White Paper

Symantec
A Division of Broadcom

Integrated Cyber Defense

Essential Security Solutions Working Together to Protect Your Business

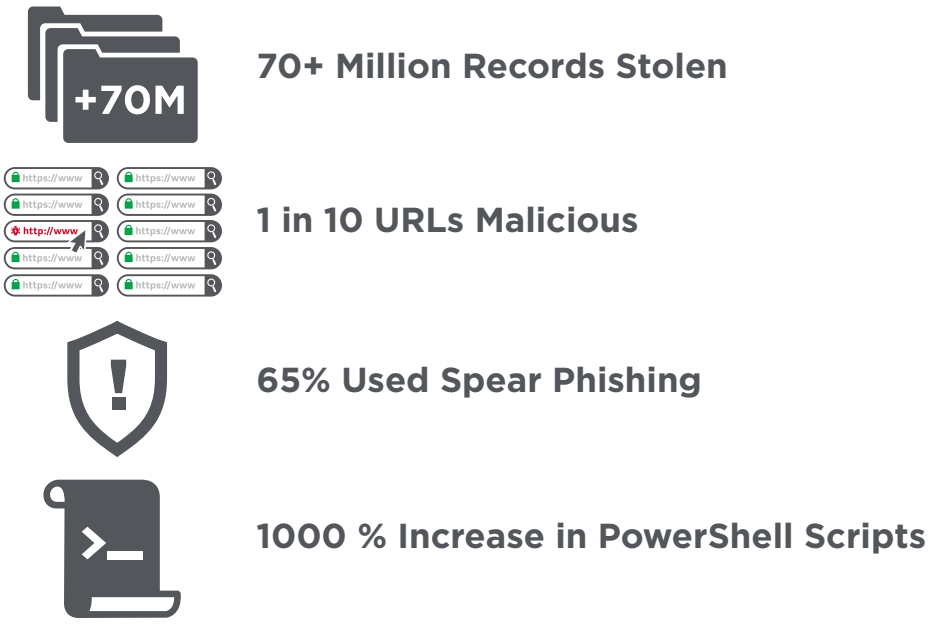
Table of Contents

Introduction

Digital channels have become the primary business and customer-engagement model pushing organizations to accelerate digital initiatives to survive in a rapidly changing environment. With digital now central to every interaction, the demand for cloud services and mobile technologies continues to increase. Cloud-enabled operations offer many benefits—from business continuity, increased business agility, and cost-savings to improved customer experience. Digital transformation, however, also comes with digital risk. The growth of cloud and mobile technologies generates more endpoints and identities to manage, more networks to secure, and more credentials and data to protect. The result is an expanding attack surface and an increasing number of vulnerable assets that place an increased burden on security leaders.

As companies digitize operations, cyber risks proliferate, with adversaries exploiting multiple vectors to infiltrate. In 2018, more than 70 million records were stolen or leaked as a result of poor Amazon Web Services configuration. One in 10 URLs were malicious. Sixty-five percent of attacks used spear phishing and 48 percent of all malicious email attachments were Microsoft Office files—up from five percent the previous year. With a 1000 percent increase in PowerShell scripts, living off the land attacks became a cybercrime mainstay. Nearly one in ten targeted attack groups now use malware to destroy and disrupt business operations, a 25 percent increase from the previous year.[1]

Figure 1: Proliferation of Cyber Risks



Complexity is the Enemy

Security and IT organizations must react quickly and aggressively to enable the enterprise's digital aspirations. However, fundamental challenges arise when understaffed cyber security teams leverage legacy cyber security operating models and point solutions to protect the organization. In addition to facing constrained budgets, 53 percent of organizations report a problematic shortage of cyber security talent.[2] Moreover, the cyber security talent crunch is expected to create 3.5 million unfilled jobs globally by 2021. [3]

Figure 2: Cyber Security Skill Shortage

53% Report Shortage of Talent

3.5 Million Unfilled Jobs Globally

For many organizations, the haphazard growth and expansion of security infrastructures has created a fragmented patchwork of expensive and complex tools that are time-consuming to integrate and manage, put extra strain on Security Operation Center (SOC) resources, and impede threat detection and response. On average, organizations have 45 security solutions and technologies in use.[4] While point security tools were adequate a decade ago, outdated systems and point solutions are insufficient for combating today's threat actors. The complexity of today's IT infrastructures combined with sub-optimal integration, inefficiencies caused by overlapping functionality, and the heterogeneity of security tools make it difficult for security pros to understand the resulting security gaps.

