Symantec
by Broadcom Software

WHITE PAPER

Symantec®: A Rich History of Security Innovation

WHITE PAPER

Symantec: A Rich History of Security Innovation

Symantec by Broadcom Software

TABLE OF CONTENTS

Executive Summary

Does Symantec® innovate? If innovation means cloud-only solutions created by scrappy startups, certainly not. Symantec's 40-year history, emphasis on integrated security, and insistence that its solutions work across on-premises and cloud environments, all disqualify it from that "innovator" class. Since its 2019 acquisition by Broadcom®—and refined focus on selling to the world's most demanding organizations—it's easy to see Symantec as just another big, slow-moving business waiting its turn for disruption.

But in a larger sense, Symantec has always innovated: by creating, selecting, acquiring, developing, and integrating security technologies; and by anticipating and aligning to security frameworks like Zero Trust and Secure Access Service Edge (SASE). Innovation continues at Symantec in many forms:

- **Replatforming** Security Software to run on Google Cloud, the world's premier high-performance, low-latency edge network
- **Product advances** to address the compliance, integration, work-from-home, and multi-cloud environment issues global enterprises face
- **Business innovations** such as consolidated simplified pricing to give Symantec customers maximum deployment flexibility at an attractive user-based price
- **Standards innovations** in collaboration with industry, government, and regulatory bodies to represent customer interests and develop interoperable solutions

The latest round of innovation is Symantec Enterprise Cloud (SEC), a consolidated hybrid-cloud solution offering data and threat protection backed by the worldwide network of Symantec Security Operations Centers. A superset of the Secure Service Edge that incorporates Zero Trust Principles, SEC is an end-to-end security solution for the most complex and extensive enterprise networks.

Symantec innovations continue, with a long-time goal of agent consolidation now within reach. A single Symantec agent will reach across technologies, platforms, and environments for consistent management of compliance, secure remote work, and cybersecurity coverage without gaps or overlap.

SYMANTEC HAS ALWAYS INNOVATED—BY CREATING, ACQUIRING, INTEGRATING, AND EXTENDING CYBERSECURITY SOLUTIONS, AND BY ANTICIPATING AND ALIGNING WITH SECURITY FRAMEWORKS LIKE ZERO TRUST AND SASE.

How Symantec Innovates

"Innovation" evokes images of scrappy startups with young coders living on pizza and energy drinks, creating technologies that erupt from garages straight into the cloud. But is the inverse true? Does maturity—of coders or corporations—rule out innovation? It's an unavoidable question for established leaders like IBM, Microsoft, General Electric, and many others. And in a field like cybersecurity, where countering malicious innovations is a key to success, it's a reasonable one.

Symantec, entering its fifth decade, is an established cybersecurity leader with a long record of accomplishment. As part of Broadcom, Symantec's strategy has been redirected from quarterly revenue from product sales to long-term partnerships with the world's preeminent companies. These customers have high expectations of Symantec, but should they expect innovation?

This paper will make the case that Symantec has always innovated—by creating, acquiring, integrating, and extending cybersecurity solutions, and by anticipating and aligning with security frameworks like Zero Trust and SASE. Since its acquisition by Broadcom in 2019, Symantec Enterprise has continued to refine and integrate key security technologies, along with replatforming its entire security offering on Google Cloud infrastructure and increasing its R&D spending. It innovates in business processes that extend, bundle, and price offerings to meet the requirements of large, distributed customers. Working with governments, regulators, and standards organizations, it innovates and shapes technologies on a global scale. And it is bringing the technologies together with Symantec Enterprise Cloud, a comprehensive offering designed to deliver data-centric, cross-platform security for large enterprises.

Innovation by Acquisition: Symantec 1989 to 2019

Founded in 1982 and public since 1989, Symantec grew its cybersecurity business by identifying and acquiring companies that had developed promising niche security technologies. Because these startups typically lacked the required resources, Symantec took on the role of developing their point products into fully featured market-ready solutions, compatible with or integrated into other security technologies. Highlights of Symantec's "Acquire, Develop, and Integrate" strategy are outlined in Table 1.

