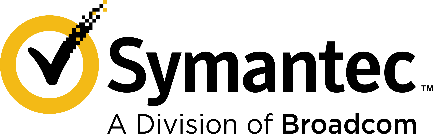
****

Partner Marketing Tool Kit

Symantec Endpoint Security Complete

How to Avoid Sophisticated Attacks and Undiscovered Breaches   
(Blind Spots)

Messaging, 5 Emails, Digital Assets, Videos, White Papers, Solution Briefs, Webcast Recordings, Blogs, Breach Assessment

March 2021

**Help Your Customers Avoid Endpoint Security Blind Spots**

Endpoint Protection, Detection and Response Are Not Enough.

**Help your customers uncover the blind spots in their security defenses and, more importantly, explain to them how to neutralize these with Symantec Endpoint Security (SES) Complete.**

Organizations around the globe are strengthening their Endpoint Protection, Endpoint Detection and Response solutions to combat today’s ever-expanding threats. Yet many continue to be breached by attackers who exploit the very tools and applications that are trusted and used in day-to-day business operations.

Why? Companies have blind spots. Moreover, traditional Endpoint Protection, Endpoint Detection and Response (EDR) solutions are not defending against these weaknesses.

Among the biggest security challenges today are:

* **‘Living-off-the-land’ attacks**: Attackers take advantage of legitimate applications that run a business and use them for malicious activities that are difficult to spot.
* **Active Directory attacks:** When this widely accessible service is unprotected, it becomes a vantage point for attackers and lateral movement.
* **Undiscovered inflight targeted breaches**: Attackers may dwell for a long time, remaining undetected due to massive amounts of data and a lack of information on attack types.

If such blind spots leave your customers exposed, they need Symantec Endpoint Security Complete (SESC). They will get more visibility into these activities and can benefit from the additional protection that their current solution does not provide.

SESC – Neutralizes These Blind Spots

* **Behavioral Isolation:** Symantec intelligence identifies, manages and blocks risky behavior; reduces attack surface ([Video](https://www.youtube.com/watch?v=fYNFE0fsKhM))
* **Active Directory Security:** AI-driven; blocks lateral movement at the point of breach; prevents attackers from stealing AD information and credentials ([Video](https://s2.content.video.llnw.net/smedia/582dd700945f4a7aa6a7bb6f0d70aead/Au/mb41cefPHOf-qUnlsyPxQyDVPNgsrydHy8Z_ewo1Y/tdad-final.mp4))
* **Threat Hunter:** Gathersglobal threat intelligence from organizations of all sizes; identifies earliest signs of hidden attacks in organizations; notifies your SOC through the product console ([White Paper](https://docs.broadcom.com/doc/SED-Threat-Hunter-WP100))

Key Campaign Resources

[**Download Email Nurture Campaign Here**](https://symantec.broadcom.com/hubfs/SED/SED%20EMEA/Blind%20Spots%20Campaign/blind-spot-email-nurture.docx)[**Digital Assets**](https://symantec.broadcom.com/hubfs/SED/SED%20EMEA/Blind%20Spots%20Campaign/symantec-blind-spots-digital-assets.zip) [**Social Assets**](https://symantec.broadcom.com/hubfs/SED/SED%20EMEA/Blind%20Spots%20Campaign/social-assets-blindspots.zip) [**Call Script**](https://symantec.broadcom.com/hubfs/SED/SED%20EMEA/Blind%20Spots%20Campaign/blind-spots-call-script.docx) [**Sales Play**](https://partnerportal.broadcom.com/en/symantec-partner-portal/symantec-sales-plays.html)

Message Summary: SESC – One Agent | One Console | One Product

[**Read Messaging ppt Slides Here**](https://symantec.broadcom.com/hubfs/SED/SED%20EMEA/Blind%20Spots%20Campaign/blind-spot-campaign-key-messages.pdf)

**SESC Goes Beyond Endpoint Protection and EDR – Full Protection, Great ROI with One Solution.**

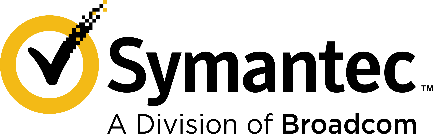
Symantec Endpoint Security Complete is a comprehensive solution that includes all the technologies organizations need for full protection against common security blind spots. It goes beyond endpoint protection and EDR. It includes ‘Behavior Isolation’ to block dangerous app behaviors. It provides ‘Active Directory Defense’ to prevent attacks on the Active Directory. It also offers ‘Threat Hunter’ bringing actionable global threat intelligence from Symantec advanced machine learning and expert security analysts.

