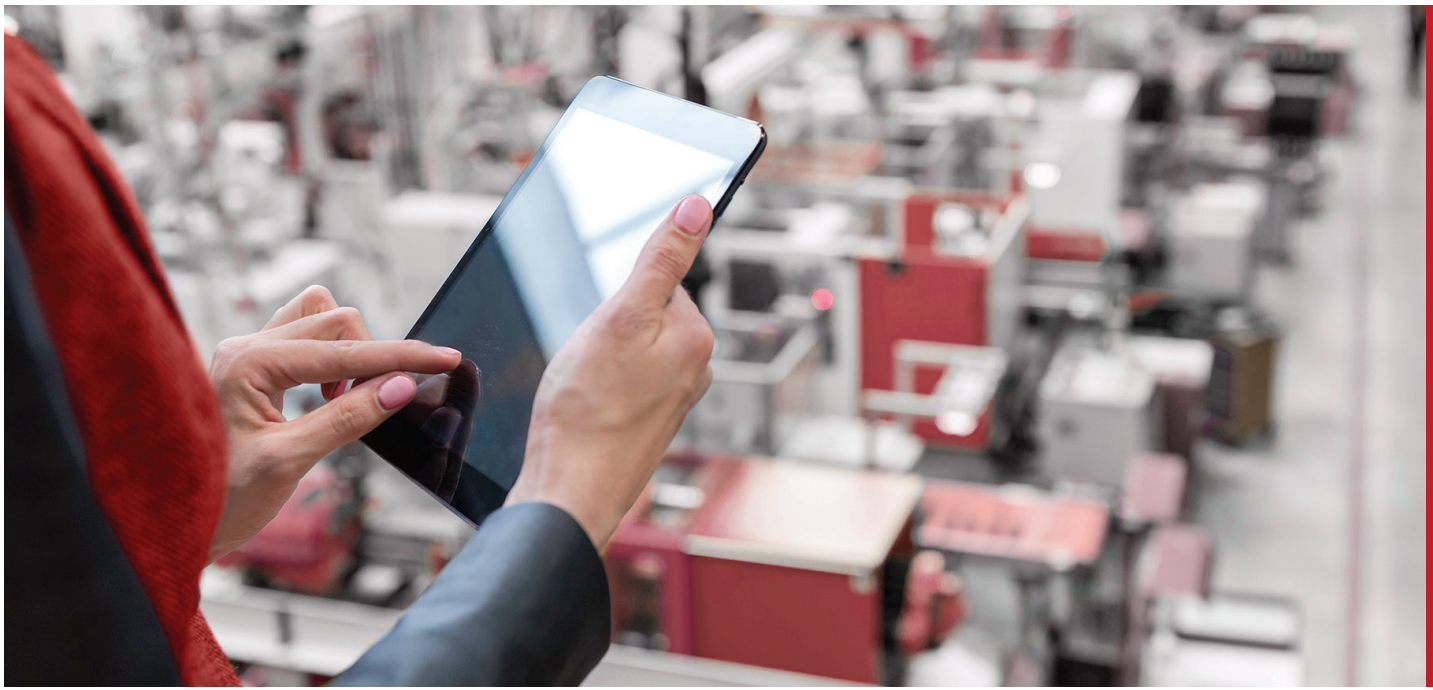
CASE STUDY

Leading Global Apparel Manufacturer Up-Levels Security

Small team bolsters defenses against ransomware and zero-day threats



Brandix Group

Customer profile
Sri Lanka's single largest apparel exporter

Industry
Apparel manufacturing

IT environment
5,500 endpoints across 42 sites in Sri Lanka, India, Bangladesh, and the Dominican Republic

By migrating to McAfee® Endpoint Security and adding McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense, this global manufacturer improved its overall security posture tremendously without adding additional staff or complexity.