Table 1: Symantec Acquisitions and Evolution of Acquired Technologies, 1989 to 2019

Company	Technology	Evolution
Certus	Antivirus	Updated, expanded, and integrated into Symantec Endpoint Security Complete—Radicati Group's Top Player seven years running.
Vontu	Data Loss Prevention	Foundation of Symantec Data Loss Prevention Core and Cloud Solutions—2021 Forrester Wave Leaders in their respective segments.
Elastica	Cloud Access Security Broker	Updated, expanded, and integrated as a control point into Data Loss Prevention Cloud.
Blue Coat	Secure Web Gateway	Available as a cloud-delivered network security service with a broad range of options and integrations—a long time leader in SWG technology.

Company	Technology	Evolution
Skycure	Mobile Threat Defense	Integrated into Symantec Endpoint Protection Mobile for predictive, multi-layered mobile defense that respects user productivity.
Fireglass	Web Isolation	Integrated into Symantec Cloud Secure Web Gateway, allowing unmanaged devices to access cloud applications safely.
Javelin	Active Directory Threat Defense	Integrated into Symantec Endpoint Security Complete to harden Active Directory and obfuscate to stop admin credential theft.
Luminate	Zero Trust Network Access	Available as Symantec Secure Access Cloud, a secure cloud gateway for access to private applications.
Bay Dynamics	Information Centric Analytics	Expanded and embedded as risk analytics within Symantec DLP Core and DLP Cloud solutions.

As the table illustrates, these acquisitions are more than point solutions chosen to boost revenue. Integrated into broader products or extended across multiple platforms, they continue to add value long after they have outlived their utility as stand-alone products.

Frameworks and Architectures

Symantec acquired, developed, and integrated security technologies to address emerging threats (data breaches, ransomware) and protect new platforms (mobile, cloud). At the same time, analyst firms were codifying these new computing environments and recommending architectures and frameworks for their defense. These are essentially commercial and analytical approaches to the same issue, so it's no surprise they converged: Symantec technologies aligned with—and in some cases anticipated—the analysts' work. Zero Trust security architecture and SASE technology provide two examples.

Zero Trust

Adoption of mobile and cloud computing platforms gradually eroded the "secure perimeter" model of cyber defense. Its successor was a perimeterless, data-centric security architecture called Zero Trust. Zero Trust is based on authenticating any person, device, or workload trying to access data, regardless of their physical location, network address, or access method, and then assigning only the access privileges associated with the authenticated entity. Zero Trust requires automation and orchestration so that component technologies can work together, and visibility and analytics to monitor, control, and govern the architecture.

SYMANTEC ACQUIRED, DEVELOPED, AND INTEGRATED SECURITY TECHNOLOGIES TO ADDRESS EMERGING THREATS AND PROTECT NEW PLATFORMS.

Well before the Zero Trust model was introduced by Forrester Research in 2009, Symantec had already assembled, developed, and offered every one of the technologies needed to implement the architecture, backed by Identity Governance and Administration solutions to automate review and certification of user access.

Zero Trust (cont.)

By the time the National Institute of Standards and Technology formalized it as SP 800-207, Symantec had taken further steps to merge Zero Trust technologies into its emerging cloud portfolio:

- **Secure Access Cloud**, a Zero Trust Network Access (ZTNA) SaaS solution to manage access to applications deployed in data centers or IaaS/PaaS clouds
- **Symantec VIP** cloud-based multifactor credentials and contextual risk analysis for unmanaged devices
- **Zero Trust data centric capabilities** built into Symantec Secure Web Gateway, CASB, Endpoint, and Email solutions, enabled by integrated Symantec DLP

ZERO TRUST AND SASE COMPONENT TECHNOLOGIES WERE ALREADY AVAILABLE FROM SYMANTEC AT THE TIME THEY WERE CODIFIED.

Secure Access Service Edge (SASE) Technology

Codified by Gartner analysts in 2019, SASE is the convergence of network and data security functions as cloud services delivered directly to users at the network edge. SASE promises to improve network and application performance, strengthen security, reduce complexity, and cut costs. A major advantage is its avoidance of the costs and latency of backhauling all traffic through centralized data centers, as is done with Virtual Private Networks, for example. In 2021, Gartner defined Secure Services Edge (SSE) as a productized subset of SASE that can be delivered as a complete solution.

