CASE STUDY

Overhauling Endpoint Protection Aids Innovation and Strengthens Security Posture

Innovative global business process transformation company transforms its own security processes with help from McAfee

Sutherland Global Services

Customer Profile
Multinational business process transformation company

Industry
Technology and business services

IT Environment
Approximately 50,000 endpoints across 16 countries on six continents

Sutherland Global Services helps over 100 *Fortune 1000* companies in 16 countries rethink and rebuild business processes for the digital age using data analytics and other technologies, design thinking expertise, and industry-specific knowledge. The Pittsford, New York-based company invested in transformation of its own endpoint security, dramatically improving its overall security posture while saving time and money. In addition, by leveraging the Open Data Exchange Layer (OpenDXL), the company is creating a unified defense in which diverse security systems work together to support and strengthen one another.

Connect With Us

Protecting Against Business Interruption and Breaches

"Every minute that a system is unavailable when a business user needs it costs us a lot of money," says Prashanth M J, Sutherland Global Services' global head of technology infrastructure. "Business interruption and data breaches are a significant risk that we want to secure against. We are constantly working to ensure that all the necessary controls are in place to minimize these risks and allow us to continue offering innovative, tailored solutions and services to our clients."

With approximately 50,000 nodes to protect, including 1,000 servers, more than 80 data/delivery centers, and a digital backbone spread across 16 countries and six continents, minimizing security risks is a mammoth task requiring many security solutions. Getting all the various systems and controls to talk with one another and share security intelligence to keep the entire extended enterprise safe is part of the technology infrastructure team's ongoing battle.

Imperative: Strategic Partners that Support Innovation

With such a large and far-flung enterprise, Sutherland Global Services depends on the help of strategic partners like McAfee. "We have developed a high level of trust in McAfee because McAfee has always delivered to meet our business requirements, including the need to be continually innovating," says Prashanth. "Innovation is what keeps our company alive and thriving."

"Our services innovate at the intersection of business and technology, transforming processes to realize our client's visions," continues Prashanth. "McAfee is continually introducing solutions that directly address our business requirements—for instance, to help us close the detection to remediation gap or to progress in our digital transformation."

Creating Unified Defenses by Leveraging OpenDXL

Prashanth also praises McAfee for developing OpenDXL, a technology industry initiative to create adaptive systems of interconnected solutions that communicate and share information for real-time, accurate security decisions. Using OpenDXL, Sutherland Global Services is currently working to integrate the company's non-McAfee security information and event management (SIEM) solution with its McAfee endpoint protection. Integration with the company's web gateway and firewall are also on Sutherland's OpenDXL roadmap.

"I see huge potential in OpenDXL," notes Prashanth. "We have multiple security products from different vendors all operating in their own silos. To create a unified defense against cyberattacks, it's very important that intelligence from one system can be used by another."

Challenges

- Provide 24/7 availability to business users worldwide
- Integrate security solutions for unified cyberdefense
- Efficiently comply with regulations, particularly for healthcare and financial services

McAfee Solutions

- McAfee® Advanced Threat Defense
- McAfee® DLP Endpoint
- McAfee® Endpoint Encryption
- McAfee® Endpoint Security
- McAfee® Endpoint Threat Defense and Response
- McAfee® ePolicy Orchestrator®
- McAfee® File Integrity Monitoring
- McAfee® Professional Services
- McAfee® Threat Intelligence Exchange

Consolidating Endpoint Protection Decreases Costs and Increases Revenue Generation Potential

To protect its endpoints worldwide, Sutherland Global Services relies heavily on the McAfee ePolicy Orchestrator (McAfee ePO™) central management console. Using McAfee ePO software, administrators manage and monitor multiple McAfee products and security functionality—antivirus, host data loss prevention, host intrusion prevention, endpoint encryption, file integrity monitoring, and more—from a single pane of glass.

"McAfee ePO [software] gives us the edge to manage our global enterprise seamlessly," claims Prashanth. "Also, it's so easy to use, I don't have to deploy expensive Level 2 or 3 security engineers."

In the past two years, as part of a complete upgrade and transformation of its endpoint protection, the company consolidated seven globally dispersed McAfee ePO software servers to one. Today, protection for all approximately 50,000 endpoints is managed through one central McAfee ePO console within the company's security operations center.

"When we decommissioned the other six McAfee ePO [software] servers, we reaped savings immediately," recalls Prashanth. "In addition to reducing hardware and software costs, data center power consumption and time spent on maintenance and overhead plummeted. We also added new functionality without having to add staff and freed up staff to spend time on more value-added activities."

"Furthermore, overhauling endpoint protection increased systems availability enterprise-wide," adds Prashanth. "And increased availability increased our potential to generate additional revenue."