SESC eliminates all blind spots and costs of breaches, addresses threats across the entire attack chain, protects all devices and key operating systems, supports hybrid environments, delivers low TCO due to single agent/single console, and achieves highest ROI with many innovative security layers all in one.

**Protecting Against Endpoint Security Blind Spots – Available Assets**

|  |  |  |
| --- | --- | --- |
| **Title** | **Type** | **How This Can Help** |
| **Endpoint Security Blind Spots** | | |
| [Can You See Your Security Blind Spots?](https://youtu.be/yfq2Mul-mQg) | Video *(CTA)* | Help your customers stay one step ahead of sophisticated attackers who are trying to bypass the most sophisticated security such as Endpoint Protection, Endpoint Detection and Response solutions. These attackers are taking advantage of what security teams cannot see – their blind spots. The video explains why and how SESC can help protect these blind spots. |
| [Do Blind Spots Leave You Exposed?](https://symantec.broadcom.com/blind-spots-resources) | Campaign Resources Landing Page | Focus on the three Blind Spots: *Living-off-the-Land, Unprotected Active Directory and Late Breach Discovery.* Provided CTAs Behavior Isolation, AD Directory Security & Threat Hunter. |
| [Endpoint Security: Eliminating Your Protection Blind Spots– Catalyst Conference 2020 Recording](https://www.youtube.com/watch?v=VNLTXwNmkaU) | Recording *(CTA)* | Typical endpoint security solutions can leave you with protection blind spots. Learn how Symantec Endpoint Security eliminates those blind spots across your environment. Adam Licata, product manager for Symantec Endpoint Security Complete, presents on three blind spots that exist in most enterprise systems and how to eliminate them. |
| [Don’t Let Attackers Exploit Your Blind Spots to Evade Detection](https://www.youtube.com/watch?v=aetFba_YUlU) | Webcast Recording | A webinar discussion on the launch of Symantec Endpoint Security Complete. |
| [Email Nurture & Digital/Social Assets)](https://symantec.broadcom.com/hubfs/SED/SED%20EMEA/Blind%20Spots%20Campaign/blind-spot-email-nurture.docx) *New!* | Customer Campaign | New! 5 Emails & digital/social assets offering: Breach Assessment, SES Infographic, Threat Hunter White Paper, Catalyst Webinar, SESC Upgrade Guide |
| **Behavior Isolation** | | |
| [Beefing Up Security with Behavior Isolation](https://www.youtube.com/watch?v=fYNFE0fsKhM) | Video *(CTA)* | With the recent rise of targeted attacks, attack surface reduction has become a critical part of every company's cyber security strategy. This powerful security technique uses intelligent rules to block attackers who seek to paralyze critical operations: Reducing the attack surface is a necessary component for an effective endpoint protection strategy; Identifying risky behaviors helps your customers home-in on attackers to block them. |
| [Getting Hit with Targeted Attacks? Symantec Endpoint Behavioral Isolation](https://www.brighttalk.com/webcast/13361/466914) | Webinar Recording | Find out:  Why attack surface reduction is a necessary component of your endpoint protection strategy  How to home in on attackers by identifying risky behaviors and blocking them  What Symantec is doing to enhance its full-feature endpoint offering and make it even easier to keep the bad guys out |
| **Threat Hunter** | | |
| [Eliminate Blind Spots and Supercharge Your SOC with Symantec Threat Hunter Insights](https://docs.broadcom.com/doc/SED-Threat-Hunter-WP100) | White Paper *(CTA)* | Threat Hunter is a new feature in SESC that empowers security teams to quickly respond to incidents and stop breaches. Symantec’s world-class threat analysts are the same cyber security experts who uncovered Suxtnet and WastedLocker. They review the machine learning insights from global customer telemetry. They provide vital insights about potential breaches to organizations directly through the SESC product console to alert SOC teams about potential breach attempts on their organization. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | | **Type** | **How This Can Help** |
| **Threat Defense for Active Directory** | | | |
| [Symantec Endpoint Threat Defense for Active Directory](https://s2.content.video.llnw.net/smedia/582dd700945f4a7aa6a7bb6f0d70aead/Au/mb41cefPHOf-qUnlsyPxQyDVPNgsrydHy8Z_ewo1Y/tdad-final.mp4) | Video *(CTA)* | | Microsoft Active Directory is an organization’s highest-valued network asset, but often the least protected, making it the number one target for attackers after they penetrate the network. Attackers need only to compromise and perform a few queries on a single device to obtain total domain dominance. This can happen in under seven minutes leaving SOC teams no time to act.It is critical to protect Active Directory from the endpoint to stop attackers on their first move. Symantec Endpoint Threat Defense for Active Directory with AI-driven intrusion detection, investigation and containment offers 99% success rate of in stopping an attacker on their first move. |