The Accelerating Shift to Integrated Cyber Defense

Burdened with a multitude of point-solutions, security leaders are consolidating security vendors to streamline the security stack, improve response, and reduce complexity. To manage risk more efficiently, digital organizations will need to leverage an integrated security architecture for unified visibility and intelligence, operational efficiency, and orchestrated security across all attack vectors. In addition to securing the enterprise, an integrated architecture must deliver rapid time to value. A successful integrated defense must therefore meet the following criteria:

- **Unify** on-premises and cloud-based security solutions and enable seamless deployment options
- **Collect, centralize, and share** data across all control points (endpoint, identity, network, cloud)
- **Integrate threat prevention, detection, and response** capabilities across all attack points, enabling the ability to automatically mitigate a threat when possible
- Offer an **open architecture**, ease of **third-party integration**, and robust third-party support

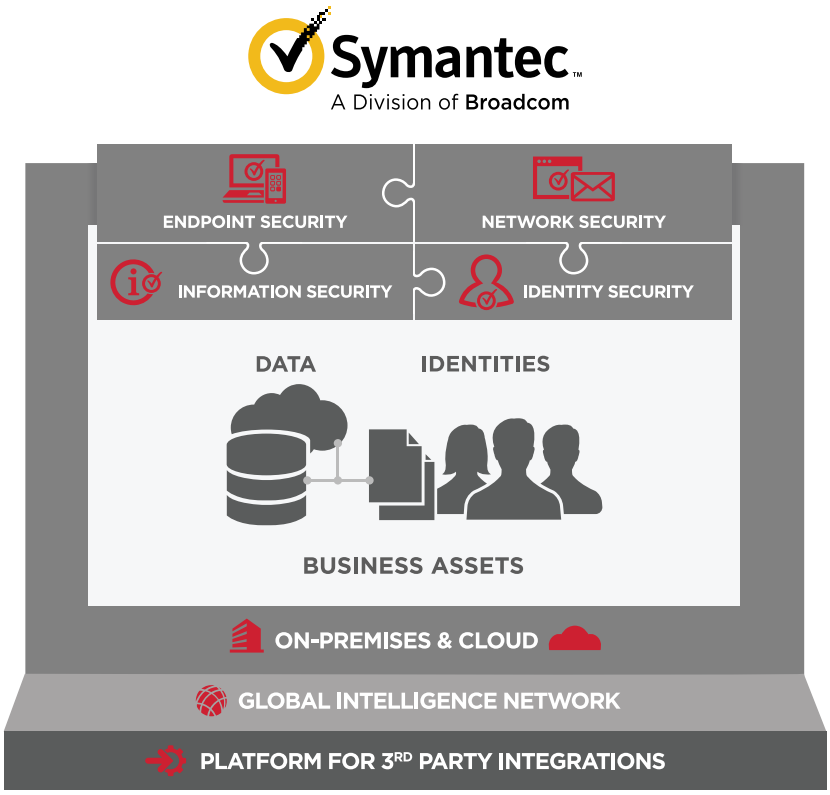
An integrated security architecture expands the security team's capabilities by providing end-to-end security orchestration, automation, and remediation, closing security gaps across vendors and product silos, centralizing and leveraging security data, and providing an omni-channel approach to identities. The security team can stop being product integrators and instead focus on what matters most.

Symantec™ Integrated Cyber Defense

As organizations embrace digital transformation and consider the principle of Zero Trust, or building a SASE architecture, there is strong appeal in leveraging an integrated approach to cyber defense. Symantec™ Integrated Cyber Defense unifies products, services, and partners to drive down the cost and complexity of cyber security—all while protecting enterprises against sophisticated threats. We combine best-of-breed information protection, threat protection, identity management, compliance, and other advanced services, powered by shared intelligence and automation across endpoints, networks, applications, and cloud app control points.

By natively integrating multiple security products into a cohesive system, Symantec Integrated Cyber Defense improves detection by coordinating the findings from individual products to detect and block events that might otherwise go unnoticed.

