



Enterprise Strategy Group | Getting to the bigger truth.™

ESG WHITE PAPER

The Need for Security Consolidation

Why Siloed Point Solutions Will Never Be Enough

By John Grady, ESG Senior Analyst

October 2022

This ESG White Paper was commissioned by Symantec, a division of Broadcom, and is distributed under license from TechTarget, Inc.

© 2022 TechTarget, Inc. All Rights Reserved.



Contents

Executive Summary	3
Enterprise Complexity Has Put Security at a Tipping Point	3
Complexity Creates Specific Challenges around Compliance, Securing Hybrid Work, and Threat Prevention.....	4
Tool Sprawl Has Led to Interest in Platforms, But.....	5
Organizations Should Prioritize Vendor Reduction and Comprehensive Security Solutions	6
Introducing Symantec Enterprise Cloud	8
The Bigger Truth	9

Executive Summary

Many enterprises are overwhelmed when it comes to cybersecurity. The threat landscape continues to expand as attackers seek to take advantage of the widening attack surface in today's hybrid, multi-cloud enterprise environments. At the same time, security teams struggle to efficiently and effectively manage an ever-growing number of point products meant to secure users, resources, and data across on-premises and cloud locations.

The growing security workload has been exacerbated by the massive talent shortfall that cybersecurity is experiencing, which makes it nearly impossible for organizations to attract and retain incremental security experts required to effectively manage the growing number of security tools offered by the range of established and start-up security vendors, each trying to carve out its own cybersecurity niche. This has left many enterprises struggling to efficiently maintain compliance, effectively enable remote and hybrid work, and comprehensively protect data and prevent threats.

The idea of cybersecurity platforms has gained traction as a way to alleviate these issues. However, in most cases, platforms require multiple vendors' products connected via open standards and APIs to address the wide range of needs of the enterprise customer. Unfortunately, this does little to reduce the complexity security teams face in terms of procuring, deploying, and managing tools from a variety of vendors. This ultimately makes it difficult to deliver better security and compliance results.

Enterprises should consider consolidated, single-vendor solutions to address these challenges. This approach can help reduce costs and simplify vendor management.

Further, when procured from an established, enterprise-class vendor with the capabilities to address a wide variety of use cases, organizations should expect better security, more efficient security operations, and consistent compliance.

Symantec Enterprise Cloud is an example of such a solution and provides data-centric hybrid cybersecurity, supported by a global threat intelligence network, with a broad portfolio of capabilities across endpoint security, network security, information security, and email security.

Symantec Enterprise Cloud provides data-centric hybrid cybersecurity, supported by a global threat intelligence network, with a broad portfolio of capabilities across endpoint security, network security, information security, and email security.

Enterprise Complexity Has Put Security at a Tipping Point

Cybersecurity continues to grow in complexity. In fact, 59% of ESG research respondents say that cybersecurity has become more difficult than it was just two years ago. There are a variety of factors driving this complexity (see Figure 1).¹ Some of the most significant include:

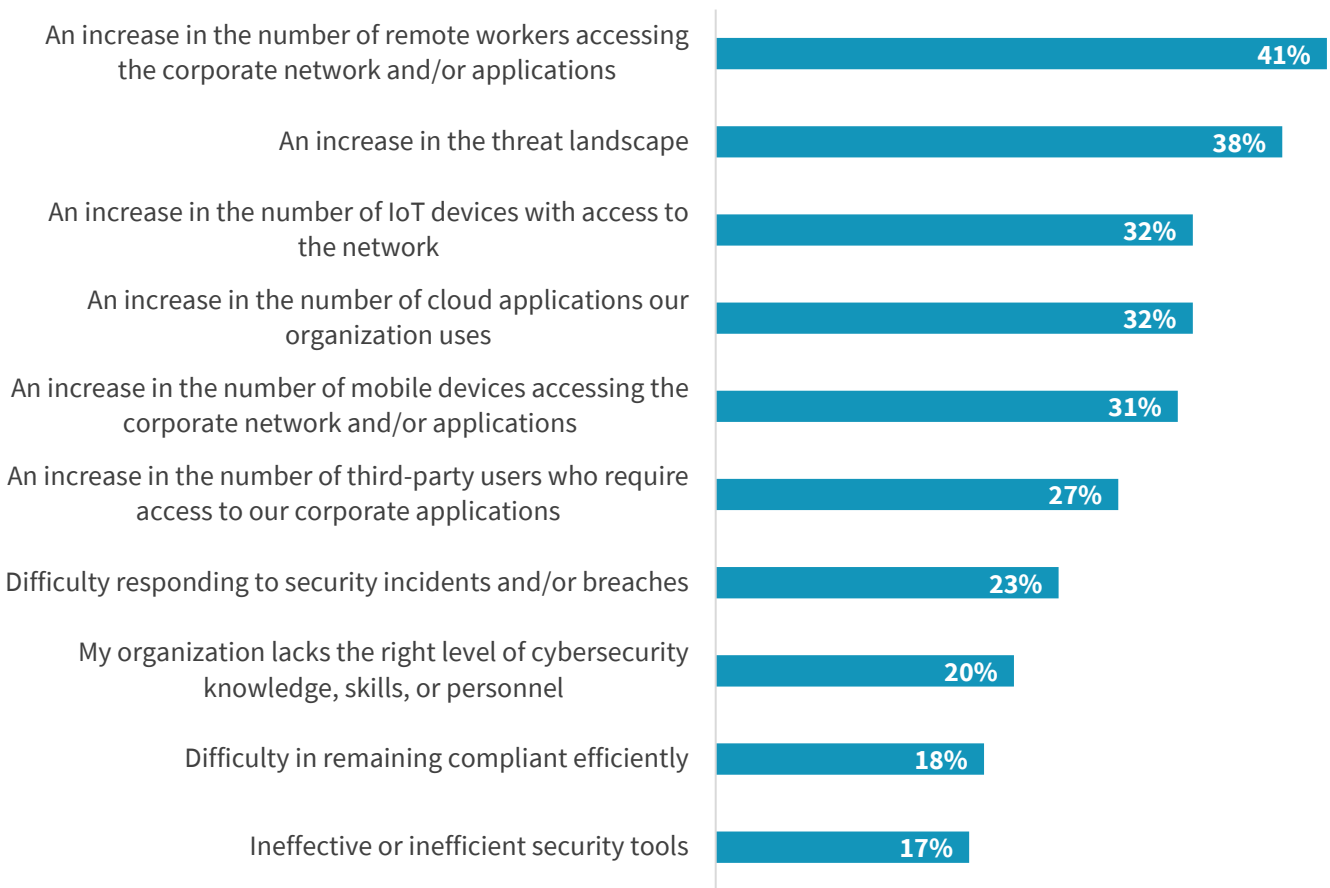
- **The distributed nature of the modern enterprise.** Users, applications, and resources are all likely to be located outside of traditional corporate offices and data centers. The modern enterprise must defend not a static, well-defined perimeter, but a sprawling and dynamic collection of entities that may be located anywhere in the world.
- **The evolving threat landscape.** Cybercrime has become a sophisticated business, with attackers often being extremely well-funded and highly motivated. Software supply chain attacks, ransomware, and advanced targeted attacks continue to make headlines and disrupt business operations for organizations of all types and sizes.

¹ Source: ESG Survey Results, [The State of Zero Trust Security Strategies](#), May 2021.

- **Ineffective tools.** Many of the established tools security teams have been relying on for years have become less effective due to the changes above. They may lack the visibility required to detect sophisticated threats, fail to properly secure remote users and cloud resources, or add complexity to response workflows when incidents do occur.
- **The skills shortage.** Adding to the aforementioned issues is the skills shortage, which can take multiple forms. Finding enough people continues to be an issue for many organizations. Yet, even in instances where roles are filled, personnel may lack the necessary skills to effectively perform their job (for example, tier-1 SOC analysts being asked to perform tier-2 functions).

Figure 1. Reasons Cybersecurity Has Become More Difficult

In your opinion, which of the following factors have been most responsible for making cybersecurity management and operations more difficult? (Percent of respondents, N=249, three responses accepted)



Source: ESG, a division of TechTarget, Inc.

Complexity Creates Specific Challenges around Compliance, Securing Hybrid Work, and Threat Prevention

These issues have created critical challenges in three key areas: compliance and governance, hybrid work, and effective threat prevention.

1. **Compliance and governance** issues have only become more pronounced as the regulatory environment has expanded. While the GDPR was the first major data privacy framework to be put in place, others, such as the

California Consumer Privacy Act (CCPA), have followed, with more on the way, such as the Virginia Consumer Data Protection Act. Established standards such as HIPAA and PCI DSS continue to evolve as well. Gaining an accurate and timely view of the organization’s compliance to so many regulations has become increasingly difficult, as the number of security tools used has grown.