| [Symantec Endpoint Threat Defense for Active Directory](https://docs.broadcom.com/doc/sep-threat-defense-ad-en) | Solution Brief | | Symantec advances endpoint security by addressing stealthy attacks or advanced persistent threats with effective Active Directory defense from the endpoint to provide autonomous  breach containment, incident response, and domain security assessment. It is the only security solution that immediately contains attackers after compromise of an endpoint, but before they can persist on the domain. |
| [Symantec Breach Assessment](https://ftpdocs.broadcom.com/PartnerContent/8/Infrastructure%20SW%20Home/Partner%20Sales/Partner%20Portal-AEM/Symantec%20Partner%20Portal/Symantec%20Campaigns/Campaigns%20-%20SESC%20-%20Blind%20Spots%20-%20Tool%20Kit/Breach%20Assessment.zip)  [Breach Assessment Guide](https://symantec.broadcom.com/hubfs/SED/SED%20EMEA/Blind%20Spots%20Campaign/symantec-breach-assessment-guide.pdf) | [Video](https://youtu.be/2vs-mc2Wnwk)  [Sample Assessment Report](https://symantec.broadcom.com/hubfs/SED/SED%20EMEA/Blind%20Spots%20Campaign/Breach%20Assessment%20Report.html)  [Customer Invitation Email](https://symantec.broadcom.com/hubfs/SED/SED%20EMEA/Blind%20Spots%20Campaign/symantec-breach-assessment-customer-invitation.docx) | Breach Assessment *(CTA)*  [How To Use](https://symantec.broadcom.com/hubfs/SED/SED%20EMEA/Blind%20Spots%20Campaign/Read%20Me%20-%20Breach%20Assessment.txt) | | Symantec Breach Assessment uncovers Active Directory (AD) breaches. Symantec Partners can offer this **AD Breach Assessment Simulator** to their customers who can run it in their environments to detect potential weaknesses.  **This tool** utilizes the functionality of Threat Defense for Active Directory **(TDAD)** **assessment capabilities** to produce a report consisting of AD misconfigurations and vulnerabilities that may exist in your customers’ domains. It can be installed in any environment and runs after inputting the passkey. It runs 14 checks and returns a report with an outline of the AD security and any anomalies. The assessment comes in a zip file can be downloaded on the Partner Portal and provided to the customer. |
| **Why Upgrade to SESC** | | | |
| [Benefits of Upgrading Your Endpoint Solution Today](https://docs.broadcom.com/doc/Why_Upgrade_SESC) | White Paper *(CTA)* | | Symantec Endpoint Security Complete delivers the most complete and integrated endpoint security platform to protect your customers’ traditional and mobile endpoints. SESC combines all of Symantec’s endpoint security technology including SEP, EDR,Mobile Threat Defense, Active Directory Defense, Behavioral Isolation, App Control and Threat Hunting – all in one package and one price. |
| [SESC Overview](https://docs.broadcom.com/doc/endpoint-security-en) | Product Sheet *(CTA)* | | As an on premise, hybrid, or cloud-based solution, the single-agent Symantec SESC platform protects all traditional and mobile endpoints, providing interlocking defenses at the device, application, and network level, and uses artificial intelligence (AI) to optimize security decisions. A unified cloud based management system simplifies protecting, detecting, and responding to all the advanced threats targeting your endpoints. |
| [Feature Comparison Chart](https://symantec.broadcom.com/hubfs/SED/SED%20EMEA/Partner%20Newsletter/February%202021/symantec-endpoint-security%20comparison%20chart.pdf) | Battle Card | | Easy-to-read chart with a feature comparison overview of SEP, SES Enterprise and SES Complete |
| [Symantec Endpoint Protection Discovery Guide](https://symantec.broadcom.com/hubfs/SED/SED%20EMEA/Partner%20Newsletter/February%202021/symantec-endpoint-security-discovery-guide.pdf) | Selling and Positioning Enablement | | Symantec Endpoint Security selling and positioning guide. This is not a CTA for end-users, this is a selling and messaging guide. |
| [Reinventing Enterprise Security](https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/symantec-leading-way-reinventing-enterprise-security) | Blog | | Learn about Symantec's endpoint innovation strategy to stay ahead of attackers. See other [Blogs here](https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/symantec-leading-way-reinventing-enterprise-security) and [here](https://symantec-enterprise-blogs.security.com/blogs/product-insights/how-you-can-make-your-threat-intelligence-intelligent). |

****