Symantec
A Division of Broadcom

Endpoint Security

Guide

Discovery Guide

Symantec Endpoint Security

Version 1.0

June 2020

Endpoint Security | Introduction

INDEX

The Challenges of Endpoint Security

Endpoints are a primary target for cyber attackers. And attacks are more sophisticated and targeted than ever. In response, many companies try to bolster their overall defense by adding multiple endpoint protection products such as EDR and threat hunting. Unfortunately, this approach weakens an organization's security posture because there are still security gaps. Companies average 7 endpoint agents per device and as most vendors' products do not talk to each other well.

So companies are challenged by the following:

- How to achieve visibility and protection for all your devices (both traditional and modern mobile ones) and all OSes?
- How do you ensure that all the technologies talk to each other and share information in a coordinated , unified manner?
- How to manage all this security with a single console and agent?

How Endpoint Security Helps

Endpoint security is the last line of defense to stop attackers from gaining access to data and the network

Endpoint Security technologies for all endpoints (traditional and mobile) address the entire attack chain through four primary areas:

- Attack Surface Reduction
- Attack Prevention
- Breach Prevention
- Detection and Response

Symantec Endpoint Security Solutions

Symantec provides a broad portfolio of endpoint security technologies to address these business challenges, including:

- **Endpoint Security**
- **Server Security**
- **Endpoint Management**
- **IoT Protection**

Customer Personas

CISOs and Security Analysts are the top decision makers for endpoint security today

CISO

How will Broadcom impact Symantec?

One team, executing much faster than before
Evidence: Release cadence

SECURITY ANALYST

Who can help me stop breaches fast?

Threat Hunting service backed by world class threat researchers and AI/ML gives analyst more signal, less noise

ENDPOINT ADMIN

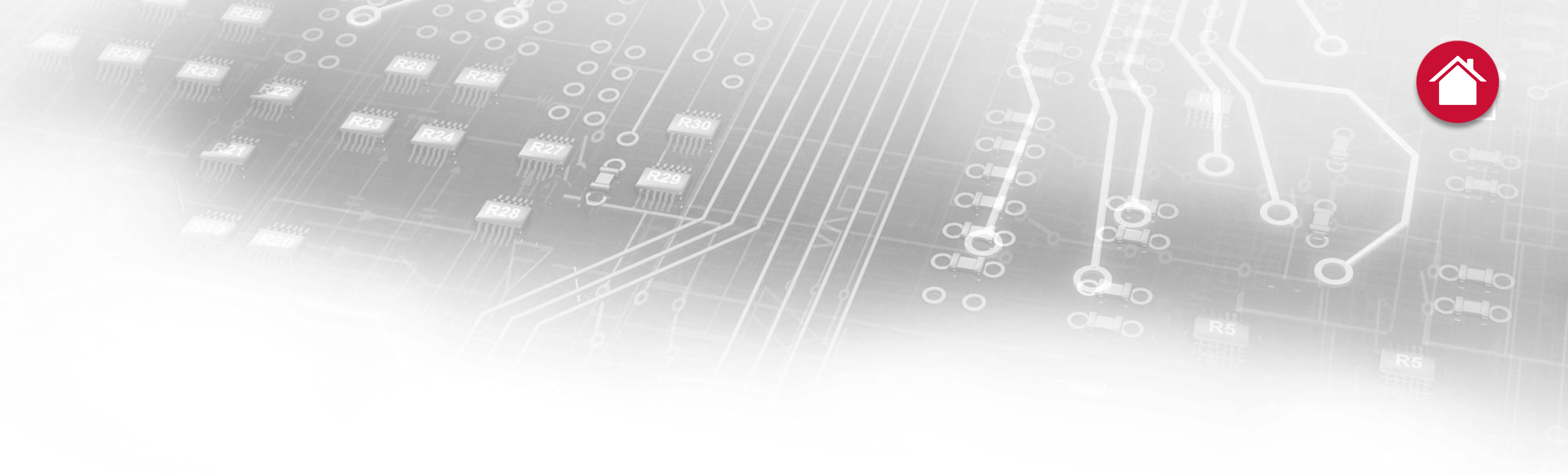
What's my Operational Overhead?

Protection across attack chain, without business disruption and false positives

PROCUREMENT

How can you save us money?

