexible nor easy to configure. Eagle Rock wanted to strengthen its current security infrastructure in order to position it well for the future, in the event that the company acquires additional upstream assets that could include another midstream asset that expands the presence of plant controls on the network. "It's all about maintaining the same mindset that we've always had regarding our security posture," Hopkins comments.

intel Security

Results

- Integrated security architecture paves the way for business expansion.
- Comprehensive threat detection ensures that security events from every source are noted and logged.
- The combination of McAfee Web Gateway and McAfee Advanced Threat Defense thwarts inbound threats from the Internet.
- Intrusion prevention monitors both external and internal activity.

McAfee Solution

As a long-time McAfee customer, Eagle Rock is addressing these requirements with a powerful new suite of McAfee security management and networking security solutions. The cornerstone is McAfee Advanced Threat Defense, providing advanced protection from today's stealthy, zero-day malware by finding zero-day threats and then notifying McAfee Network Security Platform (including IPS appliances), McAfee Email Gateway, and McAfee Web Gateway to freeze the spread of infection and prevent further infiltration. Another critical link in the strategy is McAfee Enterprise Security Manager, part of the security information and event manager (SIEM) solutions family, aggregating event, threat, and risk data to provide strong security intelligence and rapid incident response. In addition, Eagle Rock is currently deploying McAfee Deep Defender, next-generation hardware-assisted endpoint security solution co-developed with Intel.

McAfee Network Security Manager (part of McAfee Network Security Platform) provides centralized control over distributed network security appliances, while McAfee ePO software enables visibility and comprehensive management of the entire integrated security environment.

The Security Connected framework gives Eagle Rock a unified framework for integrating partner solutions such as ForeScout Network Access Control (NAC), as well as other components in the McAfee security suite.

Letting No Security Event Go Undetected

At Eagle Rock, all network-generated information, including syslog data from routers and switchers, NetFlow data from routers and firewalls, and data from McAfee ePO software and IPS appliances is fed into McAfee Enterprise Security Manager. In addition, SIEM agents are deployed to all servers in Eagle Rock's DMZ to capture Microsoft Windows logs and events. The SIEM system is even able to capture logs and events from Microsoft Office applications, including SharePoint, Exchange, and SQL Server databases. "Basically, no event gets through without being logged by the SIEM—including events from any server that has user interaction or plays a critical high-end role, such as running key financial databases and anything that has outward logging capabilities," Hopkins explains. "We're now analyzing up to 6,000 events per second, so we're very confident that we're catching anything that could be a potential threat. McAfee Enterprise Security Manager gives us that confidence."

Holistic Threat Defense

Another example of the integrated McAfee strategy is McAfee Advanced Threat Defense, which has been deployed throughout the Eagle Rock environment. "We looked at many solutions and chose McAfee Advanced Threat Defense for its ease of use and also the fact that it's a holistic system that works seamlessly in our environment—unlike competing products that operate as isolated stovepipes. That integration is a huge advantage," Hopkins notes. "With SCADA PCN, a large concern is the ability to manage advanced proficient rights and keep a close eye on every file coming across from plant devices, and McAfee Advanced Threat Defense meets those requirements nicely."

For inbound malware scanning from websites, Eagle Rock leverages the integration of McAfee Web Gateway and McAfee Advanced Threat Defense. When a user downloads content from a website, McAfee Web Gateway performs a malware analysis. If a suspicious file can't be convicted by McAfee Web Gateway, it is passed to McAfee Advanced Threat Defense for full investigation and deconstruction in its "sandboxes," using both dynamic and static code analysis. If McAfee Advanced Threat Defense finds malicious content, it issues an alert so that integrated solutions and IT staff can take action. "At first, we thought McAfee Advanced Threat Defense wasn't working because nothing was coming to it, but then we realized that McAfee Web Gateway was working so well at capturing inbound threats that not much was being sent to McAfee Advanced Threat Defense," Hopkins remarks. "The content of what users are downloading or receiving in email is a huge concern, and the internal malware analysis provided by McAfee Web Gateway working together with McAfee Advanced Threat Defense takes our security posture to a new level."

"The ability to manage the entire environment from a single ePO interface is priceless. The Security Connected vision addresses broad security challenges with best practices to help us minimize the total cost of ownership in the technology. With McAfee, we're able to continue expanding a security infrastructure that will serve our business well into the future."

——Anthony Hopkins, Senior Network Engineer

Internal and External Intrusion Prevention

Eagle Rock has deployed two pairs of McAfee NS-9100 IPS appliances, one pair at the Houston data center and the other pair in the Dallas facility. In both Dallas and Houston, the IPS systems are linked to internal firewalls within the DMZ and are also connected via Metro Ethernet to the company's colocation facilities. The IPS also scans MPLS connections out to remote sites, as well as SIP connections for voice services. "Every outbound link in our facilities has an IPS scan on it, so we are monitoring both internal and external activity," Hopkins explains.

Betting the Future on Security Connected

Eagle Rock's McAfee footprint is continuing to expand. Soon, the company will roll out McAfee Host Data Loss Prevention, McAfee Deep Command, McAfee Endpoint Encryption, and McAfee Drive Encryption. "The ability to manage the entire environment from a single McAfee ePO interface is priceless," Hopkins summarizes. "The Security Connected vision addresses broad security challenges with best practices to help us minimize the total cost of ownership in the technology. With McAfee, we're able to continue expanding a security infrastructure that will serve our business well into the future."

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

61428cs_eagle-rock_1014_ETMG