Case Study

McAfee Enterprise Security Manager Delivers Managed Security Services for the Provincial Government of New Brunswick

Government of New Brunswick

Customer profile
Network of agencies serving the 750,000 citizens of New Brunswick, Canada.

Industry
Provincial government.

IT environment
Provides Managed Security services for 33 departments and agencies.

Challenges

- Manual, decentralized security incident response.
- Lacking consolidated, correlated event management.
- Scale out managed security services across 33 departments.

The Government of New Brunswick (GNB) administers 33 departments and agencies providing the full range of government services for more than 750,000 citizens. Through its centralized security event management center (SEMC), Jamie Rees, director of information assurance and chief information security officer, manages a three-person team to provide a tiered program of managed security services for all public departments and agencies.

Business Challenge: Limited Security Visibility

When taken as a whole, GNB represents a very large and successful deployment of McAfee® security solutions. Most of the departments are running several, including McAfee antivirus and endpoint encryption solutions, McAfee Host Intrusion Prevention, McAfee Firewall Enterprise, and McAfee Web Gateway and McAfee Email Gateway. Small departments might be completely reliant on Rees and his team for security monitoring, while large departments may have their own IT staff and security tools, along with McAfee ePolicy Orchestrator® (McAfee ePO™) software to provide a centralized dashboard from which to manage virus definition updates and gain visibility into security issues.

With so much variation in security systems and networks, as well as size and staff within the departments, getting the whole picture of security incidents and malware threats throughout the environment had become a major challenge for the SEMC. Previously, for each security incident, the SEMC staff would have to call multiple system administrators and ask them to check their logs, and then manually correlate all of the data to gain a broader insight on the threat. Not only was this very time-consuming for the small IT team, but often engineers would have to physically go out and check desktops for infection. GNB needed a security information and event management (SIEM) solution.

Why McAfee: Comprehensive and Cost-Effective SIEM Solution

GNB published an RFP with a highly detailed list of requirements for a new SIEM solution. At the top of the list was centralized administration and the ability to integrate well with every security product in use by all of the departments—whether McAfee, a part of Intel Security, or from another vendor. GNB also sought a modular solution that would support a tiered service model and scale easily by adding components over time.

Of the SIEM vendors evaluated, only McAfee could meet all of GNB's compatibility, modularity, and budgetary requirements. "McAfee was able to provide a comprehensive solution without charging extra for features we needed, which come standard in the McAfee SIEM lineup," says Rees. "Like all government organizations, we have a limited budget and have to plan expenditures carefully. We needed a solution that could enable us to expand our footprint logically from year to year as the budget and needs require. McAfee's modularity enables us to better estimate our costs and budget for ongoing expansion."

intel Security

"Based on our excellent long-term relationship with McAfee, we knew we could count on the support team to help us be successful with the SIEM solution. They worked with us to create an extensible architecture that makes it extremely easy to deploy the system in virtually any security environment we might find in one of our departments."

—Rick Ouellette, Deputy CIO, Executive Council Office, Government of New Brunswick

McAfee solutions

- McAfee Enterprise Security Manager
- McAfee Enterprise Log Manager
- McAfee Advanced Correlation Engine
- McAfee Event Receiver
- McAfee ePolicy Orchestrator

Results

- 95% reduction in the time required to resolve workstation issues.
- A modular solution that supports a limited budget and a tiered SIEM service offering.
- Compatibility with all security data-generating devices throughout the broader organization.
- Greater accountability to key stakeholders.

The McAfee SIEM Solution

The GNB security environment now includes two McAfee Enterprise Security Manager devices, McAfee Advanced Correlation Engine, and two McAfee Enterprise Log Manager appliances. In addition to supporting internal security for the Executive Council Office, these components enable the SEMC to offer four tiers of SIEM services to the department ranging from a complete build-out on the department's network, to simple deployment of an event receiver, in which the SEMC's own "manager of managers," McAfee Enterprise Security Manager, collects and correlates the department's security event data.