Lowest TCO in market, single vendor for all security and IT infra needs



Symantec Endpoint Security Complete

Positioning SESC

Elevator Pitch

Endpoints are a primary target for cyber attackers as threats, malware variants, and attack frequency are all increasing. In response, many companies bolster their overall defense by adding multiple endpoint protection products. However, this approach can actually weaken an organization's security posture. With Symantec, you can end the compromises. Why choose between the best security and the greatest simplicity when you can have both?

Market Trends

Security Risks

- 80% increase in iOS and Android vulnerabilities
- 56% increase in risky WiFi networks
- 62% increase in enterprise targeted ransomware
- 100% increase in malicious PowerShell scripts
- 197 days avg. to identify a breach, 69 days avg. to contain
- Active Directory is #1 attack target and it takes less than 7 minutes to infiltrate

Management Complexity

- ~7 different endpoint agents installed, adding cost, complexity, and risk

Leading Questions

- How do you currently reduce the attack surface of your endpoints?
- What is your visibility into attacks on iOS and Android devices
- How do you prevent breaches and stop attackers moving laterally from the endpoint across your network?
- How do you hunt for threats and address breaches?

Value Proposition

In <25 words:

Symantec Endpoint Security Complete delivers the most complete endpoint security platform to protect all your endpoints across the entire attack chain.

In <60 words:

Symantec Endpoint Security Complete delivers the most complete and integrated endpoint security platform to protect all your traditional and mobile endpoints. As an on-premises, hybrid, or cloud-based solution, this single-agent Symantec solution delivers innovative antimalware, EDR, app control app isolation, and AD security to protect your devices across the entire attack chain.

Differentiators

Most awarded endpoint security solution – Gartner MQ leader, Forrester Wave leader, Radicati top leader, AV-Test Best Protection/Performance, SE Labs Best Enterprise Endpoint.

Protection with multilayered defense from all attack vectors at industry leading efficacy - Combination of core and next gen technologies in one solution protects across the entire attack chain to stop known and unknown threats. SESC provides better breadth and depth of protections that go beyond competitor features that use standalone technologies that only address limited points in the attack chain; All validated by 3rd-parties

Gain best ROI and reduce complexity with a single-agent, integrated platform – Multiple endpoint security engines in a single agent solution (e.g. antimalware, EDR, deception, app isolation, app control, AD protections, etc.) for ease of deployment and management.

Protect all endpoints (all device types and OSes) – Deep protections for laptops, desktops, and mobile devices; includes Windows, macOS, Linux, iOS Android, Windows 10 in S mode, and Windows 10 for ARM

Follow your cloud journey– Industry leading Endpoint Security, now fully cloud managed, is flexible across on-premises or cloud without any new agent to install for an easy upgrade from on-premises to cloud

Realize integrations at scale - No other vendor provides an integrated solution that orchestrates a response at the endpoint triggered by the detection of a threat at the network gateway (i.e. web and email security gateways).

Use advanced machine learning backed by the largest global intelligence network – Powered by AI analyzing more than 3.7 trillion lines of telemetry for the industry's broadest and deepest threat intelligence across endpoints, emails, and web.

Proof Points

Industry Validation

Infographic with all key industry wins

Customer Quotes

"We have seen a 60 percent drop in malware events'