As with Zero Trust, its component technologies were already available from Symantec at the time SASE was codified. Table 2 illustrates how Symantec technologies are aligned to the Gartner SASE framework, as validated by third-party Tolly Enterprises, LLC.

Table 2: Symantec SASE Technologies

Gartner Framework Component	Functional Area	Current Symantec Solution
Secure Web Gateway	Secure Web Gateway • URL Threat Prevention & Classification • Advanced Content Analysis (Malware sandboxing)	Symantec Web Protection
CASB	Cloud Application Security Broker (CASB)	Symantec DLP Cloud
ZTNA/VPN	Zero Trust Network Access	Symantec Secure Access Cloud
FWaaS	Cloud Firewall	Symantec Web Protection
Remote Browser Isolation	Remote Browser Isolation	Symantec Web Protection
Decryption	SSL Inspection	Symantec Web Protection
Data Loss Prevention	Data Loss Prevention	Symantec DLP Cloud

Source: Tolly Enterprises LLC Report #222122, July, 2022

Where alignment with the framework is inexact, it is often because Symantec includes a technology (for example, protecting data at rest) or environment (for example on-premises) underrepresented in the original framework.

SYMANTEC ENTERPRISE MARKET PENETRATION

- **195** COMPANIES IN THE FORTUNE 500
- **697** COMPANIES IN THE GLOBAL 2000
- **13 OF 13** TOP BANKS
- **8 OF 10** TOP TELECOM COMPANIES
- **7 OF 10** TOP AUTOMAKERS
- **150M+** ENTERPRISE USERS WORLDWIDE

Broadcom Acquires Symantec Enterprise

In November 2019 Broadcom acquired the Enterprise Security business of Symantec Corporation, with the stated goal of "... expanding our footprint of mission critical infrastructure software within our core Global 2000 customer base."

Symantec's Enterprise Security business—detached from its small-business and Norton consumer lines—was and remains closely aligned with Broadcom's strategic focus on the world's largest companies. As the sidebar shows, Symantec products enjoy excellent penetration of this premium segment, and retain plenty of room to grow.

The acquisition had dramatic effects on Symantec strategy. Long-term growth replaced quarterly revenue as its primary focus, and spending was redeployed from the pursuit of new accounts to consulting and support for established customers.

Like Marketing and Sales resources, innovation was marshalled to advance the interests of Broadcom's global customer base, focusing on the areas most important to those clients:

- **Compliance**—a major driver for large multinationals, and growing fast as new regulatory authorities assert themselves and older ones fragment regionally.
- **Integration**—a priority for large companies any time, enhanced now by opportunities to integrate Symantec solutions with Broadcom ValueOps™, AIOps, and other enterprise software.
- **Work-from-anywhere**—an accomplished fact post-pandemic, and a significant challenge to build a secure, productive user experience on top of infrastructure that wasn't designed for it.
- **Hybrid and multi-cloud environments**—on-premises infrastructure is out of fashion, but data residency and security concerns keep most multinationals from going all-in on the cloud.

Following the Broadcom acquisition, the pace of new-product announcements and press releases abated, and many analysts thought Symantec had "gone dark" on innovation. But this period was in fact one of the busiest, most productive, and most innovative in its history, as Symantec rebuilt its entire security infrastructure in the cloud, to serve the needs of its global clients.

Post-Acquisition Innovation

After the Broadcom acquisition, it quickly became clear that to serve enterprise customers from the cloud at high performance levels, Symantec needed to replatform its cloud portfolio.

Strategic Partnership with Google

We saw above that a SASE architecture delivers security services directly to devices at the network edge, eliminating the wasteful "touch base" with the home data center for every transaction. But speed and latency still matter in the cloud: if the edge network is bandwidth-constrained or physically distant from a user's device, latency will grow and performance will suffer.