Faster, Easier Compliance Reporting Helps Raise Compliance Levels to Over 95%

Consolidation to one central console reaped huge time savings in the area of compliance, especially in healthcare and financial services industries. "With one central console, compliance reporting is now many times more efficient," affirms Prashanth. "We can quickly and easily provide dashboards that are customized and contextualized to the security owners of the various geographies, clients, or industries. As a result, it's much easier to produce the required reports, and our compliance level has increased to over 95%."

Results

- Reduced administrative overhead and hardware and software costs
- Enhanced systems availability
- Increased potential to generate more revenue
- Easier management of endpoint protection, freeing up administrators worldwide
- Stronger, multilayered defense against malware, including zero-day threats
- Much more efficient compliance reporting worldwide
- Compliance levels increased to over 95%
- Faster time to threat detection and response

Multilayered, Threat-Sharing Protection Strengthens Defense Against Zero-Day Threats

Migrating to McAfee Endpoint Security from McAfee® VirusScan® Enterprise was another critical piece of the organization's endpoint protection revamp. "We knew it was time for robust, next-generation anti-malware with extra layers of protection, and, thankfully, McAfee had what we needed," explains Prashanth. "We especially wanted to use Dynamic Application Containment to quarantine unknown files and Real Protect machine learning functionality to analyze suspicious files on the fly."

The company also migrated to McAfee Endpoint Security to take advantage of McAfee Threat Intelligence Exchange, which stores continually updated global and local threat intelligence and shares it bidirectionally via the Data Exchange Layer (DXL) to all DXL-connected systems. McAfee Endpoint Security connects to DXL out of the box. "So, when one of our endpoints encounters a malicious file, or a global research center finds a new zero-day threat, rather than having to wait for signatures to be available and pushed out by an administrator, all our endpoints automatically know about it immediately," explains Prashanth.

Sutherland Global Services enlisted McAfee Professional Services to help execute a smooth, phased migration to McAfee Endpoint Security that had zero impact upon systems availability for business users across the globe. Migration for all endpoints to McAfee Endpoint Security included the solution's Advanced Threat Protection module, which contains the Dynamic Application Containment and Real Protect technologies. The company also deployed the DXL fabric and McAfee Threat Intelligence Exchange throughout its network.

Accelerating Incident Response

As part of its endpoint protection transformation, Sutherland Global Services also implemented a McAfee Advanced Threat Defense appliance for dynamic and static sandbox analysis. "McAfee Advanced Threat Defense helps us in two important ways," notes Prashanth. "First, when our endpoints encounter an unknown file and quarantine it, the file is sent directly to the McAfee appliance for in-depth analysis. Once analyzed, the result is then shared, via [McAfee Threat Intelligence Exchange] across the enterprise. In this way, we have caught quite a few malicious files and proactively protected all our endpoints."

> "Our services innovate at the intersection of business and technology to transform processes to realize our client's visions. McAfee is continually introducing solutions that directly address our business requirements—for instance, to help us close the detection to remediation gap or progress in our digital transformation."
>
> —Prashanth M J, Senior VP, Global Head of Technology Infrastructure, Sutherland Global Services

"Second, McAfee Advanced Threat Defense accelerates our IoC investigation process," continues Prashanth. "In the past, for every unknown IoC, we had to send a hash sample to McAfee support and wait to be told whether it was malicious. With McAfee Advanced Threat Defense, we can now analyze the IoC ourselves and more quickly determine the appropriate action to take."

In addition, the company is in the process of adding McAfee Endpoint Threat Defense and Response to boost its ability to proactively hunt for threats. "We want to be more offensive, not just defensive," says Prashanth. "I expect McAfee Endpoint Threat Defense and Response to be one of the most important tools in our armory to protect against dormant threats that might be in our environment just waiting for triggers... It all boils down to speed of response. The right actions are useless if you don't respond fast enough."

To Be Prepared for the Future, More Than Products Are Needed

"Our partnership with McAfee has been extremely fruitful, helping me feel confident that our systems are protected and ready for the future." states Sutherland Global Services CIO and Chief Digital Officer Doug Gilbert. "Whom you partner with is not just about a product or products—it's about the entire ecosystem. With McAfee, we have people rallying around us—not just to sell products but to help us design, deploy, maintain, and optimize them."

In the future, as Sutherland Global Services moves increasingly into the cloud and its already in motion digital transformation, McAfee will continue to play a critical role. Prashanth cites the new McAfee® MVISION products as another example of innovation that is sure to help his company: "Because the threat landscape is so complicated, you need to work together. McAfee brings [the right] technology to us. We bring business domain [knowledge]. 'Together is Power' is the right way to move forward."

"Our partnership with McAfee has been extremely fruitful, helping me feel confident that our systems are protected. Whom you partner with is not just about a product or products—it's about the entire ecosystem. With McAfee, we have people rallying around us—not just to sell products but to help us design, deploy, maintain, and optimize them."

—Doug Gilbert, CIO and Chief Digital Officer, Sutherland Global Services

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

4322_0719
JULY 2019