Vicki Gavin

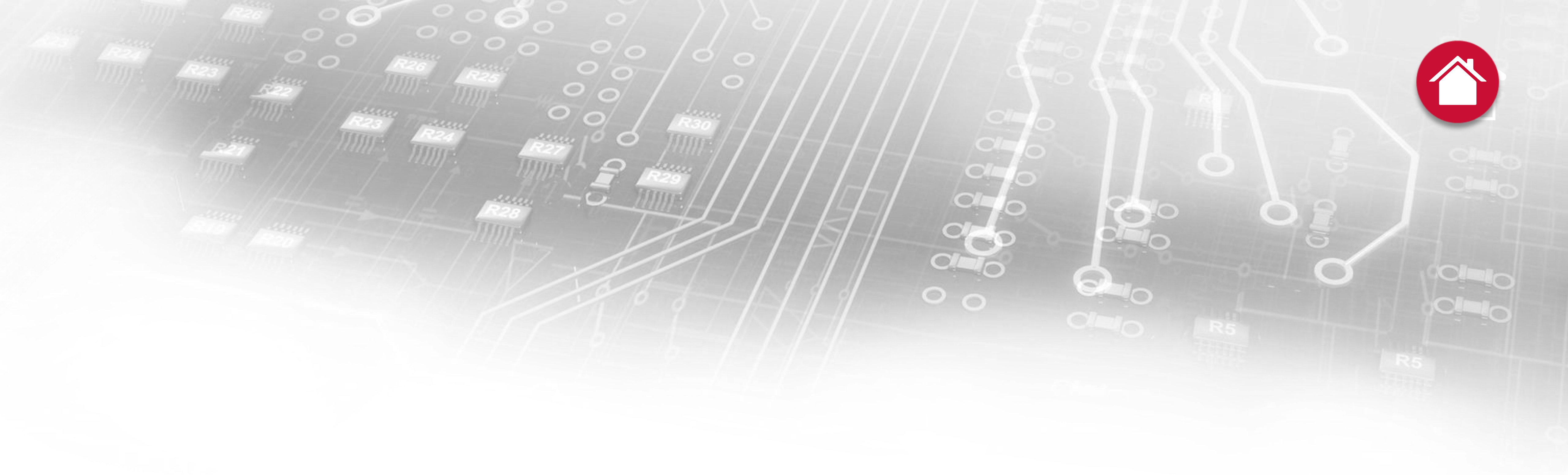
-Compliance Director, Head of Business Continuity, Cyber Security, and Data Privacy, The Economist

Prospecting

How to position and sell SESC

Goal	Challenges	Discovery	Positioning	Enablement
SELL SESC TO NEW CUSTOMERS; **UPGRADE SEP/SESE TO SESC**	• Customer needs advanced protections across the entire attack chain • Customers need enhanced capabilities without increasing load and complexity on the endpoint with more agents • Customer wants to protect all their devices, traditional and mobile from attacks and threats.	• How do you currently reduce the attack surface of your endpoints? • What is your visibility into attacks on iOS and Android devices • How do you prevent breaches and stop attackers moving laterally from the endpoint across your network? • How do you hunt threats and address breaches?	• In each case, position SESC, our flagship product which features protection across the entire attack chain: attack surface reduction, attack prevention, breach prevention, and detection & response	• SES Partner Training • SES Customer Deck • SES Migration FAQ • SES Technical Training

Assets	Awareness	Education	Validation	Adoption
BUYER & CUSTOMER JOURNEY	• Prevention Matters Video (first panel)	• Endpoint Webinar (Art & Adam) • SES Solution Brief • 'Endpoint Security vs. APT' video (resource section of SESC page) • Endpoint White Papers (EDR, App Control, Active Directory security, etc.	• AV-Test Best Protection for 5 consecutive years and Best Performance • SE Labs Best Enterprise Endpoint (Annual Report 2019 - page 12) • EPP - Gartner Peer Insights Customer Choice Award 2019 • EDR – Gartner Peer Insights Customer Choice Award 2020 • Industry Awards Infographic	• Why upgrade/transition to SESC (customer letter) • SEP to SESC migration steps KB • How to videos (tips and tricks) for SESC capabilities (EDR, app isolation, app control, AD security, etc.)



Symantec Endpoint Security Enterprise

Positioning SESE

Elevator Pitch

Endpoints are a primary target for cyber attackers as threats, malware variants, and attack frequency are all increasing. And with the growing remote workforce, companies need to protect both traditional and modern, mobile endpoints as well as BYOD and UYOD. And with the transition to cloud, companies need a solution that will walk their cloud journey and support all deployment options: on-premises, in the cloud, and a hybrid approach

Market Trends

Security Risks

- 80% increase in iOS and Android vulnerabilities
- 56% increase in risky WiFi networks
- 62% increase in enterprise targeted ransomware

Management Complexity

- ~7 different endpoint agents installed, adding cost, complexity, and risk

Leading Questions

- How do you want to manage your endpoint security (on-premises, cloud, or hybrid)?
- What are all the operating systems you use in your organization?
- How many attacks have there been on your company's mobile devices?
- How do you secure all the endpoints accessing your network, especially with the growing remote workforce?