To drive these constraints to an absolute minimum, Broadcom Software rewrote and replatformed its entire offering—more than 80 products and services, including all Symantec solutions—as Software-as-a-Service solutions

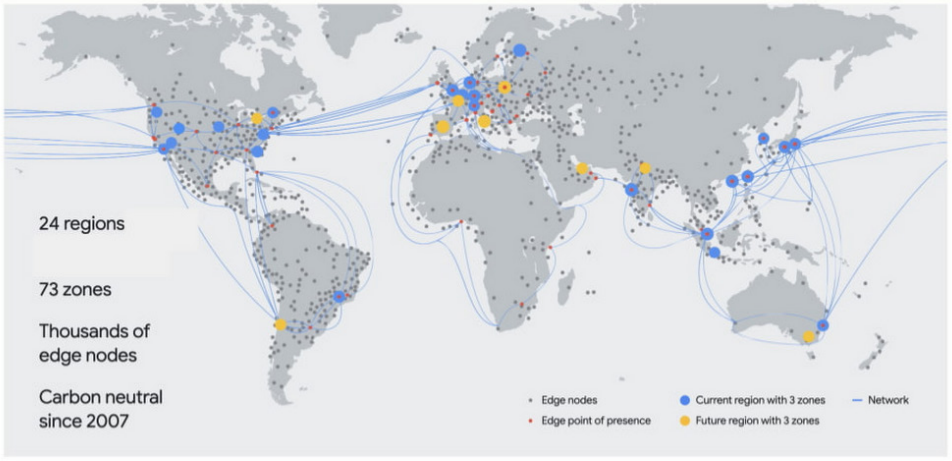
Strategic Partnership with Google (cont.)

on Google Cloud infrastructure, in containerized environments under Kubernetes orchestration. Google now provides Broadcom and Symantec users the following advantages:

- **Global range**, interconnecting ISPs, content providers, and users on a high-speed private network
- **Edge points of presence (POPs)** on 180+ internet exchanges and at 160+ interconnection facilities worldwide (see Figure 1, below), reducing costs and latency
- **Efficient routing** on Google's private backbone, minimizing traffic over the public Internet
- **Unmatched scale**
- **Elasticity** in response to unpredictable changes
- **Stability** and resilience in the face of disruptions

While the 18-month migration unquestionably had an impact on its customers, Symantec now delivers cloud-delivered security at superior performance levels, as validated by third parties. Compared to the public Internet, Symantec SASE on Google Cloud delivered 144% greater throughput with 62% lower latency for encrypted traffic, and 14% greater throughput with 19% lower latency for unencrypted traffic. The Symantec advantage in total transaction time grew with the physical distance between parties, from 21% better than public Internet for same-city transactions, to 62% better for California-to-Singapore transactions.

Figure 1: The Network Edge, as Defined by Google Cloud, February, 2021



Source: Google Cloud Blog

The Google Cloud backbone benefits Broadcom as well as its customers: users onboard faster, and the latest technologies assure consistently high service levels. Symantec also collaborated with Google to create Localization Zones—a way to make sure web content is localized for the country where the request originates, even when the ISP is located outside its borders. For its initiative—and assistance—Broadcom received Google Cloud's Customer of the Year Award for 2021.

Innovation by Product Line

None of this should be taken to indicate that product innovation stopped in the period following Broadcom's acquisition of Symantec. Broadcom is, after all, a company that reinvests more than 20% of its revenue in R&D year after year as a matter of policy. Table 3 shows a sample of the product innovations introduced by Symantec after the Broadcom acquisition, including during the height of its Google Cloud replatforming effort.