Sri Lanka's single largest apparel exporter, the Brandix Group, develops, manufacturers, and markets end-to-end apparel solutions to global fashion super brands, including Victoria's Secret, Gap Inc., Lands' End, and Marks & Spencer—to name a few. The company employs approximately 48,000 people and has 42 manufacturing facilities spread across Sri Lanka as well as in India, Bangladesh, and the Dominican Republic.

Company Growth Mandates Security Boost

In recent years, Brandix has experienced rapid growth. The company was lauded as Sri Lanka's Exporter of the Year the past five years by the Export Development Board and Most Valuable Export Brand the past three years by Brand Finance. With increased recognition and additional customers come additional security risk. "With the success and growth of our business, we knew we needed to take information security to the next level," says Manager of Microsoft Technologies Janaka Sampath who oversees endpoint protection across the extended Brandix enterprise. "Upper management agreed and mandated it."

Even without growth, notes Janaka, the business would still have faced challenges. "With new avenues for threats opening daily, keeping security products up to date and staying current is an ongoing challenge," he says. "Staying current also means we need to periodically benchmark the capabilities of our security tools against competitive solutions to make sure we are protected as well as we can be."

Why Brandix Stayed with McAfee

Not long ago, as part of its benchmarking and due diligence processes, Brandix began to consider alternatives for endpoint protection. The company had used McAfee® antivirus solutions to protect endpoints for many years and had kept renewing its McAfee licenses because its McAfee products continued to meet requirements. Janaka admits, though, that newer endpoint protection products that do not rely on signatures for detection had begun to catch his attention.

After looking at these other endpoint solutions, however, he concluded that sticking with McAfee for endpoint protection still made the most sense because McAfee had improved its product offering. "McAfee is continually responding to the market and threat landscape, evolving its product line to meet the latest demands to keep environments secure," says Janaka. "The new, more intelligent and dynamic McAfee Endpoint Security is a perfect example. So is McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense, all of which we decided to add to our security arsenal."

More Robust Endpoint Protection Against Zero-Day Threats

Using the McAfee migration tool, Janaka's team migrated the antivirus engine of the McAfee Complete Endpoint Protection Advanced suite—McAfee VirusScan® Enterprise—to the McAfee Complete Endpoint Threat Protection Suite. "It was a seamless transition and our users didn't even notice," recalls Janaka. "And on the administrative side, the McAfee Endpoint Security interface is lightweight and simple to use."

Brandix also deployed the Adaptive Threat Prevention module option, which adds Dynamic Application Containment (DAC) functionality and Real Protect

Challenges

- Keep security current as the company grows and threats change
- Protect against ransomware and zero-day threats
- Manage security effectively with a small team

McAfee Solution

- McAfee Advanced Threat Defense
- McAfee Complete Endpoint Threat Protection
- McAfee DLP Endpoint
- McAfee Endpoint Security
- McAfee Threat Intelligence Exchange

Results

- Enables centralized security administration by a small team
- Simplifies management and reduces operational overhead
- Accelerates response time and mitigates risk for zero-day attacks
- Protects sensitive data, preventing unauthorized removal via USB device

machine learning technology. "DAC and Real Protect provide another layer of protection that goes well beyond signature-based detection," notes Janaka. "These new capabilities played a key role in our decision to go with McAfee Endpoint Security."

DAC quarantines suspicious but not convicted files and prevents them from executing. It protects "patient zero" and its neighbors from infection while providing an opportunity to analyze the suspicious file and determine whether it is truly malicious. Real Protect uses cloud-based intelligence, based on millions of malicious samples and static and dynamic behavioral analysis to automatically match attributes and behaviors of unknown files against threat models to effectively convict zero-day malware. Brandix is running DAC in "productivity mode" first, fine-tuning and teaching it to avoid false positives before moving to "balance mode." In Brandix's in-house tests with malware and greyware samples and mutations of samples, the impact of DAC and Real Protect has been impressive. "In our simulations, McAfee Endpoint Security has detected and blocked ransomware and zero-day threats very effectively," claims Janaka.

