Case Study

CDCR Streamlines Security Management with "Security Connected" Strategy

California Department of Corrections and Rehabilitation (CDCR)

Customer Profile
Operates California state prison, parole, and rehabilitation systems.

Industry
Public sector.

IT environment
700 servers and 29,000 endpoints across 37 locations.

Challenge
Protecting sensitive data over a wide security landscape with limited staff.

McAfee Solution
- McAfee Network Security Platform
- McAfee Enterprise Security Manager
- McAfee Enterprise Log Manager
- McAfee Advanced Correlation Engine
- McAfee Event Receiver
- McAfee Complete Data Protection
- McAfee Risk Advisor
- McAfee Vulnerability Manager
- McAfee ePolicy Orchestrator
- McAfee Complete Endpoint Protection Enterprise
- McAfee Platinum Support
- McAfee Deep Defender

Results
- Compliance with policy standards.
- Dashboards enable centralized security management and provide easy access for executive reporting.

The California Department of Corrections and Rehabilitation (CDCR) oversees 34 state adult prisons and three juvenile facilities, a variety of community correctional facilities, and all adult and juvenile parole systems within the state. The department employs approximately 57,000 people and is one of the largest state government departments in the United States. CDCR's Enterprise Information Services (EIS) division is tasked with managing CDCR's information security program. EIS is responsible for securing information for all adult and juvenile institutions across the state, including parole units, and for supporting information systems with minimal impact to the business operations.

Business Trigger: A Layered Approach to Protecting Sensitive Information Across a Complex Landscape

EIS has the responsibility of protecting personal data for CDCR personnel and the inmate population in an environment that includes multiple data centers, more than 700 servers located across the state, 29,000 endpoints, and the network. CDCR has to comply with California state regulations for securing and protecting information. If the information involves the federal Criminal Justice Information System, federal rules might also apply.

CDCR manages sensitive and confidential data, including information on gang activity and victim records. The CDCR environment includes multiple complex and cross-functional "Big Data" environments, so internal and external networks need to be protected and secure. Security safeguards, like encryption, are critical to enforcing security policy. Nowadays, damages resulting from security vulnerabilities can lead to damaged reputation, safety issues for inmates, families and prison staff, and legal liability. "We take maintaining the availability and integrity of our systems very seriously," explains Joe Panora, director of EIS.

Solution Focus: Centralized, High Performance Security and Risk Management

With more than 29,000 endpoint devices, correlating log data to identify security events became unfeasible. Turning to the McAfee® Enterprise Security Manager security information and event management (SIEM) solution provided CDCR with a centralized solution that would help identify security violations and risk issues quickly.

"We are able to centralize everything with McAfee ESM [Enterprise Security Manager]," explains agency information security officer Scott MacDonald. When the team had to perform an investigation in the past, a staff member would have to log into each server manually to identify server activity because log data wasn't centralized. Furthermore, there wasn't enough storage on the servers, so the logs would roll over after one and one-half days.

With McAfee Enterprise Security Manager, the servers have sufficient storage to hold log data for six months to a year. CDCR is able to go back in time to see logon activity or identify a malware issue because they can see activity by one user account on multiple devices across the state. McAfee Enterprise Log Manager and McAfee Advanced Correlation Engine consolidate and automatically correlate log information from CDCR's servers, firewalls, and proxies. "We are able to obtain actionable information," says MacDonald. "We can correlate between firewalls and endpoint devices to identify activity."

Collective Protection for Network-Connected Devices

To achieve true perimeter security, McAfee Network Security Platform, coupled with McAfee Enterprise Security Manager, enables the agency to organize multiple security technologies to collectively discover and block threats to CDCR's

intel Security

"By taking advantage of the McAfee suite of products, managing security has been a big cost avoidance."

—Scott MacDonald, Agency Information Security Officer

network. CDCR was able to take advantage of this in the past year to block risks to the organization, such as peer-to-peer file sharing, Skype, and Bit Torrent-type traffic. Though it is not normally easy to block this type of activity with firewalls, McAfee Network Security Platform gives IT the ability to identify certain type of traffic that has been disallowed and then shut it down.

McAfee Network Security Platform also provides buffer overflow protection as CDCR transitions from Microsoft Windows XP to Microsoft Windows 7, providing protection against browser vulnerabilities.