Table 3: Symantec Post-Acquisition Innovations

Symantec Innovations by Product Line
ENDPOINT SECURITY
• Adaptive Security consolidates information from agents across a geography, department, or other entity to respond to local conditions, not a global common denominator. • New dashboards highlight unusual behaviors on high-risk apps: PowerShell, Net.exc, etc., to thwart ransomware "live off the land" and targeted attacks. • Endpoint management console moved to the cloud. • Solution regionalization, to address data sovereignty and other regional issues. • Threat Defense for Active Directory (TDAD) protects Active Directory integrity, obfuscates AD, and counteracts credential-stealing and lateral migration typical of ransomware attacks. • Agent consolidation: Single agent to integrate traffic steering needed for Cloud SWG.
INFORMATION SECURITY
• Continuous development of Data Loss Prevention from version 15 to 16, with 17 on the way. • New policies based on risk-scoring using Information Centric Analytics, built on UEBA capabilities, but usable by Business Units. • Consolidation across events for easier management. • Quarantining organized using ServiceNow integration, reducing the need for monitoring. • GDPR compliance innovations, for example obfuscation that allows administrators to look at events without violating privacy regulations. • CASB now offers Oracle management via the cloud version of Enforce. • CASB has added API, Securlet, and Gateway solutions for data trust and data in motion.
NETWORK SECURITY
• Secure Web Gateway is now offered as virtual machines or as a cloud service with a single console for all form factors. • Multiple network capabilities are now available as a single SWG solution including Cloud SWG, Edge SWG, Isolation, Content Analysis, SSL Inspection, App Visibility and Control, Intelligence Service and Centralize Management & Reporting. • Newly developed Cloud Firewall Service launched and added to all SWG customers. • Selective traffic steering integrated into Secure Web Gateway and the consolidated endpoint security agent of Symantec Enterprise Security Complete. • Agent-based and agentless ZTNA is now an alternative to VPN, with lower cost, fewer security issues, and less complexity.
PLATFORMS AND ENVIRONMENTS
• A single Symantec Enterprise Security Complete agent consolidating Secure Web Gateway, Zero Trust Network Access, CASB and Endpoint capability. • Moving toward the hybrid—not cloud-only—platform large multinationals need. • Extending user and entity behavior analytics (UEBA) from on-premises to CloudSOC CASB and DLP Cloud. • Introducing Mirror Gateway technology to allow completely unmanaged devices, with no agents of any kind, to access corporate networks safely. • Extending the DLP agent to cover macOS and Linux. • Created Localization Zones to localize web content for the geographic origin of a request, regardless of the ISP's location.

Many of these innovations constitute integrations or extensions of a technology across on-premises, private/hybrid, and public clouds. A long-time Symantec goal—a single agent and console across Symantec Enterprise Cloud—is coming within reach, and already exists for the cloud. The company is also moving toward a single console, for a substantial reduction in management overhead.

Business Innovations

Just as it invests to improve the manageability of its products, Symantec innovates to streamline and accelerate its own business processes for the benefit of enterprise customers. Hundreds of SKUs categorized by function, computing environment, platform, and more are now available under consolidated, simplified, per-user annual pricing that offer unrestricted access to a security category—endpoint, identity, network, data, and more. Enterprise customers that now hold twenty or thirty contracts with Symantec—with an assortment of terms and expiration dates—can now achieve the complete protection of Symantec Enterprise Cloud with just four. Customers realize the following benefits:

- Access to the full range of solutions in a product line, for protection without gaps
- Predictable annual costs, even when usage expands
- Lower overall cybersecurity costs
- Increased flexibility to try new cybersecurity technologies at no financial risk
- Simplified maintenance, upgrade and renewal processes
- Dedicated customer service arrangements to help customers get the most from solutions
- Customer choice of form factor to deploy or redeploy security capabilities: software, hardware, virtual on IaaS, or SaaS, within a single contract

These pricing plans are available for most Broadcom Software products, opening the prospect of simplified company-wide contracts covering cybersecurity, automation, DevOps, and other Broadcom technologies.

Community and Standards Innovations

As regulatory and standards compliance looms larger in the decision-making processes of multinational corporations, it becomes more important for them to have an advocate who understands the issues and likely business impacts of those decisions. Symantec has taken on that role for years, advising the U.S. Government, European Union, United Nations, and an assortment of technical bodies, advocating policies to protect its customers without imposing unnecessary burdens on their operations. The callout below details some of the most important examples.