Figure 3: Symantec Integrated Cyber Defense



Organizations also need to be able to store and retrieve data from different places. PII data must be treated differently than non-PII data. Organizations need to set proper access rules, decide where the information gets stored, and account for privacy considerations. This requirement can get complicated as different regions around the country and globe have different regulations governing privacy. With integrated cyber defense, there's no guesswork. Symantec Integrated Cyber Defense offers a way to handle data in a normalized and centralized way, allowing for field filtering, types of events, and forwarding to the right destinations.

The Symantec Solution Difference

Through the ability to unify on-prem and cloud environments, leverage deep threat intelligence, and integrate third-party technologies, Symantec solutions are uniquely positioned to empower organizations to drive down the cost and complexity of cyber security and derive more value from existing cyber security technology investments.

On-Premises, Cloud, and Hybrid Environments

An overnight shift to digital has caused heartburn in many organizations—how do you unify what's on-premises and what is moving to the cloud?

Figure 4: Symantec Integrated Cyber Defense Ecosystem

Symantec, A Division of Broadcom, has the first and only solution that unifies and coordinates security functions across both cloud and on-premises systems. Enterprises can embrace the cloud as it makes sense for them, without sacrificing past investments and reliance on critical infrastructure.

Third-Party Integration

The acceleration of digital transformation initiatives is impacting cyber security in organizations and challenging security leaders to change the way they approach cyber security and risk. Against a backdrop of stagnant budgets and dissatisfied boards, security leaders must not only modernize their approach to cyber security and risk, but also continue to protect the investment in the existing security stack.

Symantec Integrated Cyber Defense provides an open ecosystem that makes it easy to integrate third-party products and to share intelligence through a rich set of open application programming interfaces (APIs). Over 120 certified technology partners create the broadest ecosystem in cyber security, enabling a coordinated and best-in-class approach to threat protection, detection, and response across an organization's endpoints, networks, email, and cloud applications.

Global Intelligence Network

Symantec Integrated Cyber Defense is bolstered by its Global Intelligence Network (GIN), which correlates data from the following sources:

- 175,000,000 endpoints
- 80,000,000 Web proxies
- More than 126,000,000 attack sensors
- More than 25,000 vulnerabilities
- More than 500 security experts in seven global SOC centers around the world

By applying artificial intelligence to analyze over nine petabytes of security threat data, we offer the broadest and deepest set of threat intelligence in the industry. In addition, our solution automatically updates its intelligence on millions of malicious files and URL threat indicators daily. From endpoints to servers, and at the network traffic level, Symantec Integrated Cyber Defense shares telemetry amassed from Symantec customers across the globe, creating a deeper level of protection that no other company can match.

Symantec Global Intelligence Detects WastedLocker Ransomware Attacks

Evil Corp is not just a fictional company in a TV show. It is a real-world sophisticated cybercrime gang that has continued undeterred by FBI indictments of its leaders. In June 2020, Evil Corp launched a targeted ransomware attack called WastedLocker against some of the largest U.S. companies. This attack could have easily knocked them all out. The goal of the attacks was to cripple the victim's IT infrastructure by encrypting most of their computers and servers in order to demand a multimillion-dollar ransom.

Discovery and Findings

The initial compromise involved the SocGholish framework, which was delivered to the victim in a zipped JavaScript file masquerading as a browser update through compromised legitimate websites. A second JavaScript file profiled the computer using commands such as whoami, net user, and net group. Next, it used PowerShell to download additional discovery-related PowerShell scripts. Once the attackers gained access to the victim's network, they used Cobalt Strike in tandem with a number of living-off-the-land tools to steal credentials, escalate privileges, and move across the network to deploy the WastedLocker ransomware on multiple computers.

The attacks were proactively detected on a number of customer networks by our targeted attack cloud analytics. Targeted attack cloud analytics have the ability to quickly analyze data from GIN and transform that data into more meaningful, actionable security intelligence. By querying the totality of the data collected across all threat categories, the analytics engine provides insights into the full scope of even the most sophisticated threat campaigns. The Threat Hunter team reviewed and verified the activity and quickly realized it corresponded closely to publicly documented activity seen in the early stages of WastedLocker attacks.