Even for the larger agencies with their own McAfee Enterprise Security Manager deployment, the SEMC is able to pull event data from any type of network device including routers and switches, servers, firewalls, intrusion detection systems, Windows event logs from directories, and the departmental instances of McAfee ePO software. For one of GNB's largest service agencies, the SEMC McAfee Enterprise Security Manager is collecting logs and information on at least 700 devices. "If it's a security-related device deployed somewhere in the ecosystem, we're taking feeds from it," Rees remarks.

"We strive to continuously improve corporate IT governance, to enable the business of GNB," says Rick Ouellette, GNB's deputy CIO. "With this project, our goal was to improve the view into GNB-wide security events while at the same time leveraging existing security solutions."

Real Productivity Improvements

With McAfee Enterprise Security Manager, the SEMC team no longer has to manually collect and correlate event data from multiple departments. Now, with the SIEM automatically pulling and correlating data from devices throughout the GNB ecosystem, the team is able to access the information instantly from its central location, generate detailed reports that identify events of concern that should be elevated, and then work remotely with the involved departments to quickly implement a fix. This means that team members are spending 95% less of their valuable time having to physically attend to workstations in the GNB field. "I'm lucky to have a talented and inquisitive staff, and they're very good at identifying and researching potential threats that might impact multiple departments or even affect national security," says Rees. "With McAfee Enterprise Security Manager, they can spend more of their time working on projects that have more strategic value to our organization," Rees explains.

"Clients have expressed appreciation of that value. [SEMC's] expertise and recommendations were key factors in getting the business approval to put in place proper proactive measures, people and process to move through the various stages of security in order to secure our network and digital infrastructure," says Marc-André Arseneau, IT Infrastructure Manager of Collège communautaire du Nouveau-Brunswick.

"Very early, we were able to tune up McAfee ESM [Enterprise Security Manager] to help determine if any potential exploit traffic was infiltrating our network. This was a huge boon to our operation because it enabled us to be proactive and have mitigations and workarounds in place before Heartbleed ever became a threat, and we could show management that we were well-prepared."

—Jamie Rees, Director of Information Assurance and CISO, Executive Council Office, Government of New Brunswick

Proactive and Accountable Security Management

GNB also leverages the McAfee SIEM solution to monitor internal security operations and proactively head off malware for the Executive Council Office. One recent example was the Heartbleed open SSL virus that threatened many users of secure web servers. "Very early, we were able to tune McAfee Enterprise Security Manager to help determine if any potential exploit traffic was infiltrating our network," Rees relates. "This was a huge boon to our operation because it enabled us to be proactive and have mitigations and workarounds in place before Heartbleed ever became a threat, and we could show management that we were well-prepared."

Rees adds that accountability to upper-level executives and GNB's executive council is one of the key benefits of McAfee Enterprise Security Manager because it's so easy to generate reports and demonstrate the system's effectiveness. "I can log into the SIEM from my iPad and show stakeholders—including the CEOs and CIOs of the departments—how well the solution is working throughout the province," he says. "We're building thought leadership throughout the Atlantic Provinces, and it's all possible because of McAfee Enterprise Security Manager."

A Long-Term Security Partner

"Based on our excellent long-term relationship with McAfee, we knew we could count on the support team to help us be successful with our SIEM solution," Ouellette says. "They worked with us to create an extensible architecture that makes it extremely easy to deploy the system in virtually any security environment we might find in one of our departments."

"With McAfee SIEM, we have the ability to generate comprehensive and up-to-the-minute data about our overall security situation, but without the right team, data is just data. We have a fantastic group of security professionals working at all levels in our government, and McAfee SIEM solutions help them use their skills to the utmost to keep our entire network safe," Rees concludes.

intel Security

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

61218cs_govt-new-brunswick_0714B_fnl_ETMG