CASE STUDY

McAfee™
Together is power.

Canadian Retailer Embraces an Integrated Defense

Detection and response shrinks from days and weeks to minutes

Liquor Control Board of Ontario

Customer profile
One of world's largest retailers of beverage alcohol

Industry
Retail

IT environment
5,000 endpoints across 650 stores and corporate headquarters

Built upon a McAfee® integrated security platform, this Canadian retailer's adaptable threat defense infrastructure allows its small information security team to efficiently and effectively manage security, including finding and responding to cyberthreats in minutes across its extended enterprise.

One of the world's largest buyers, retailers, and wholesalers of beverage alcohol, the Liquor Control Board of Ontario (LCBO) operates 650 retail stores across the Canadian province. In addition to its brick and mortar stores, the government-owned agency also offers e-commerce and mobile purchasing, enabling customers to order via desktop or smartphone and have purchases delivered to homes, businesses, or local stores. Each store has a point-of-sale server, plus two to ten cash register terminals, for a total of approximately 5,000 endpoints across Ontario.

Greater Value and Better Protection than MSP

Always looking to maximize value, LCBO was searching for a new managed security provider to provide better security services. "As we looked at managed service providers (MSPs), we came to the realization that we could get more value with our own high-quality staff and the right tools," recalls LCBO Director of Information Security Simon Brown, who oversees a small information security team and reports directly to the organization's CIO. "Plus, we would no longer have to rely on external businesses that will never know our business as well as we do."

Because it has a very lean security staff, LCBO desired efficient, easy-to-use security solutions. Although Brown liked the ease of use of the McAfee® ePolicy Orchestrator® (McAfee ePO™) console, which his team relies on to manage McAfee endpoint protection as well as McAfee Endpoint Encryption and McAfee File and Removable Media Protection, he had not seriously considered McAfee ePO software as a means of managing other enterprise security solutions until a new push for standardization came from his CIO.

Together, Brown and his team looked more closely at the integrated security approach touted by McAfee, an approach that could enable the superior in-house defenses they sought, enabling them to eliminate the MSP. "It was at that point we began to view McAfee as a strategic partner," recalls Brown.

Strategically Rolling Out an Integrated Threat Defense Architecture

"Because of the McAfee integrated security platform—the way all its solutions work together and enhance each other—it made total sense to leverage our existing McAfee endpoint environment and McAfee ePO software," notes Brown. First the LCBO team consolidated the five instances of McAfee ePO software into one production console and one quality assurance console. Then they deployed additional McAfee solutions, starting with McAfee Enterprise Security Manager and other components of the McAfee SIEM, because LCBO's legacy SIEM was being obsoleted.

"We decided out of the gate that we would obtain the best value out of McAfee Threat Intelligence Exchange, McAfee Advanced Threat Defense, and McAfee Endpoint Threat Defense and Response," says Brown. "It didn't make sense to deploy these solutions without McAfee Endpoint Security in place, so we rolled it out after the SIEM and then layered in the other solutions."

Fast, Powerful, Easy-to-Use SIEM with Superior Licensing Model

In addition to improved protection and visibility, moving to the McAfee SIEM also made financial sense for the LCBO. With the legacy SIEM, cost was tied to events per second (EPS), so every time LCBO increased coverage of the environment to include more sources, the cost increased. With the McAfee SIEM, LCBO can add as many log sources as desired with no increase in cost.

LCBO's McAfee SIEM receives input from each of the McAfee solutions it has deployed as well as intrusion prevention systems (IPS), firewalls, domain controllers,

Challenges

- Provide better value and 24/7 protection than an MSP.
- Manage effectively with small information security staff.
- Minimize gap between detection of threat and protection or correction.

McAfee solution

- McAfee Active Response
- McAfee ePolicy Orchestrator
- McAfee Complete Endpoint Threat Protection
- McAfee Endpoint Security
- McAfee Endpoint Encryption
- McAfee File and Removable Media Protection
- McAfee Endpoint Threat Defense and Response
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense
- McAfee SIEM: McAfee Advanced Correlation Engine, McAfee Enterprise Log Manager, McAfee Enterprise Security Manager, McAfee Event Receiver, McAfee Global Threat Intelligence for SIEM
- McAfee Database Activity Monitoring
- McAfee Web Gateway

routers, Microsoft Active Directory, wireless controllers, database servers, threat intelligence feeds—McAfee Global Threat Intelligence and open-source and Canadian Cyber Incident Response Centre (CCIRC)—and much more. Brown has been impressed with the solution's speed and power, as well as ease of use.

"When the indicators of compromise for the WannaCry ransomware came through late on a Friday evening, I was able to go into the McAfee Enterprise Security Manager and set up alerts by myself," notes Brown. "I found it very intuitive, even though I am definitely not an SIEM expert."

Peace of Mind with McAfee Endpoint Security and Dynamic Application Containment

Next LCBO deployed McAfee Endpoint Security version 10.5, migrating the McAfee VirusScan® Enterprise engine in the McAfee Complete Endpoint Threat Protection suite to the McAfee Endpoint Security Threat Prevention module. The security team turned on the cloud-based Real Protect machine learning functionality in the McAfee Endpoint Security Adaptive Threat Protection module to categorize files encountered at the endpoint based on the attributes and behavior of millions of malicious samples. Any file categorized as potentially malicious is quarantined using the Dynamic Application Containment (DAC) feature until the McAfee Advanced Threat Defense sandboxing appliance has analyzed it and either convicted it or deemed it safe.