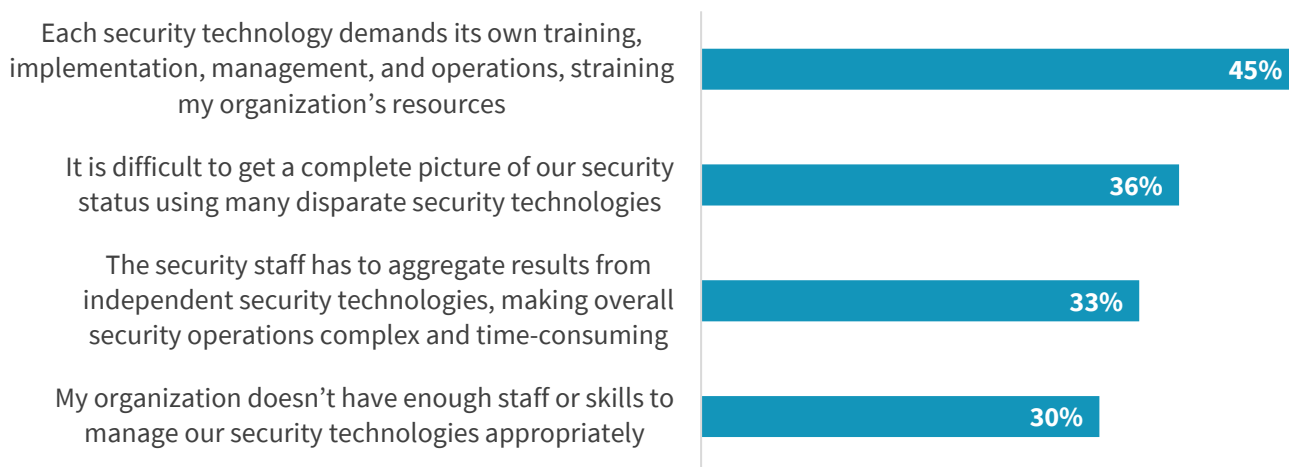
2. **Changing work models** continue to challenge organizations more than two years after the beginning of the pandemic. Many still struggle with the foundational elements of effectively providing secure access for users working remotely. With the shift to hybrid models well underway, organizations now must ensure both consistent security and a uniform user experience for users regardless of whether they are in the office or working remotely.
3. **Maintaining effective threat protection** is more difficult than ever due to all the factors mentioned previously: bad actors have more effective tools and tactics at their disposal than ever before, the attack surface is more distributed and thus harder to defend, security tools often work in silos rather than in concert with one another, and security teams often do not have the skills necessary to be effective.

Tool Sprawl Has Led to Interest in Platforms, But...

ESG research has found that 47% of enterprise organizations (those with more than 1,000 employees) use 11 or more cybersecurity technology vendors. Further, a third of enterprises say they rely on 25 or more different cybersecurity technology products. ESG research respondents have reported a variety of issues from utilizing this number of siloed point tools (see Figure 2).² Some of the most significant challenges include the separate training, deployment, and management required for each tool; difficulty accurately understanding the organization’s security posture; and the added complexity to security operations overall.

Figure 2. Top Four Challenges In Using a Variety of Point Tools

Which of the following represent the biggest challenges associated with managing an assortment of security products from different vendors? (Percent of respondents, N=280, three response accepted)



Source: ESG, a division of TechTarget, Inc.

² Source: ESG Complete Survey Results, [ESG/ISSA Cybersecurity Process and Technology Survey](#), June 2022. All ESG research references and charts in this white paper are from this survey results set, unless otherwise noted.

As a result, 46% of large organizations are currently consolidating or are considering consolidating the number of cybersecurity vendors with whom they do business to help ease these burdens. At the same time, the industry has begun to focus on platforms that integrate multiple tools or security services, delivering them as an integrated entity. Many cybersecurity vendors have positioned their portfolios of point products as cybersecurity platforms to raise their stature in the eyes of enterprise security professionals as the demand for platform-based solutions continues to increase.

However, the term “platform” itself has become overused and misunderstood by the industry and by enterprises looking for more integrated solutions. ESG research has found that 67% of cybersecurity professionals believe that a platform is defined as an agreed-upon standard architecture provided by multiple vendors as an open suite of heterogeneous products integrated through standard APIs and development tools. While this may sound appealing on the surface, this approach does not necessarily mean these platforms are easy to deploy, use, or maintain. Further, while adopting a platform may help streamline security efforts to an extent, it does not directly support the need for consolidation that many organizations are searching for to reduce costs, simplify procurement and processes, standardize policies, and, ultimately, strengthen security.