Threat Hunters Respond

The discovery enabled the Threat Hunter team to identify additional organizations that had been targeted by WastedLocker and identify additional tools, tactics, and procedures used by the attackers. This information enabled Symantec analysts to strengthen Symantec protections against all stages of the attack. Concurrently, the Threat Hunter team delivered early warnings to 68 customers. By proactively reaching out by phone and email, the team successfully enabled the disruption of attacks.

Integrated Cyber Defense: The Four Pillars

With distributed work teams, there's an increased emphasis on protecting all attack points. These are activities that standalone products simply can not duplicate. To provide the most complete and effective asset protection in the industry, Symantec Integrated Cyber Defense delivers Endpoint Security, Network Security (Web and email), Information Security, and Identity Security across on-premises and cloud infrastructures.

Symantec Endpoint Security

The cloud has transformed business and made it routine for employees to access data and applications remotely from billions of devices. People now work from anywhere and BYOD has added billions of devices into the enterprise ecosystem.

Today, endpoint protection needs to take into account devices, apps, and networks. The challenge is that fileless, ransomware, and other emerging threats are penetrating old defenses. Stealthy attacks and living off the land are harder to spot than malware—and a plethora of endpoint operating systems creates additional security complexity.

Symantec Endpoint Security is a critical line of defense in preventing devices from being used as part of a cyberattack and from keeping the sensitive information stored on those devices from falling into the wrong hands. As an on-premises, hybrid, or cloud-based solution, Endpoint Security uses attack surface reduction, attack prevention, breach prevention, and detection and response capabilities to protect traditional and mobile endpoint devices.

In addition to the Endpoint Security functionality, GIN plays an important role in endpoint protection. The sophisticated threat intelligence helps security teams better assess risks, optimize security decisions, and take the proper actions to counter imminent threats. GIN also applies a deep range of machine learning, advanced analytics, and artificial intelligence to help detect threats and initiate a response—whether that is through automation or a SOC analyst.

The Symantec Endpoint Security modules include:

- Endpoint Security
- Server Security
- Storage Protection
- Endpoint Management

Symantec Network Security

The traditional network perimeter is gone, users are everywhere, and they need quick access to data and cloud applications around the clock. Email and the Web are the lifeblood and essential communication means for almost every modern organization. They also happen to be the main vectors exploited in cyberattacks, so keeping them safe is essential in reducing security risk and maintaining business continuity. The challenge is that blind spots from encrypted traffic create vulnerabilities, spear phishing attacks are on the rise, and modern threats overwhelm aging network defenses.

In the cloud, on-premises, or both, you need to stop inbound and outbound threats targeting your end users, information, and key infrastructure. Today's Web and email protection must account for this new reality while balancing security, performance, complexity, and cost.

Symantec Network Security enables fast, secure, and compliant access to enterprise data over modern Web and email workflows. Network Security provides seamless integration of Web and email security technologies. It covers endpoint, cloud, network and email vectors; advanced threat protection, isolation and encrypted traffic management; and email threat detection and response with strong visibility and remediation capabilities.

The Symantec Network Security modules include:

- Secure Web Gateway
- Web Isolation
- Secure Email Gateway
- Content Analysis with Sandboxing
- Forensics and Encrypted Traffic Management
- Zero Trust Network Access (ZTNA)

Symantec Information Security

It is critical that you protect your organization from data leaks and exfiltration. You must understand how your sensitive data moves across users, devices, and networks. You need to know when the data is at greatest risk for exposure, and make sure that the data does not fall into the wrong hands. However, security teams face unprecedented challenges when it comes to data governance and protection. They are defending an increasingly blurred network perimeter and expanded attack surfaces, addressing a myriad of regulatory and compliance requirements, and accelerating the digital shift from legacy to hybrid cloud environments.

In a *Zero Trust* model where you cannot trust anything in or out of your network, focusing the perimeter around the data and protecting it with intelligent authentication is the best security approach. Most authentication solutions on the market authenticate access to almost everything *but* your data. To successfully implement Zero Trust, what is needed is visibility into who is accessing your data both on-premises and in the cloud. Before a user is granted access, all risk factors surrounding the user and their authenticating device need to be evaluated.

Network security architectures that place the enterprise data center at the center of connectivity requirements inhibit the dynamic access requirements of digital business. The alternative is consolidating networking and SaaS capabilities into SASE so that security policies are tied to validating identities rather than the protection of IP addresses—and identities are no longer based on location.