Value Proposition

In <25 words:

Symantec Endpoint Security Enterprise delivers advanced protections for all your traditional and mobile endpoints. It supports on-premises, cloud, and hybrid management models

In <60 words:

Symantec Endpoint Security Enterprise delivers advanced protections for all your traditional and mobile endpoints. As an on-premises, hybrid, or cloud-based solution, the single-agent Symantec solution uses artificial intelligence (AI) to optimize security decisions to protect against known and unknown threats and attacks.

Differentiators

Most awarded endpoint security solution – Gartner MQ leader, Forrester Wave leader, Radicati top leader, AV-Test Best Protection/Performance, SE Labs Best Enterprise Endpoint.

Reduce complexity with a single-agent, integrated platform – Symantec combines multiple endpoint security engines into a single agent solution for ease of deployment and management.

Protect all endpoints (all device types and OSes) – Deep protections for laptops, desktops, and mobile devices; includes Windows, macOS, Linux, iOS Android, Windows 10 in S mode, and Windows 10 for ARM

Follow your cloud journey– Industry leading Endpoint Protection, now fully cloud managed, is flexible across on-premises or cloud without any new agent to install for an easy upgrade from on-premises to cloud

Realize integrations at scale - No other vendor provides an integrated solution that orchestrates a response at the endpoint triggered by the detection of a threat at the network gateway (i.e. web and email security gateways).

Use advanced machine learning backed by the largest global intelligence network – Powered by AI analyzing more than 3.7 trillion lines of telemetry for the industry's broadest and deepest threat intelligence across endpoints, emails, and web.

Proof Points

Industry Validation

Infographic with all key industry wins

Customer Quotes

"We have seen a 60 percent drop in malware events'

Vicki Gavin

-Compliance Director, Head of Business Continuity, Cyber Security, and Data Privacy, The Economist

Prospecting

How to position and sell SESE

Goal	Challenges	Discovery	Positioning	Enablement
SELL SESE TO NEW CUSTOMERS; **UPGRADE SEP SBE/ SEPC TO SESE**	• Customer wants to protect all their devices, traditional and mobile from attacks and threats. • Customer needs an easy, effective transition from SEP SBE and SEP Cloud to another endpoint security solution	• How would you like to manage your endpoint protection: on-premises, in the cloud, or hybrid? Perhaps you are on-premises now and want to transition to cloud shortly. • What is your visibility into attacks on iOS and Android devices • How are you addressing BYOD and UYOD issues associated with the increase in remote workers due to COVID-19?	• If customer needs a new endpoint protection product, then position SESE which features on-premises, cloud, and hybrid management models • If customer owns SEP SBE or SEP Cloud, then position SESE as the solution to protect desktops, laptops, and mobile devices.	• SES Partner Training • SES Customer Deck • SES Migration FAQ • SES Technical Training

Assets	Awareness	Education	Validation	Adoption
BUYER & CUSTOMER JOURNEY	• Prevention Matters Video (first panel)	• Endpoint Webinar (Art & Adam) • SES Solution Brief • Endpoint White Papers	• AV-Test Best Protection for 5 consecutive years and Best Performance • SE Labs Best Enterprise Endpoint (Annual Report 2019 - page 12) • EPP - Gartner Peer Insights Customer Choice Award 2019 • Industry Awards Infographic	• Why upgrade/transition to SES (customer letter) • SBE/SEPC to SES Migration Steps KB • SEP to SES Migration Steps KB and FAQ

Competitive Battle Cards

For all endpoint battlecards, please find them at:
https://drive.google.com/drive/folders/1dMnmSB66hVIiYgrw3Qx_y3BSEf_CIAQZ

CrowdStrike Falcon Prevent (1 of 3)

CROWDSTRIKE APPROACH

CrowdStrike Falcon is a Cloud-native Platform that provides Next-gen AV and EDR in a single agent.

The CrowdStrike (CS) Falcon platform is cloud-native endpoint protection. It delivers and unifies IT Hygiene, next-generation antivirus, endpoint detection and response (EDR), managed threat hunting, and threat intelligence — all delivered in a single lightweight agent.