Organizations Should Prioritize Vendor Reduction and Comprehensive Security Solutions

There are a variety of benefits organizations can realize by reducing the number of security vendors and investing in comprehensive, consolidated cybersecurity solutions, whether or not the solution identifies itself as a platform (see Figure 3). Reducing the number of vendors an organization does business with simplifies procurement by also reducing the number of contracts, reducing complexity, and streamlining procurement and deployment. From the procurement perspective, the fewer cybersecurity vendors the better.

There are a variety of benefits organizations can realize by reducing the number of security vendors and investing in comprehensive, consolidated cybersecurity solutions.

Perhaps the largest benefit of consolidating to a single vendor is gaining the ability to leverage a shared intelligence database that not only ensures information shared between parts of the vendor’s solution doesn’t get lost in translation, but also can identify threats faster than disconnected point products where critical intelligence might slip through the cracks.

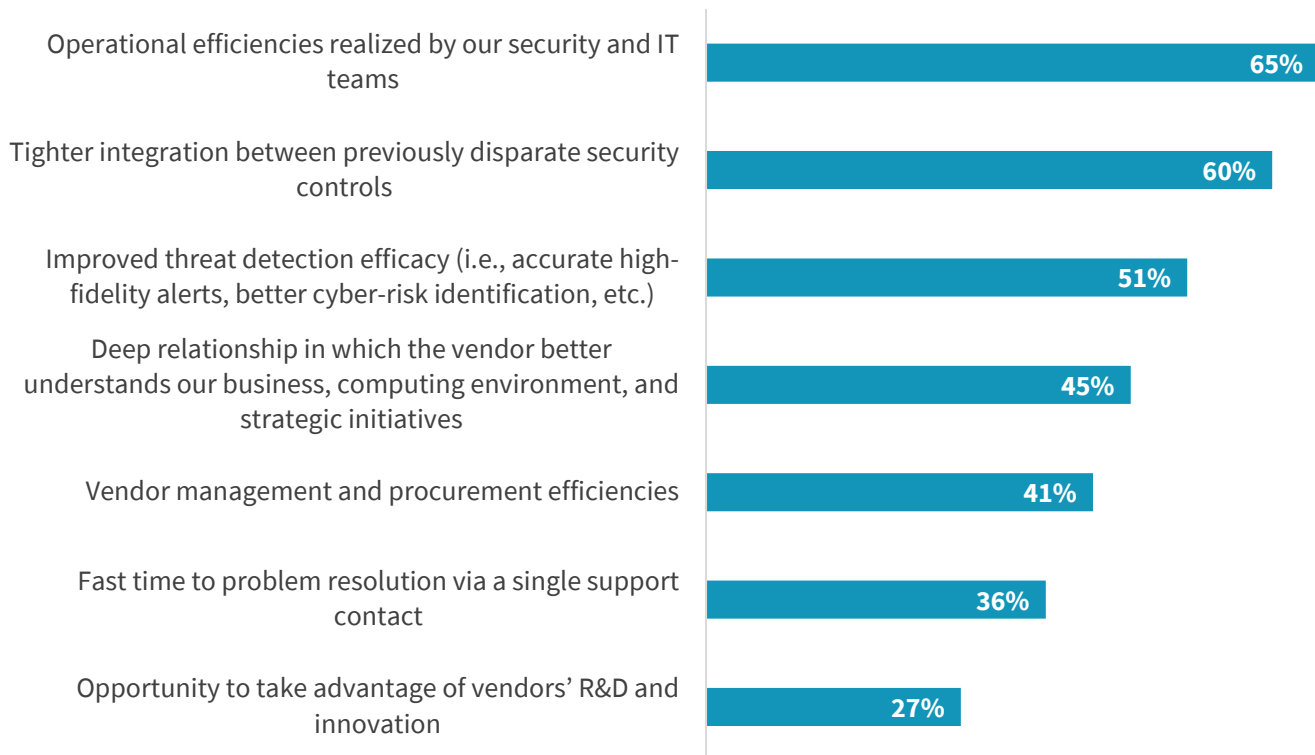
Consolidation also can lead to improvements for the ease of use of a cybersecurity solution, especially when a comprehensive solution is designed to leverage a common user interface (UI). This can greatly accelerate the ability to learn and access multiple security capabilities and functions without the need to re-learn the basics for each tool. Further, the centralized reporting a consolidated solution offers can streamline compliance reporting and help ensure adherence to any relevant regulatory requirements.