Symantec Information Security gives you total visibility and control of data flowing across your organization with a tightly integrated solution that works seamlessly to strengthen your security posture and zero trust capabilities. Information Security sets the standard for data protection with best-of-breed tools that can protect your data at the endpoint, across networks and in the cloud, pinpoint high-risk behaviors so you can stop insider threats in their tracks, and enable remote employees who access corporate resources and data to work safely and productively.

The Symantec Information Security modules include:

- Data Loss Prevention
- CloudSOC CASB
- Information Centric Analytics

Symantec Identity Security

Businesses are driven by the need to launch new applications and services quickly to connect customers and employees to services anywhere and at any time. The challenge is that users and applications are a primary point of attack by cyber criminals hoping to exploit their access and privileges and do harm. To protect the business, you need to provide secure access to authorized resources, prevent accidental data leakage, guard against the misuse of credentials and accounts, and protect user privacy.

Symantec Identity Security mitigates these security risks by enforcing granular security policies to stop unauthorized access to sensitive resources and data while providing seamless access to trusted users. Identity Security leverages intelligence from GIN and advanced analytics across all products to analyze activity on the endpoint and confidently determine the legitimacy of human and non-human identities.

The Symantec Identity Security modules include:

- Authentication
- Access Management
- Privileged Access Management
- Identity Management

Powerful Integrations for Strategic, Proactive Cyber Defense

Every new breach is another reminder that no single technology will adequately protect an enterprise against all cyber security risks. Symantec Integrated Cyber Defense answers the challenge in a way that sets it apart from legacy security approaches by delivering integration at the product level, across Symantec products, and across the entire security stack, including third-party systems.

Product-Level Integration

At the product level, Symantec Integrated Cyber Defense reduces complexity by integrating previously standalone solutions into single, coherent products. One example is Symantec Endpoint Security Complete (SESC), which integrates Symantec Endpoint Protection (SEP), Symantec Endpoint Detection and Response (EDR), Threat Detection Active Directory, and Mobile Security into a single product to deliver pre-attack surface reduction, attack prevention, breach prevention, and response and remediation. Customers only need to install one agent, which performs all the necessary tasks. This kind of integration has more value for customers—not just because they get better protection, but because it also makes it easier for them to configure and deploy.

For those often-beleaguered SOC defenders, SESC product-level integration makes it easier for them to do their job. Here is an example:

1. The SOC analyst receives an incident from the EDR, capabilities included in SESC.
2. After doing some research, they identify how the threat ended up being in their environment.
3. While still in the same console, they can then take the appropriate action.
4. Additionally, they can identify and block the particular behavior pattern from reoccurring. This action is accomplished by setting the behavior isolation policy to reduce the attack surface for potential future attack attempts. As added benefit, the system minimizes the number of alerts SOCs need to investigate. The SOCs are now able to focus on more pressing threats.

Cross-Product Integration

Symantec Integrated Cyber Defense provides enhanced security outcomes by integrating technologies across separate Symantec products. Integrating information from multiple solutions, whether on-prem or cloud based, simply offers better threat visibility. It provides a greater opportunity to conduct correlations and apply threat intelligence to identify threats that otherwise might have been missed if the products had not been integrated. It also reduces response times between the time a suspicious file is identified and the time it gets blocked.

As an example, Symantec Integrated Cyber Defense consolidates the agents between Symantec Web Security Service (WSS) and SEP. Agent consolidation is critical in maintaining lower operational costs, better security posture, and better protections. A single agent for SEP, EDR, and WSS allows for easy deployment among the products, less time to manage agents, and increased protection as it is easier for the products to work together to detect and block threats.

Cross-product integration plays a vital role in digital transformation efforts. As more companies transition from on-prem solutions to cloud and SaaS-based services, they face new challenges and requirements as they set up their environments. More than ever, they will need solutions working together to help them successfully engineer this transformation in a secure way. They need the ability to understand who is accessing what types of data and from where. WSS and Symantec CloudSOC (CASB) extend data compliance policies to remote offices and remote users without impacting traffic to the data center. The integrated products inspect traffic on the upload and download and apply policies for compliance. By combining WSS (URL Filtering+AV) + CloudSOC integration, CloudSOC policies are inspected at WSS and if violated instruct WSS to block the traffic.