SYMANTEC APPROACH

Symantec has the most advanced, integrated, and complete endpoint security solution for traditional and mobile devices in the cloud, on-prem and hybrid

Interlocking prevention technologies help defend against advanced attack methods and vectors; secure any device, anywhere with a high-performance, lightweight solution

Symantec's single light weight agent provides comprehensive protection across Windows, Mac, Linux, and mobile with industry leading prevention and EDR capability

SYMANTEC DIFFERENTIATORS – Elevator Counter Pitch to CrowdStrike

Symantec Endpoint Security Complete Provides Comprehensive Security with an easy to deploy Single Agent

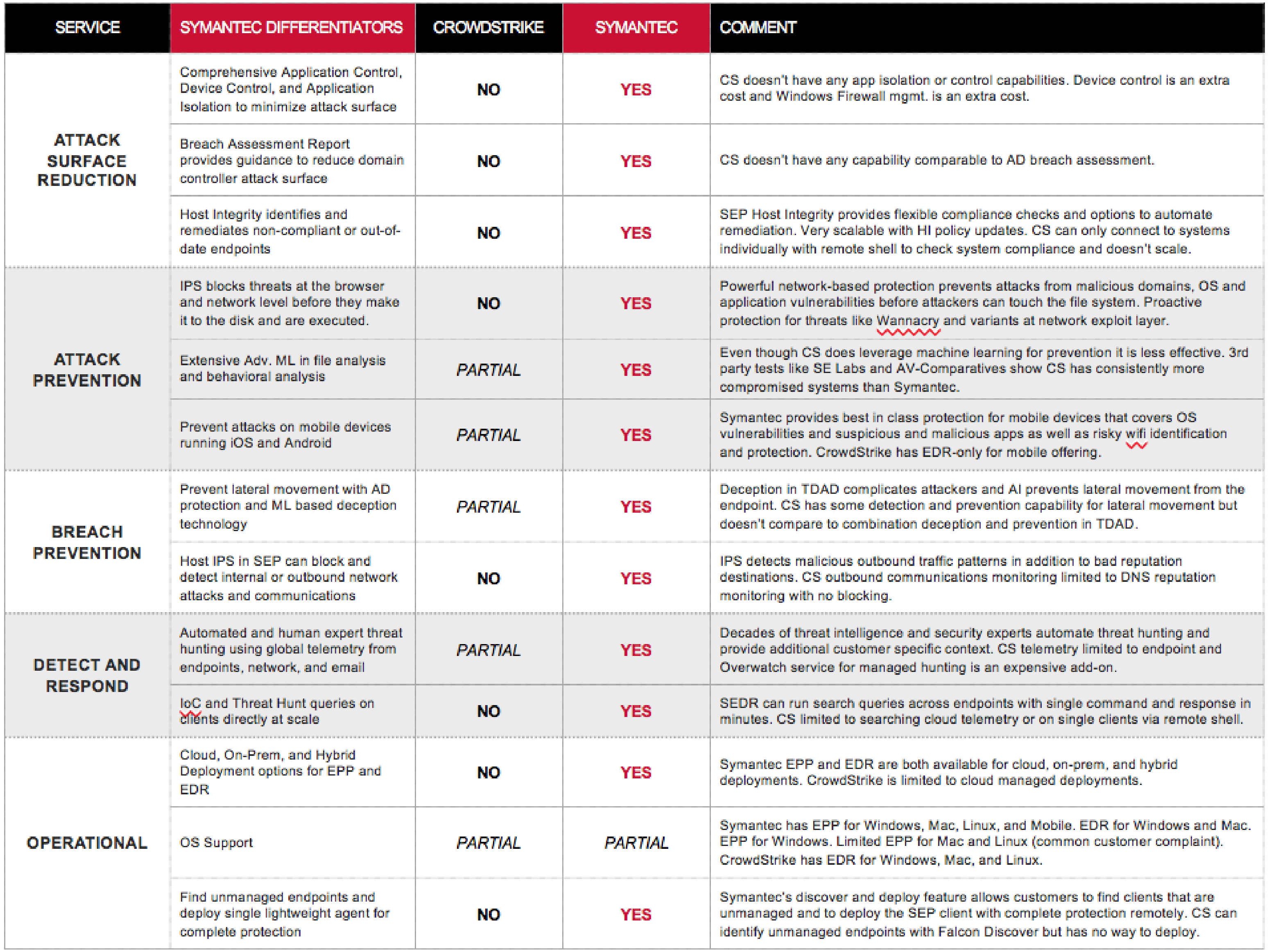
Symantec's single agent architecture combines core protection technologies like antivirus, IPS, etc., with leading-edge technologies such as EDR, adv. machine learning, memory exploit mitigation, behavioral analysis, and advanced application defenses. Symantec delivers best in class coverage for Mac, Linux, iOS, and Android.