Consolidation to a single vendor also opens the door for a single agent, which will reduce the total footprint for security tools, reduce or eliminate conflict between multiple security products, simplify operations with unified management, and create a better overall end-user experience.

Doing business with fewer vendors also helps streamline reporting for security incidents, since having a single log enables the enterprise to have a single source of the truth for event tracking and access attempts, making it easier to surface anomalies before they become problematic.

Figure 3. Value Expected from Reducing the Number of Security Vendors Used

Which of the following best represents your organization's perspective on the value of procuring cybersecurity solutions from **fewer** enterprise-class cybersecurity companies?
(Percent of respondents, N=130, multiple responses accepted)



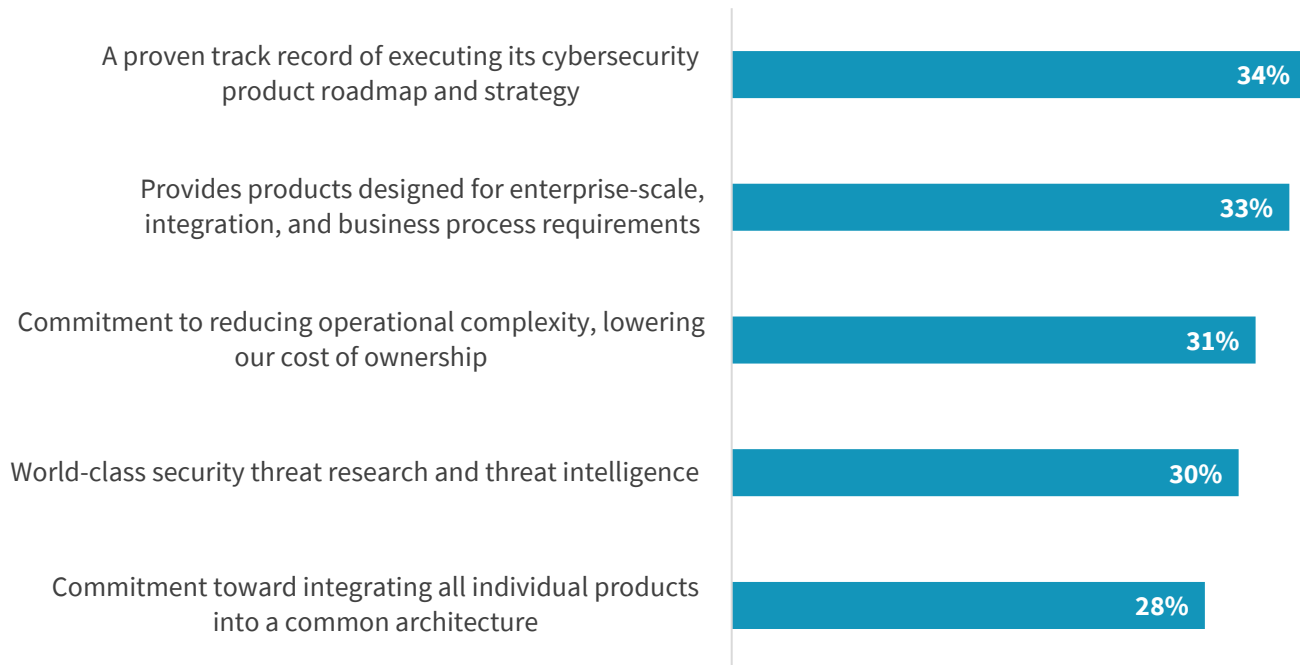
Source: ESG, a division of TechTarget, Inc.

Several leading cybersecurity vendors now offer broad enterprise coverage with proven capabilities and platforms that span on-premises, cloud, SaaS, and hybrid environments to further reduce complexity. When considering a consolidated solution or platform, it is important that it includes capabilities to support hybrid work, the ability to secure enterprise data regardless of its location, and the ability to protect enterprise assets of all kinds.

Enterprise security teams should choose a vendor that offers support of broader security initiatives. Although newer offerings like secure access service edge (SASE), extended detection and response (XDR), and zero trust are all important today—and will all certainly remain important in the future—trends do shift quickly, so vendors must be agile with platform solutions that can adapt as new initiatives emerge to support evolving security approaches without breaking existing security. Typically, this means choosing those vendors that have the right technological breadth and depth to deliver on evolving or emerging security trends in the months and years to come.

