Case Study

A Security Connected Approach to Endpoint and Network Security at CEMEX

CEMEX

Customer profile
A global building materials company.

Industry
Manufacturing.

IT environment
Approximately 25,000 endpoints spread across 50 countries.

Challenge
Efficiently safeguard all endpoints and improve visibility and management of overall security posture.

McAfee solution

- McAfee ePolicy Orchestrator
- McAfee Next Generation Firewall
- VirusScan Enterprise
- McAfee Host Intrusion Prevention
- McAfee Application Control for PCs
- McAfee Host Data Loss Prevention
- McAfee Personal Firewall
- McAfee Endpoint Encryption
- McAfee Global Threat Intelligence
- McAfee Email Gateway
- McAfee Web Gateway
- McAfee Professional Services

CEMEX is a global building materials company that produces, distributes, and sells cement, concrete, aggregates, and related building materials and services to customers and communities throughout the Americas, Europe, Africa, Asia, and the Middle East. Based in Monterrey, Mexico, CEMEX employs more than 43,000, with operations in 50 countries spanning four continents. The company is also the world's leading supplier of ready-mix concrete.

Business Trigger: Enterprise Security to Combat Increasingly Sophisticated Threats

As a global company, CEMEX faces security challenges at all levels of the business—from the systems on the manufacturing plant floor and business applications safeguarding sensitive information to the front-end and customer-facing applications. The need to have an integrated protection approach between the endpoints and the perimeter security has become a must rather than an option. Previously, the company relied on a mixed-vendor security environment that included several vendors' products.

"The incompatibility among different security solutions was a large hurdle that created inefficiencies for the security operations staff," relates Romeo Siquijor, chief information security officer and enterprise security head for process and IT, CEMEX. "We had little visibility on the overall security environment, and we had to push policies out one by one. We needed a more efficient means of managing the platforms with a more integrated approach."

Solution Focus: The Security Connected Platform from McAfee

To address these requirements, CEMEX has been gradually replacing its multivendor security environment with an integrated, single-vendor solution from McAfee. The company began with McAfee® VirusScan® Enterprise antivirus software and McAfee Host Intrusion Prevention as a first layer of defense on its desktops. CEMEX has also installed McAfee Application Control, which blocks the installation of unauthorized applications and foils advanced persistent threats, and McAfee Personal Firewall to block malware coming in to endpoints from the Internet. McAfee Application Control uses dynamic whitelisting technology and the McAfee Global Threat Intelligence cloud-based reputation service to provide complete protection from unwanted applications and code.

More recently, CEMEX faced increased threats from malware introduced through incoming emails and downloaded inadvertently when users access certain websites. To keep these types of threats at bay, the company added McAfee Email Gateway and McAfee Web Gateway to its security framework. The mix was not complete without McAfee Next Generation Firewall as a first line of defense at the network perimeter.

McAfee ePolicy Orchestrator® (McAfee ePO™) software provides centralized management and control over the entire security platform, giving CEMEX a unified view into its security posture and the ability to publish consistent policies and make changes from a single dashboard.

Why McAfee: A Holistic Approach to Enterprise Security

Today, more than 80% of CEMEX's security platform consists of McAfee solutions—a percentage that is growing with the company moves to install the entire McAfee protection suite. "With the objective to have a single-vendor enterprise security platform, we know we've made the right choice with McAfee," notes Siquijor. "McAfee solutions are consistently named as leaders in the Gartner Magic Quadrant, and no other vendor has achieved the level of integration that McAfee has by far, with centralized management from a single [McAfee] ePO console. In our own evaluations, McAfee products consistently outpace their competition in cost, market presence, technology, and technical support."

An Integrated Platform with Flexible Security Administration

With security data rolled up to a single McAfee ePO server in the security operations center (SOC) in Monterrey, Mexico, CEMEX administrators have visibility across the entire company infrastructure. They can decide which security tasks to manage globally from the SOC and which to offload to local or regional administrators by giving them limited access rights to McAfee ePO software. As CEMEX continues to migrate to a security framework based on integrated McAfee solutions, the company is benefiting from the ability of endpoint, network, and data security solutions to share information with one another for even greater visibility and more efficient, faster remediation. "McAfee ePO gives us all the flexibility we need to manage most of our security platforms efficiently," remarks Siquijor.

