CASE STUDY

McAfee Helps Colorado Adopt New Controls for Tighter Cybersecurity

Immediate and Effective Remediation with McAfee SIEM

State of Colorado

Customer Profile
Information Technology for the State of Colorado

Industry
State and local government

IT Environment
27,000 nodes and 16 departments

Having a limited budget and resource constraints, the State of Colorado turned to McAfee's SIEM solution to meet compliance standards.

When Jonathan Trull took on a new position as chief information security officer (CISO) for the Governor's Office of Information Technology (OIT) in Colorado, he inherited some challenges, starting with funding shortfalls and overly burdensome security controls. "I came into the job with a $6,000 budget for IT security for the whole state," said Trull of the task he took on in 2012, after serving for years as Colorado's deputy state auditor.

But the lack of budget was only part of the challenge in revamping the governor's IT security department. Also problematic was the existing security control framework—the NIST 800-53, a long document with guidelines that were tough to fully implement given the OIT staff and budget available. Trull wanted to turn the resource allocation on its head. "Instead of focusing 80% of our time and resources on compliance with regulations such as PCI and HIPAA and 20% on real security risk improvement, the idea was to flip that," explained Trull. "And—while complying with regulations—spend 80% of our time using technical resources that are the most effective in stopping information from being compromised. I knew if I could get the money and the tools, I could achieve greater risk reduction."

Following the Customer's Needs: Situational Awareness

After successfully convincing the executive and legislative branches to provide funds to tighten security, Trull started looking for tool sets to help him accomplish his goals. "From my position, what I seek more than anything is situational awareness in real time. I want to know the current state of my systems, who is attacking them, and how and what their level of compliance is with our security configuration. What I needed was a way to roll up that collected information into one pane of glass," said Trull. "The only product I found that met all of my criteria and allowed that data to seamlessly integrate into one dashboard was McAfee."

His decision to engage McAfee products and personnel meant successful deployment of streamlined controls and better practices that make the state safer from cyberattacks.

Challenge

Prove compliance with HIPAA and PCI by adopting Council on CyberSecurity Security Controls with limited budget and resources

McAfee Solutions

- McAfee® ePolicy Orchestrator® (McAfee ePO™)
- McAfee Enterprise Security Manager
- McAfee Enterprise Log Manager
- McAfee Advanced Correlation Engine
- McAfee Event Receiver
- McAfee Network Security Platform

Results

- Aggressively achieved first five controls per set goal
- Ability to administer virus scans and obtain software inventory with McAfee ePO software
- Vulnerability ranking within McAfee Enterprise Security Manager allows for more immediate and effective remediation

Tackling the Council on CyberSecurity Top 20 Critical Security Controls

Using McAfee technologies, OIT implemented the first five

1 Inventory of all network devices

Both authorized and unauthorized, removing unauthorized devices within 48 hours of discovery. McAfee Asset Manager, McAfee Rogue System Detection, and McAfee ePO software for discovery and inventory of network devices.

2 Inventory of all authorized and unauthorized software

The latter, including media players, peer-to-peer, and malicious software. McAfee Application Control to control the inventory of software that is approved to run on computers. McAfee ePO software to control risk and application reputation from McAfee Global Threat Intelligence.

3 Establishing secure standard configuration of devices

McAfee Application Control and McAfee Policy Auditor for Center for Internet Standards benchmarks.

4 Vulnerability remediation assessment

McAfee Policy Auditor to scan the endpoints.

5 Malware defense

McAfee VirusScan® engine on endpoints.
McAfee Web Gateway to block sites known to deliver malicious payloads.

Focusing on Critical Security Controls

OIT adopted the Council on CyberSecurity's Top 20 Critical Security Controls as its new structure for 90% of the state's IT security, starting with the first five controls. The McAfee team took inventory of the technologies the state already had, and then made a grid showing gaps and what needed to be done to move the project towards the customer's goal. A deal was struck: a 50/50 combination of products and three years of on-site professional consultation. The contract also included flexible McAfee product licensing. The State of Colorado selected technology consisting of 15 products to address the Top 20 Critical Security Controls and its security project goals. OIT wasn't ready to implement and/or use all of the tools on day one, but the deal structured by McAfee made the decision easy, and OIT knew all of the tools would eventually be needed as the project progressed.

"We went full in with McAfee to implement the first five controls, which are heavy lifts in themselves," Trull said. "I wanted to ensure that we were in this together. The goal was to achieve the five controls within the timeframe we wanted—to really get the ball rolling, get the hardware and networking installed and build the human processes into these tools. I pushed them hard. The timeline was very, very difficult, but it worked."

Additional McAfee solutions

- McAfee Application Control
- McAfee Change Control
- McAfee Complete Endpoint Protection—Enterprise suite
- McAfee Data Center suite
- McAfee Database Activity Monitoring
- McAfee ePO Deep Command
- McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus
- McAfee Policy Auditor

"The only product I found that met all of my criteria and allowed that data to seamlessly integrate into one dashboard was McAfee."

—Jonathan Trull, Chief Information Security Officer, State of Colorado

Better Information Aids Better Decision-Making

McAfee ePO software enables the team to administer everything from virus scans to the agent that pulls inventory for software and more. It's the central nervous system that ensures everything is working and that critical data is flowing in from every vertical source. "[McAfee] Enterprise Security Manager is the aggregator and correlator of all that data," Trull said. "Whatever threats, whatever viruses that hit us feed into ESM [McAfee Enterprise Security Manager] through the [McAfee] Network Security Platform, firewalls and [McAfee] Vulnerability Manager. Our SIEM helps us make sense of it all and make better decisions."

Once identified, those threats require immediate remediation. In the past, there were high, medium, and low vulnerabilities, and

OIT tried to patch everything. Now, if the SIEM identifies something as a high vulnerability, OIT knows there is an active threat against it and the threat rises to the top of the team's remediation efforts. "The McAfee tools help us with situational awareness, key decision-making, allocation of resources, and—very importantly—help us decide where we spend our precious time. I'm extremely satisfied," concludes Trull.

"Whatever threats, whatever viruses that hit us feed into ESM [McAfee Enterprise Security Manager] through [McAfee] Network Security Platform, firewalls and [McAfee] Vulnerability Manager. Our SIEM helps us make sense of it all and make better decisions."

—Jonathan Trull, Chief Information Security Officer, State of Colorado

McAfee
Together is power.

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

61599cs_state-of-colorado_1214
DECEMBER 2014