In another example we look at how to use Symantec Information Centric Analytics (ICA) to detect insider threats. ICA is a user and entity behavior analytics platform that, when integrated with Symantec Data Loss Prevention (DLP), SEP, and CASB, enables rapid identification of insider threats and cyber breaches. Through centralized analytics, extensive dashboards, and in-depth metrics, ICA escalates those issues that might otherwise go unnoticed or demand complex analysis. With automated remediation recommendations, ICA provides organizations with the visibility and workflows necessary to directly reduce exposure to sophisticated threats, greatly reducing manual effort. For example, ICA integrates assessment of policy violations across DLP, endpoint, and cloud systems, along with application of user analytics, to create the full context around a data exfiltration scheme carried out by a disgruntled worker. In another example, if there is evidence of a compromised system or account resulting from malware infection, combined with a high-risk DLP policy incident, ICA synthesizes these factors to drive visualization and mitigation of an externally driven attack.

Integration with Third-Party Solutions

To empower organizations to optimize the security stack, Symantec Integrated Cyber Defense allows for the integration of third-party solutions through Integrated Cyber Defense Exchange (ICDx), a data exchange technology for sharing events and intelligence across Symantec systems and third-party systems. Before ICDx, users needing protection across various control points had to engineer their own solution to collect telemetry across control points and normalize it so they could correlate that telemetry. With ICDx, users essentially get *plug and play* data normalization, centralizing threat telemetry for better threat hunting.

The Symantec Integrated Cyber Defense open architecture makes it easy to integrate third-party products and share intelligence. A rich set of open APIs vastly simplify integrations with Symantec Integrated Cyber Defense. This integration provides enhanced protection, investigation, and remediation across an organization's endpoints, networks, email, and cloud applications. More than 120 certified technology partners delivering 250+ applications and services create the broadest ecosystem in cyber security, enabling a coordinated and best-in-class approach to threat protection, detection, and response. It is up to customers to choose what fits best for their environment. Whatever their solution is, Symantec Integrated Cyber Defense integrations will drive toward the common goal of building a more robust security ecosystem and help customers blunt the attempts of adversaries. The upshot is that customers get to use security products that complement each other and get more effective security at a reduced cost.

One example of integration across the security stack is the pairing of ICDx + EDR for evolving threats and extended detection and response activities. The integration allows ICDx to collect threat telemetry from all endpoints, normalize that data, and then share it. The combination of ICDx + email security.cloud for evolving threats further supports extended detection and response. This integration exposes analytics on emails, endpoints, Web, network, data loss prevention, and more. The intelligence can be integrated into your security environment for faster, more effective correlation and response.

Summary

Enterprises face a constantly changing threat landscape that puts valued identities and information at risk. With scarce cyber security talent and limited budgets, organizations are left to figure out how to efficiently and effectively manage their security and compliance posture at a reasonable cost. In the past, security professionals sought out best-of-breed point tools, but few are integrated or share data across the security stack. This creates an environment where enterprises have solutions from multiple vendors deployed, which leads to high costs, administrative overhead, and little efficiency. As the threat landscape continues to evolve, it is increasingly clear that disconnected point tools can no longer support enterprise security requirements. What is needed is integrated cyber defense that unifies products, services, and partners to drive down the cost and complexity of cyber security, while protecting enterprises against sophisticated threats and delivering an exceptional digital customer experience.

Symantec Integrated Cyber Defense delivers endpoint, Web, email, information, and identity security across on-premises and cloud infrastructures. It provides the most complete and effective protection in the industry, allowing enterprises to embrace the cloud as it makes sense for them without sacrificing past investments and reliance on critical infrastructure. After decades of investing in individual security solutions that operate independently, enterprises can finally reduce operational complexity and optimize the effectiveness of their investments with the only solutions in the industry able to seamlessly share and leverage threat intelligence, management consoles, policies, and agents.

References

1 Ponemon Institute and IBM Security, Cyber Resilient Organization Report 2020, July 2020.
2 Oltsik, Jon, ESG Research Report, 2019 Technology Spending Intentions Survey, February 2019.
3 Perhach, Paulette, The New York Times, The Mad Dash to Find a Cybersecurity Force, November 2018.
4 Ponemon Institute and IBM Security, Cyber Resilient Organization Report 2020, July 2020.

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

ICD-ESS-WP100 March 18, 2021