While CrowdStrike does have a strong EDR offering it is lacking in many endpoint protection controls, namely around attack surface reduction, network protection, and on-access detection of non-PE files. CrowdStrike relies largely on behavioral analysis, allowing potentially malicious files to execute before being blocked and relying heavily on cloud access for effectiveness. CrowdStrike has minimal Mac and Linux prevention and no prevention technology for mobile devices.

Symantec EDR leverages broad telemetry across endpoint, email, and network for flexible deployments including cloud, on-prem or hybrid.

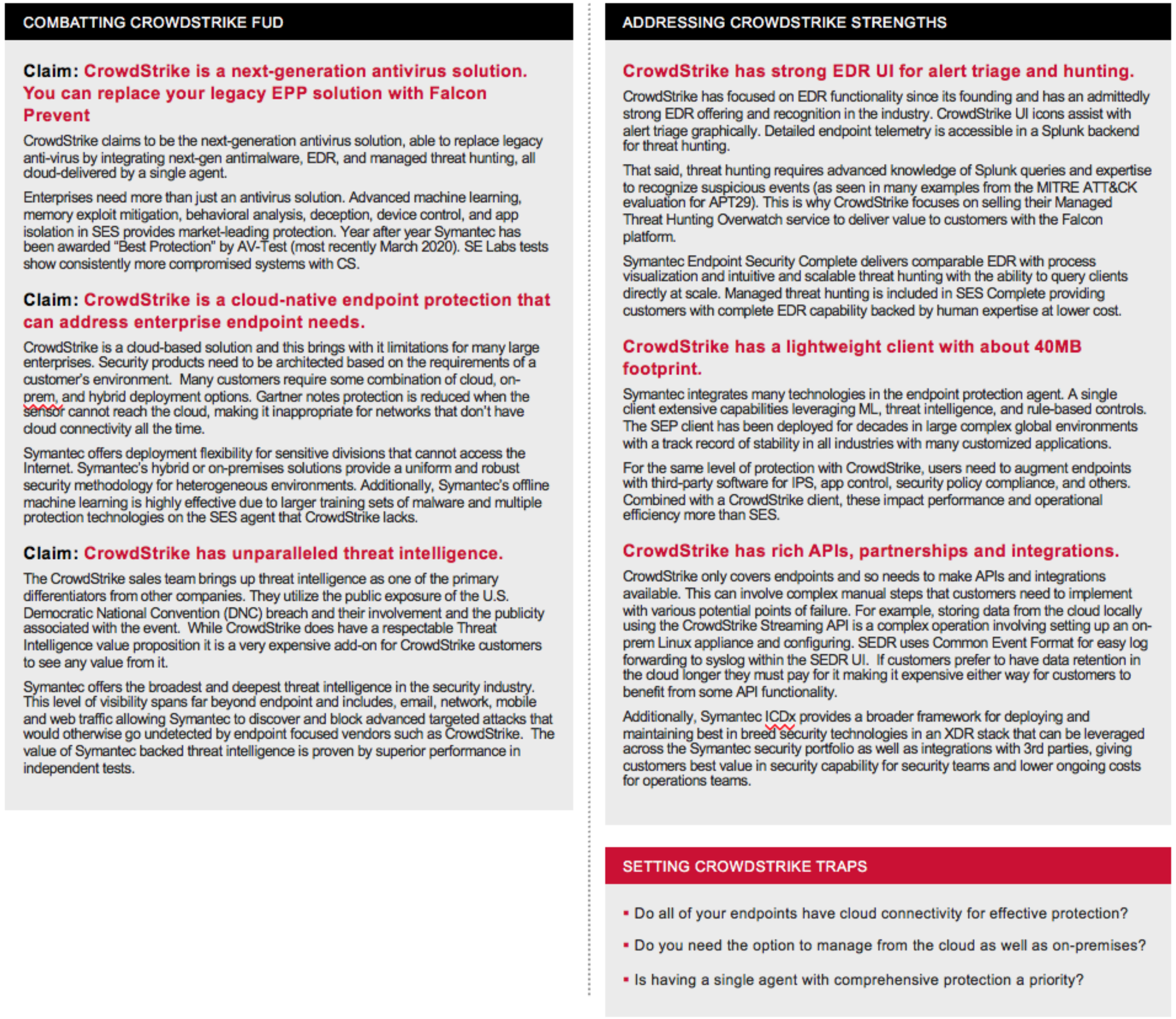
Symantec leverages security expertise over decades of experience and telemetry far broader than endpoints to deliver high quality EDR alerting. CrowdStrike does not have an on-prem offering and cannot compete with the breadth or depth of Symantec's endpoint, email and network telemetry as well as security portfolio.

