The Innovation Imperative:

Solutions for the Cyber Lifecycle

When it comes to responding to the current cyber threat landscape, innovation is a must. The problem is not just that threats are growing more numerous and sophisticated, it's also that organizations have an increasingly complex environment to secure. Each aspect of the enterprise—from the data center and the cloud to the endpoint and the Internet of Things—represents a potential entry point to malicious actors. At Symantec, we understand that to be effective, innovation must be continuous—and it must be deployed as part of a larger Integrated Cyber Defense strategy.

Security Operations Center

Security Orchestration, Automation and Response
Demisto's SOAR platform integrates with multiple Symantec products to centralize visibility and help security teams to harmonize endpoint protection, threat protection and incident monitoring actions.

Targeted Attack Analytics
An AI-based "virtual analyst," TAA sifts through mountains of false alerts to identify truly targeted activity and generate a prioritized incident report, helping human analysts accelerate their response time.

The Cloud

CloudSOC Cloud Access Security Broker
CloudSOC CASB extends an agency's existing governance, compliance and data security policies to the cloud, applying machine learning techniques to application intelligence, transactional activity, user behavior analytics and data loss prevention.

Cloud Workload Protection
The Cloud Workload Protection Suite integrates natively with public cloud APIs to provide elastic, scalable security, with a single cloud-based console working across public and private clouds and on-premise systems.

Integrated Cyber Defense

Symantec's Integrated Cyber Defense Platform unifies cloud and on-premises security to provide threat protection, information protection and compliance across all endpoints, networks, email and cloud applications—powered by the largest threat intelligence network.

The Network

Web/Email Isolation
Symantec Web and Email Isolation provide the last line of defense against web-based zero-day malware, executing web sessions away from endpoints and sending only safe rendering information to users' browsers.

Symantec Secure Web Gateway
This cloud-based network security service makes it possible to create and provision policies once, and enforce operational consistency across your entire deployment—regardless of location or device—using a unified management console.

The Endpoint

Machine Learning-Based Log Processing
Part of Symantec Endpoint Security, this tool uses AI/machine learning to flag potentially alarming trends that might elude human analysts and traditional log management tools.

Deception
With SEP deception capabilities, customers can deploy customizable decoys—which include fake credentials, files and other enticing assets—to lure adversaries into exposing their presence before more damage is done.

Internet of Things

USB Scanning
The Industrial Control System Protection Neural defends against malware or other attacks—both known and unknown—that are launched when a USB device is inserted into an otherwise-isolated industry control system.

Critical System Protection
Designed to protect legacy systems and embedded devices, CSP adds layers of defense at the kernel level to prevent unhygienic operations at the endpoint, effectively freezing systems so that malicious content is unable to run.