SYMANTEC COMMUNITY AND STANDARDS INNOVATIONS

- Symantec is the leading cybersecurity vendor presence on the Internet Engineering Task Force (IETF) and International Telecommunications Union (ITU), the United Nations community that defines the future of Telecommunications and Information and Communications Technology. In the past few years, Symantec has contributed to the following endeavors:
  - Participated in ITU-T Study Group 17–Security, to develop **global security standards**. The company recently seconded a Symantec employee to serve as Vice President of the Study Group.
  - Contributed its Integrated Cyber Defense schema to the Open Cybersecurity Schema Framework (OCSF) project in an effort to break down data silos and normalize data between cyber security solutions for faster data analysis. This **blog post** and this **article in *Forbes*** describe the significance of this innovation.
  - Been at the forefront of TLS 1.3 decryption efforts, representing its customers' need to inspect traffic for malware that may be cloaked by advanced encryption. **This blog post** outlines the issues.
  - Prepared its solutions for Encrypted Client Hello (ECH), a TLS extension that closes the final gap in end-to-end transport layer encryption. Symantec identified a problem—again related to inspection—that put its customers at regulatory risk, and is active in defining a solution.
  - Countered "hyper-regionalization" of Internet standards, as regulations and standards intersect to create smaller and smaller islands of consistent regulation, with borders that can't be crossed without compliance tests and possible intervention.
- Symantec is represented and active in Brussels as the European Union Council presidency and European Parliament define the Digital Operational Resilience Act (DORA). As a result of its participation, Symantec products will be DORA compliant even before the Act takes effect.
- Symantec participates in the European Data Protection Board as a leader in Data Protection software. It recently identified a risk in the compliance audit process, and corrected it by obfuscating personally identifiable information during administrative review.

The Next Innovation Cycle

Symantec continues to innovate in security frameworks and architectures, with the goal to reduce management and compliance complexity, and the gaps and overlaps that plague patchwork security architectures. It has introduced an enterprise-spanning solution that extends the Gartner SASE framework to sharpen its focus on data protection, compliance, and threat intelligence.

Symantec Enterprise Cloud

The solution, Symantec Enterprise Cloud (SEC) is based on these principles:

- **Consolidation:** Multiple endpoint agents drain client resources, add complexity, and increase costs. SEC's single agent for all endpoints—laptops, desktops, tablets, phones, servers, and cloud workloads—stops agent sprawl, reduces complexity, and gives managers a single view across all endpoints. Consolidated with the Cloud Secure Web Gateway, the agent provides both endpoint and network security to roaming endpoints.
- **Hybrid cloud:** Many organizations must maintain a corporate data center for business, legal, or regulatory reasons: their cloud migration will always be to a hybrid cloud environment. For them, Symantec Enterprise Cloud can be deployed as a single entity spanning on-premises and cloud environments, with unified management of both. Alternatively, it can be deployed as a 100% on-premises solution with an on-premises enforcement point, or as an entirely cloud-based implementation with the enforcement point in the cloud.
- **Data and threat protection together:** Symantec Enterprise Cloud combines Data Loss Prevention (DLP) to protect data crossing networks, gateways, and endpoints, with threat protection to identify and mitigate attacks. Threat detection capabilities are fed by Symantec threat hunting teams and the Symantec Global Intelligence Network, which uses artificial intelligence to distill over nine petabytes of data into actionable threat information.
- **SOC integration:** Integration among cybersecurity tools allows our team of highly skilled threat hunting team to evaluate threat information, discern patterns, block attacks, and engage with customers to augment their SOC operations.
- **Compliance:** SEC applies and manage compliances controls consistently across organizations. A single governance team can manage data risk and perform audits from one platform, on-premises or in the cloud.
- **SSE:** Support for Secure Service Edge (SSE) is part Symantec's hybrid capable, data-centric security architecture.

What's Next?