"Knowing that any file that is not already tagged as trusted will be contained before it can cause damage gives me considerable peace of mind," says Brown. "I would tell my counterparts in other organizations with [McAfee VirusScan Enterprise] that it is important to spend time up front to ensure you migrate rule sets from 'like to like,' but the benefits of migrating to McAfee Endpoint Security far outweigh any work required to make the transition."

Enhanced Search Capabilities Dramatically Shrinking Time to Find Threats and Respond

For improved forensics and faster resolution of threats across endpoints, LCBO deployed McAfee Endpoint Threat Defense and Response across all back-office and point-of-service servers and production desktops. Brown's team frequently uses the solution's McAfee Active Response Search functionality and the McAfee Active Response Workspace, both accessed from the McAfee ePO console. "With McAfee Active Response, we can quickly and easily search for hashes, filenames, IP addresses. You name it, we go find it," says Brown. "Finding suspicious files fast reduces the time needed to respond appropriately and shrinks the window of vulnerability."

"In the [McAfee] Active Response workspace, we can view a list of all potential threats, high-risk threats, and threat timelines. We can click on an executable or other suspicious file, drill down to discover where it is installed, see what it is doing to its host system, and get a full read-out of its behavior," he elaborates. "We can then click to take action, such as mark the file as known trusted or known malicious, or end or delete the process for one system or companywide—all from one console. It really is remarkable."

Reduced Detection and Response Time Deemed a "Game Changer"

In a typical potential threat scenario, as soon as a potentially malicious file has been sent to McAfee Advanced Threat Defense or the McAfee Threat Intelligence Exchange reputation database, Brown's team receives an alert from the McAfee SIEM, and then opens a case.

"McAfee Advanced Threat Defense gives us a better idea of the nature of the hash value or file name that is tripping the alert," explains Brown. "Then we search

Results

- Faster detection and faster incident response time.
- Peace of mind that unknown files will be contained before infecting "patient zero."
- Reduction in operational overhead, including reducing consoles from six to three
- Visibility expanded to include intra- and out-of-network traffic.

using McAfee Endpoint Threat Defense and Response or McAfee Threat Intelligence Exchange to find out where the file exists, on which endpoint. Within minutes after being alerted, either by the SIEM or an email, we can ascertain whether the threat has been dealt with, and, if not, take appropriate action,"

"That we can now quickly see exactly where an infection exists within our entire environment and, if we want to, within minutes remove it—not only from that endpoint but from every single endpoint in our network—is a game changer," says Brown. "We simply couldn't do anything like that before. It would have taken much longer to find the executable and remove it throughout the environment."

Visibility Extended to Include Lateral and Out-of-Band Traffic

LCBO already had another sandboxing appliance but wanted to add McAfee Advanced Threat Defense for two reasons: first, because of its integration via the McAfee Data Exchange Layer open-source platform to other McAfee security systems, and second, because its incumbent sandbox is limited to perimeter-based detection. "With our employees increasingly working from anywhere, the perimeter is dissolving," says Brown. "With our existing sandbox, we could analyze 'north-south' traffic coming into and leaving the network but not 'east-west' traffic crossing the network. McAfee Advanced Threat Defense and its integration with McAfee Threat Intelligence Exchange and McAfee Endpoint Threat Defense and Response give us that visibility."

In addition, if a user is out of network, not only can McAfee ePO software push out corporate security policies to his or her laptop, but it can also highlight any malware that hits the laptop before it returns inside the network. Thus, defenses can be set in motion. The file's reputation can be added to the McAfee Threat Intelligence Exchange database and all systems can be updated to block the file even before LCBO's network has encountered the malware. "Being able to see internal lateral and out-of-band traffic is a huge advantage," claims Brown.

Integration: The Key to Quick Recovery

LCBO is also in the process of rolling out McAfee Web Gateway and McAfee Database Activity Monitoring. McAfee Web Gateway will offload some of the web-filtering load from the organization's IPS appliances and enable suspicious files entering via the web to be sent directly to McAfee Advanced Threat Defense for analysis. McAfee Database Activity Monitoring will watch key databases for out-of-the-ordinary activity and help combat "permissions creep."

"Ultimately, the main benefits of the McAfee ecosystem are integration and speed to recovery, which is itself a byproduct of integration," concludes Brown. "With everything integrated, we can manage our entire security infrastructure from two to three panes of glass instead of six or seven. Fewer things to see, fewer things to miss and the ability to recover from an attack in minutes to an hour, rather than days or weeks, just can't be overstated," he points out.

> "That we can now quickly see exactly where an infection exists within our entire environment and, if we want to, within minutes remove it—not only from that endpoint but from every single endpoint in our network—is a game changer. We simply couldn't do anything like that before. It would have taken much longer to find the executable and remove it throughout the environment."
>
> —Simon Brown, Director of Information Security, Liquor Control Board of Ontario

McAfee™
Together is power.

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

3455_0817
AUGUST 2017