Case Study

Chicago Protects Critical Infrastructure and Services with Security Connected

City of Chicago

Customer Profile
Third largest city in the US by population, with almost three million residents.

Seventh largest city in the world by GDP.

Industry
State/local government.

IT environment
All departments, including critical infrastructure within water and aviation.

Challenge
Protect citizens from advanced, multilevel cyberthreats.

McAfee solution
- McAfee ePolicy Orchestrator® (McAfee ePO™) software
- VirusScan® Enterprise
- McAfee Endpoint Encryption
- McAfee Host Intrusion Prevention for Desktops
- McAfee Change Control
- McAfee Enterprise Security Manager (SIEM)
- McAfee Risk Advisor
- McAfee Network Security Platform
- McAfee Web Gateway
- McAfee Vulnerability Manager
- McAfee Advanced Threat Defense

The City of Chicago's recently formed Information Security Office (ISO) is charged with overseeing cybersecurity across all areas of the city, including critical infrastructure within the water, aviation, and public safety departments. Under the leadership of Chief Information Security Officer Arlan McMillan, the ISO has accomplished a great deal:

- Built the city's first information security office.
- Chartered, revamped, and expanded city-wide information technology and security policies.
- Created a security education and awareness program.
- Built 12 security services designed to meet the needs of individual departments.

These services include perimeter security, threat and vulnerability management, continuous security monitoring, and incident response, leveraging a variety of McAfee® solutions as part of their core delivery.

Closing a Security Gap

Like all large US cities, Chicago has a significant amount of critical infrastructure that requires protection. The water department supplies fresh water to more than 44% of the residents of Illinois, and the aviation department manages Chicago O'Hare and Midway airports, respectively the country's second- and thirty-second-busiest. The prominence of these departments makes them attractive targets for would-be sabotage, especially resulting from a compromised IT network.

"The US government now identifies cyberattack as the number one threat to the nation's security," McMillan explains. "Our mayor, Rahm Emanuel, understands these risks on a national level based on his former position as Chief of Staff for the Obama administration, so he had the leadership and foresight to recognize that Chicago needed a dedicated focus on security."

With the creation of the ISO, the City of Chicago sought a comprehensive and integrated suite of security solutions to protect all IT resources serving critical infrastructure departments.

McAfee Solution

"The days of isolated systems that don't talk to each other might have been adequate before, but the tremendous amount of data in the network today makes it impossible for human analysts to identify threats in a timely manner. All systems have to be highly integrated and informing each other of potential threats," McMillan relates. "And like most government organizations, we'll always be constrained by staff resources—both in the number of people we need to get the job done and people with the right skill sets."

intel Security

Results

- Maximized staff resources.
- Malware incidents reduced by 2,000%.
- Centralized management and analysis.
- Integrated security event logging that captures events throughout the environment.

These factors made the ISO an ideal candidate for the Security Connected strategy. "Of the different solutions we considered, only McAfee has a complete toolbox that we can leverage in an integrated way. That's why we chose to standardize on McAfee," McMillan adds.

For endpoint protection, the ISO has installed VirusScan Enterprise for Windows and UNIX. McAfee Endpoint Encryption protects mobile users' laptops, and the ISO is currently installing McAfee Host Intrusion Prevention for Desktops. McAfee Change Control protects a select group of higher-sensitivity servers.

On the network side, ISO has deployed a full complement of McAfee solutions, including McAfee Enterprise Security Manager, McAfee Risk Advisor, the McAfee Network Security Platform, McAfee Web Gateway, and McAfee Vulnerability Manager. ISO is also currently deploying McAfee Advanced Threat Defense, which will be integrated with McAfee Web Gateway and McAfee Network Security Platform.

Tying it all together is McAfee ePO software, which provides a centralized dashboard for controlling, managing, and analyzing the entire McAfee ecosystem within the ISO.

The ISO makes extensive use of McAfee Professional Services, including a dedicated Resident Support Account Manager (RSAM) who works onsite to help the ISO team deploy and tune the integrated solutions. "With our resource constraints, both in head count and skill set, our RSAM plays a critical role in helping us optimize our security infrastructure," McMillan comments.

Comprehensive Logging and Intrusion Prevention

The City of Chicago ISO is now logging and managing more than 10,000 events per second with McAfee Enterprise Security Manager, and the number is expected to double by the end of the year. The first SIEM priority is to track security events from firewalls and other systems in the critical infrastructure, including the water and aviation departments. The ISO is also targeting departments with regulatory requirements, including PCI and HIPAA and all criminal justice information systems. Through integration with other key McAfee solutions, McAfee Enterprise Security Manager collects and logs security events from every critical security device. This includes about a dozen IPS devices deployed at strategic locations in the critical infrastructure network.

"McAfee SIEM is a large step forward for the city," relates Paul Bivian, security architect and manager for the ISO. "Before, we had small deployments of another SIEM solution that were very targeted and isolated, and they were focused on operations rather than security. Now, we'll be able to log and manage every security event from every device in each department to give us a comprehensive picture of the overall security environment."

Tightening Up Vulnerabilities

In addition, the ISO has deployed the McAfee Vulnerability Manager scanning appliances throughout the city. When McAfee Vulnerability Manager identifies a security vulnerability within a particular department, the ISO works with the system owners to understand and rank the vulnerability and then remediate it as required—both incidentally and during scheduled scans.

"With the improvements in patch management and validation provided by McAfee Vulnerability Manager, the tuning we've done to VirusScan on the endpoints, and improvements to our scanning schedule, I can say that we've been able to reduce identified malware in our environment by more than 2,000%," McMillan relates. "With McAfee Vulnerability Manager checking that patches were deployed effectively, in addition to the ad hoc and pinpointed vulnerability checks it performs against critical systems, we've been able to reduce malware incidents from tens of thousands to practically none."

"An integrated security architecture is critical not only to our ability to proactively identify and react to threats, but also to magnify a limited workforce as much as possible. The Security Connected vision and strategy was an ideal fit with our own."

—Arlan McMillan, CISO/HIPAA Security Officer

One Pane of Glass to Simplify Management

Both the ISO and its outsourced IT provider are able to access the central McAfee ePO console to view the entire security infrastructure and generate reports to support compliance. "[McAfee] ePO's reporting and analysis tools save a tremendous amount of time. In an instant, we can analyze events and determine version and update status for each device," Bivian says. "[McAfee] ePO's integration with other tools such as a network security platform means we don't have to query each system or take extra steps to spot events or identify threats."

Security Connected for Comprehensive Protection

In creating the ISO, the City of Chicago has had an opportunity to build a "greenfield" security architecture that will offer comprehensive protection for the critical infrastructure and departments that serve every resident—especially as cyberthreats continue to grow in number and sophistication.

"With malicious traffic becoming ever more complex and multilevel, there's far too much data to analyze security events independently or with manual techniques. The only road ahead is to leverage technologies that can work together to do the heavy lifting of analyzing and neutralizing threats," McMillan says. "Therefore, an integrated security architecture is critical not only to our ability to proactively identify and react to threats, but also to magnify a limited workforce as much as possible. The Security Connected vision and strategy was an ideal fit to our own."

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

61427cs_city-of-chicago_1014_ETMG