Figure 4. Top Five Attributes for Enterprise Cybersecurity Vendors

In your view, which of the following attributes would you consider to be the **most important** for an enterprise-class cybersecurity vendor? (Percent of respondents, N=280)



Source: ESG, a division of TechTarget, Inc.

Introducing Symantec Enterprise Cloud

One solution that meets these requirements is Symantec Enterprise Cloud, a data-centric hybrid cybersecurity offering that is available as a complete enterprise solution. Symantec Enterprise Cloud is supported by a global threat intelligence network that analyzes 11 trillion elements of telemetry, which entails ingesting billions of new data points each and every day. This enables Symantec to provide visibility across endpoints, networks, email, and the cloud and paints a broad and comprehensive threat picture for enterprises that utilize multiple Symantec offerings. Additionally, Symantec collects data from other security vendors' products, which gives enterprises a complete view into suspicious or anomalous activity regardless of where it is flagged.

Symantec Enterprise Cloud is available through a portfolio licensing agreement (PLA). The PLA covers Symantec's Endpoint Security, Network Security, Information Security, and Email Security portfolios to meet the individual needs of any enterprise, up to and including delivering complete security services edge (SSE) and extended detection and response. Through this consolidated approach, Symantec Enterprise Cloud helps organizations improve the efficiency and effectiveness of compliance management and remote work enablement, while providing data and threat protection everywhere. Benefits of the Symantec PLA include:

- Consistent compliance enforcement across on-premises, cloud, and hybrid environments to prevent issues from slipping through the cracks.
- Support for cloud transformation efforts of any size and at any scale, all on the enterprise's timeline, so there is no need to rush a migration due to possible security lapses during migration.

- A flexible consumption-based pricing strategy in which enterprises can pay only for the elements they use, helping to reduce overall security expenditures, or choose to sign up for all capabilities from day one.
- Improved effectiveness of security personnel and the SOC by providing broad, comprehensive, trusted, and actionable data across all control points, as well as by eliminating the need for security teams to learn multiple vendor user interfaces.

Symantec Enterprise Cloud supports a variety of use cases across the different portfolios comprising the solution. These include:

- **Protecting users accessing the internet.** Symantec Web Protection provides flexible hybrid deployment models through a “buy once, use anywhere” software licensing model. The product includes secure web gateway, content and file inspection, high risk isolation, and firewall-as-a-service capabilities.
- **Ensuring secure access to, and the protection of, private applications.** Symantec Network Protection includes everything in Web Protection plus zero trust network access, sandboxing for unknown file types, and full web isolation. This helps organizations ensure private applications are available only to those users that require access and are protected from unauthorized access, malicious uploads, and other threats.
- **Securing cloud-resident data.** Symantec DLP Cloud provides full CASB functionality to protect against threats, provide visibility, and extend DLP policies to both sanctioned SaaS and IaaS deployments and across shadow IT. This ultimately helps ensure data residency requirements and address regulatory compliance concerns.
- **Accurately securing data across all channels.** Symantec DLP Core allows customers to accurately discover and protect sensitive data. The ability to apply a “write once, enforce everywhere” policy helps streamline DLP management. The product includes coverage for endpoint, network, and storage; fully integrates with DLP Cloud for hybrid deployments; and includes user and entity behavior analytics to improve detection of insider threats and advanced attacks on sensitive data.
- **Protecting endpoints and threat response.** Symantec Endpoint Security Complete provides protection across all devices, including mobile. The single agent model supports traditional endpoint protection, endpoint detection and response (EDR), and extended detection and response capabilities. Additionally, the product prevents credential theft with Active Directory Defense.

The Bigger Truth

Security teams have a wide range of goals and key performance metrics they are measured against. Yet, at the end of the day, these can be distilled down into three key areas: are the controls required to remain compliant to the relevant regulations in my industry in place, am I enabling my employees to be securely productive, and am I prepared to protect my data and prevent threats in my environment? Unfortunately, the shift to the cloud, adoption of remote and hybrid work, proliferation of point tools, and acute shortage of cybersecurity skills have made achieving these goals more difficult than ever.

Consolidation, when supported by a well-established enterprise-class vendor with proven technology, can help improve compliance management, enable remote work, and improve data protection and threat prevention effectiveness. Symantec has the breadth of capabilities, wealth of threat intelligence telemetry, and cybersecurity track record to deliver comprehensive data-centric hybrid security for the large enterprise through Symantec Enterprise Cloud.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188