Enterprise-Level Firewalls

McAfee Next Generation Firewall plays a critical role in CEMEX's integrated security strategy. Working in concert with McAfee Network Security Platform, McAfee Next Generation Firewall secures the CEMEX perimeter in Mexico, as well as remote sites in Spain and the US. Castillo notes that the ongoing McAfee strategy for integrating McAfee Next Generation Firewall with the rest of the security suite—which is the essence of Security Connected—is what sets it apart from other firewall solutions.

"We considered installing a general-purpose [unified threat management] UTM-style firewall from another vendor, but our operation needs very specific enterprise-level firewalls—and that's where McAfee Next Generation Firewall is really strong," he comments. "Failover is an especially valuable feature for high availability and traffic management. In fact, we have had no major incident with network performance since we installed McAfee Next Generation Firewall years ago."

Powerful New Efficiencies

McAfee Application Control is a powerful example of the efficiencies of centralized administration. The solution blocks advanced threats without requiring signature updates. From the McAfee ePO console, CEMEX administrators are able to consistently enable legitimate applications, block known and unknown malware, and properly manage new application software. Unlike most whitelisting solutions that require security administrators to create and continually update a list of all approved applications, with McAfee Application Control, administrators simply define the path that needs to be followed to install new applications. If software isn't licensed, it simply won't be installed if application control is installed.

"The ability to define general policy rather than software-specific policies saves us a tremendous amount of time and effort," explains Siquijor. "Reporting and search functionalities within the McAfee solution makes it easier for us to pinpoint vulnerabilities—such as PCs with out-of-date virus definitions, security system thresholds, and compliance of software licenses to name a few."

"McAfee solutions are consistently named as leaders in the Gartner Magic Quadrant, and no other vendor has achieved the level of integration that McAfee has, with centralized management from a single [McAfee] ePO console. In our own evaluations, McAfee products consistently outpace their competition in cost, market presence, technology, and technical support."

—Romeo Siquijor, Chief Information Security Officer

Results

- Safeguards against zero-day advanced persistent threats without signature updates.
- Greatly diminishes administrative time, from defining policies to repairing workstations.
- Protects more than 26,000 endpoints from email, web, and application-generated attacks.
- Provides streamlined and integrated management of large, global security platform.

Locking Down Endpoint Security

Working together, VirusScan Enterprise, McAfee Host Intrusion Prevention, McAfee Personal Firewall, and McAfee Application Control now protect more than 26,000 endpoints at CEMEX. The company has just ramped up an initiative for McAfee Endpoint Encryption and McAfee Host Data Loss Prevention, both of which will be initially rolled out to 10 departments that handle sensitive business and personal information, such as human resources, planning, legal, and others. "Data loss is becoming a threat all across the globe, but we're focusing first on regions that have stricter requirements for privacy protection, such as several European countries," Siquijor says. "With [McAfee] ePO, we can manage the rollout of solutions such as endpoint encryption and data loss prevention in a phased manner without disrupting end-user operations."

Heading Off Web and Email Attacks

According to Siquijor, McAfee Email Gateway offers a critical defense against email-borne malware. Although the monthly volume of incoming emails has grown from seven million when McAfee Email Gateway was implemented to about 12 million currently, the percentage of malicious or unwanted email in this traffic has grown two-fold in this timeframe.

In addition, CEMEX has fully deployed McAfee Web Gateway to work in conjunction with McAfee Application Control in the manufacturing plants and dispatch centers, both of which are vulnerable due to unapproved applications or malicious websites. Prior to installing these applications, users on plant floors were installing and uninstalling applications at a rate that was dragging down system performance and tying up IT administrative time. Now, McAfee Application Control blocks any applications that are not on CEMEX's approved whitelist, and McAfee Web Gateway filters a volume of around 50 to 150 million website hits every month, blocking malicious adware and preventing access to sites with questionable reputations.

Finally, McAfee Next Generation Firewall protects the last Internet-facing frontier of the CEMEX network. Integrating application control, intrusion prevention, and evasion prevention in a single network security solution over a unified threat management platform will be a major innovation to help the company stay ahead of evolving threats. "Since we installed McAfee Next Generation Firewall, we have not experienced a major virus outbreak affecting our perimeter," Siquijor remarks. "With a secured perimeter, efficient endpoint protection, and new controls we are adding to manage sensitive information within the environment, we're beginning to feel reasonably confident that we're covering our bases for enterprise security."

Ensuring a Smooth Deployment

Lastly, in order to maximize security services and technology solutions, CEMEX benefited from McAfee Professional Services. "McAfee Professional Services has been there to help CEMEX implement key projects during rollout and for trouble shooting problems," said Siquijor.

intel Security

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

61345cs_cemex_0914B_ETMG