Simplified Management and Reduced Operational Overhead

Another reason Brandix stayed with McAfee was to continue leveraging the McAfee® ePolicy Orchestrator® (McAfee ePO™) management console, which allows administration of multiple security solutions, not just endpoint protection, from a single pane of glass. "McAfee ePO [software] reduces overhead and simplifies administration so much that we can manage security with just a few individuals," says Janaka. "It reduces the need to think about security as much. It allows us to focus on more value-added activities."

To bolster defenses, Brandix supplemented McAfee Complete Endpoint Threat Protection and the dynamic McAfee Endpoint Security framework with McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense. McAfee Threat Intelligence Exchange combines multiple internal and external threat information sources in a threat intelligence database and instantly shares this data across integrated systems, including McAfee Advanced Threat Defense. McAfee Advanced Threat Defense, a market-leading sandboxing solution that provides sophisticated dynamic and static behavioral analysis of unknown files, is, in Janaka's words, "an extremely valuable tool that increases our ability to protect against zero-day attacks exponentially."

Using McAfee ePO software, Janaka and his small team can manage each of these solutions from headquarters, from one common, web-based console, setting policies and pushing them out to the company's sites worldwide, while small remote teams at each of the company's major sites also use McAfee ePO software to monitor day-to-day security in their respective environments.

Stronger Security Posture and Faster Response Thanks to Integration

Brandix purposefully implemented all three McAfee solutions—McAfee Endpoint Security, McAfee Threat Intelligence Exchange, and McAfee Advanced Threat Defense—to take advantage of their integration via the

Data Exchange Layer (DXL), an open-source platform that connects security components for real-time data exchange without requiring point-to-point application programming interface (API) connections. McAfee Threat Intelligence Exchange uses DXL to aggregate and share global and local threat information across DXL-connected systems as soon as it becomes available. Since McAfee Endpoint Security is built to leverage DXL, now when a Brandix endpoint encounters a suspicious or malicious file, that information is immediately conveyed to McAfee Threat Intelligence Exchange, which compares it to its reputation database and, if no match is found, immediately shares it with McAfee Advanced Threat Defense for analysis. If McAfee Advanced Threat Defense concludes the file is malicious, that information is instantly shared with all systems in the environment connected via DXL.

"Aggregating and sharing threat intelligence that has been gathered at various levels, from a range of sources, significantly enhances our security posture," explains Janaka. "With McAfee Threat Intelligence Exchange and our integrated security platform, we can respond to threats much more quickly and mitigate risk more effectively. For instance, if a user attempts to download, knowingly or unknowingly, a file that violates our security policy or causes suspicious activity detected by McAfee Endpoint Security, we can immediately blacklist the file and prevent it from executing anywhere in our highly distributed environment."

Safeguarding Sensitive Data and Building an Adaptable Threat Defense Lifecycle

As the company continues to grow—reaping accolades and recognition and adding new apparel products for new customers—so does the risk of sensitive product information falling into the wrong hands. That's why Brandix takes data loss prevention very seriously. To prevent sensitive data from moving to unauthorized USBs or other storage devices, the company deployed McAfee DLP Endpoint. As with its other McAfee solutions, Janaka and his colleagues can set policies, push out updates, and monitor data protection easily from the McAfee ePO console.

In the past, Janaka has been pleased with how McAfee products have met requirements and continued to evolve. He also expresses satisfaction with the level of support Brandix has received from McAfee personnel. However, today what he praises most about McAfee is its ability to support the company's growth with an adaptable threat defense lifecycle that can be managed by a small team. "The biggest benefit of our decision to go with McAfee Endpoint Security and the McAfee integrated security platform," he says, "is that it takes our security to next level without a huge hassle."

> "... DAC and Real Protect provide another layer of protection that goes well beyond signature-based detection. These new capabilities played a key role in our decision to go with McAfee Endpoint Security."
>
> —Janaka Sampath, Manager, Microsoft Technologies, Brandix

McAfee
Together is power.

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

3662_1017
OCTOBER 2017