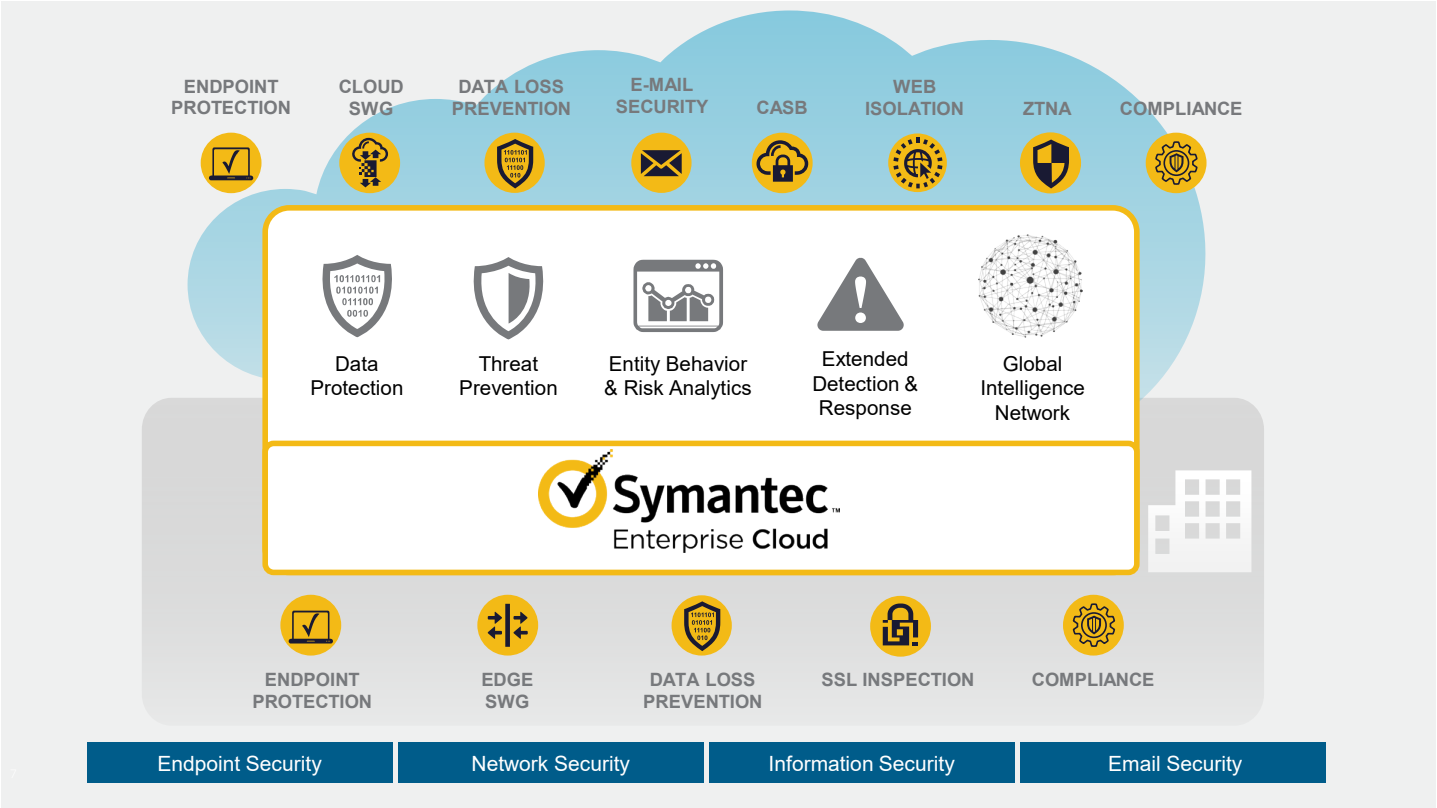
Over the next few years, Symantec products will integrate seamlessly with one another as the company continues to refine and execute its vision for Symantec Enterprise Cloud. Customers can look forward to:

- A single Symantec agent across technologies, platforms, and environments—a long-time cyber security goal, now within reach
- Consistent management of compliance, securing remote work, and data and threat protection across the entire enterprise environment
- Capabilities delivered in product upgrades covered under then-current licensing agreements

What's Next? (cont.)

Consolidation is the key to simplicity, effective management, consistent compliance, an improved user experience, and more effective use of both internal (logs) and external (intelligence) data. Symantec Enterprise Cloud delivers all of it, and is available at simple, per-user annual pricing covering Endpoint, Network, Information, and Email Security solutions enterprise-wide.

Figure 3: Symantec Enterprise Cloud



Conclusions

A narrow view of innovation focuses on niche product development by startups, and favors trends like today's cloud-only solutions. A broader view considers all the ways companies innovate: through acquisitions, in thought leadership, by aligning their solutions with customer requirements, and by shaping the business and regulatory environments.

Over its history, Symantec has remained at the forefront of all these forms of innovation in cyber security. As a division of Broadcom, Symantec continues to innovate its products, business models, and community efforts on behalf of its customers.

BROADCOM SOFTWARE

About Broadcom Software

Broadcom Software is a world leader in business-critical software that modernizes, optimizes, and protects the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software has an extensive portfolio of industry-leading infrastructure and security software, including AIOps, Cybersecurity, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

SYM-SI-WP100 December 1, 2022