CDCR has also adopted McAfee Risk Advisor. "If you're aware of the products and information in your environment, it's straightforward to identify a missing patch. [McAfee] Risk Advisor accounts for all the services that you're running in the environment and correlates threat feeds with vulnerability and countermeasure information to score the true risk to the organization. That has a lot of value," says MacDonald.

Reduced Workload and Improved Visibility Streamlines Security Management

CDCR invested in McAfee technologies to reduce complexity and streamline security management while improving visibility into the environment. The team uses McAfee® ePolicy Orchestrator® (McAfee ePO™) software to centrally manage CDCR's security posture. McAfee Complete Endpoint Protection is CDCR's antivirus threat handler for known malware signatures, including spyware, adware, viruses, Trojans, worms, and pre-identified unwanted software (for example, key loggers and password crackers). CDCR takes advantage of McAfee ePO software's automatic remediation capability to automatically delete, clean, or quarantine systems that don't meet policy compliance standards.

When previously faced with a malware situation, the team would have to send local IT staff to the site to work on the system. Now they are able to configure the McAfee antivirus scanning engine with rules to perform the remediation automatically. It has reduced the workload and provided cost avoidance in the amount of approximately half a million dollars over the last two years because CDCR no longer has to send staff out to perform manual updates. CDCR credits its ability to proactively isolate and remediate attacks to the Security Connected framework, which has resulted in far less staff downtime and improved employee productivity.

The team uses McAfee Vulnerability Manager to automate scans that go out to all systems, workstations, and servers on a monthly basis for security patching, to keep policy violations in check, and to meet compliance standards. It verifies the Microsoft System Center Configuration Manager (SCCM) environment. CDCR also uses McAfee Vulnerability Manager to scan database servers or a single host, like a website, to check for vulnerabilities.

Figure 1. Incident management.

Host defense is accomplished by deploying McAfee Complete Data Protection, which provides encryption for laptops, safeguarding confidential information on devices that are prone to loss or theft. McAfee Host Data Loss Prevention (McAfee Host DLP) monitors the environment to protect against data leakage of confidential information. CDCR has been able to lock out USB drives, and this has significantly decreased the number of viruses in the environment. The department also uses McAfee Host DLP for situational awareness to protect users or for notifications. For example, if someone is sending confidential information, such as a spreadsheet with Social Security numbers, to someone outside the network, users can be notified and continuing activity monitored.

McAfee Powers Security Metrics Dashboards

McAfee technologies helped CDCR create a dashboard to display high-level success metrics "at-a-glance" to division and department executives. The dashboards are accessible from CDCR's Microsoft SharePoint 2010 platform.

"With such a small staff, relative to the size and complexity of our organization, we needed a centralized solution that lets us automate as much of the environment as possible," concludes Panora. "With McAfee, we can integrate our security solutions and create a comprehensive security overview while reducing staff workload. Using the Security Connected framework supports our overall strategy of reducing staff resources for manual virus activity. Security isn't a cost savings, but by taking advantage of the McAfee suite of products, managing security has been a big cost avoidance."

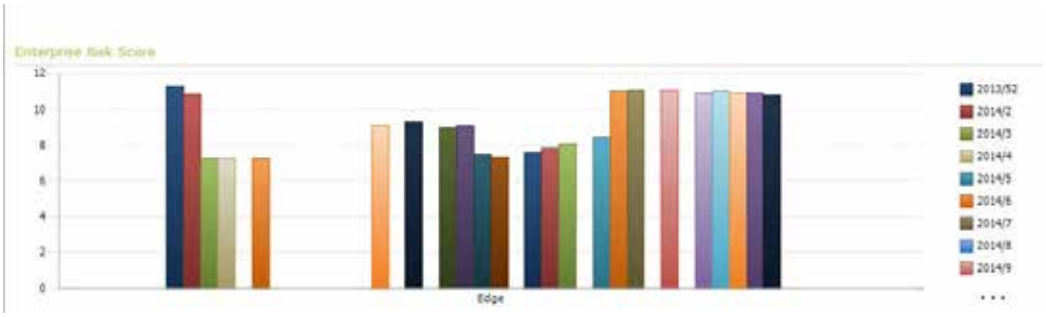

Figure 2. Vulnerability scan.

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

61540cs_cdcr_1214_ETMG