CrowdStrike Falcon Prevent (2 of 3)



SERVICE	SYMANTEC DIFFERENTIATORS	CROWDSTRIKE	SYMANTEC	COMMENT
ATTACK SURFACE REDUCTION	Comprehensive Application Control, Device Control, and Application Isolation to minimize attack surface	**NO**	**YES**	CS doesn't have any app isolation or control capabilities. Device control is an extra cost and Windows Firewall mgmt. is an extra cost.
	Breach Assessment Report provides guidance to reduce domain controller attack surface	**NO**	**YES**	CS doesn't have any capability comparable to AD breach assessment.
	Host Integrity identifies and remediates non-compliant or out-of-date endpoints	**NO**	**YES**	SEP Host Integrity provides flexible compliance checks and options to automate remediation. Very scalable with HI policy updates. CS can only connect to systems individually with remote shell to check system compliance and doesn't scale.
ATTACK PREVENTION	IPS blocks threats at the browser and network level before they make it to the disk and are executed.	**NO**	**YES**	Powerful network-based protection prevents attacks from malicious domains, OS and application vulnerabilities before attackers can touch the file system. Proactive protection for threats like Wannacry and variants at network exploit layer.
	Extensive Adv. ML in file analysis and behavioral analysis	*PARTIAL*	**YES**	Even though CS does leverage machine learning for prevention it is less effective. 3rd party tests like SE Labs and AV-Comparatives show CS has consistently more compromised systems than Symantec.
	Prevent attacks on mobile devices running iOS and Android	*PARTIAL*	**YES**	Symantec provides best in class protection for mobile devices that covers OS vulnerabilities and suspicious and malicious apps as well as risky wifi identification and protection. CrowdStrike has EDR-only for mobile offering.
BREACH PREVENTION	Prevent lateral movement with AD protection and ML based deception technology	*PARTIAL*	**YES**	Deception in TDAD complicates attackers and AI prevents lateral movement from the endpoint. CS has some detection and prevention capability for lateral movement but doesn't compare to combination deception and prevention in TDAD.
	Host IPS in SEP can block and detect internal or outbound network attacks and communications	**NO**	**YES**	IPS detects malicious outbound traffic patterns in addition to bad reputation destinations. CS outbound communications monitoring limited to DNS reputation monitoring with no blocking.
DETECT AND RESPOND	Automated and human expert threat hunting using global telemetry from endpoints, network, and email	*PARTIAL*	**YES**	Decades of threat intelligence and security experts automate threat hunting and provide additional customer specific context. CS telemetry limited to endpoint and Overwatch service for managed hunting is an expensive add-on.
	IoC and Threat Hunt queries on clients directly at scale	**NO**	**YES**	SEDR can run search queries across endpoints with single command and response in minutes. CS limited to searching cloud telemetry or on single clients via remote shell.
OPERATIONAL	Cloud, On-Prem, and Hybrid Deployment options for EPP and EDR	**NO**	**YES**	Symantec EPP and EDR are both available for cloud, on-prem, and hybrid deployments. CrowdStrike is limited to cloud managed deployments.
	OS Support	*PARTIAL*	*PARTIAL*	Symantec has EPP for Windows, Mac, Linux, and Mobile. EDR for Windows and Mac. EPP for Windows. Limited EPP for Mac and Linux (common customer complaint). CrowdStrike has EDR for Windows, Mac, and Linux.
	Find unmanaged endpoints and deploy single lightweight agent for complete protection	**NO**	**YES**	Symantec's discover and deploy feature allows customers to find clients that are unmanaged and to deploy the SEP client with complete protection remotely. CS can identify unmanaged endpoints with Falcon Discover but has no way to deploy.

CrowdStrike Falcon Prevent (3 of 3)



COMBATTING CROWDSTRIKE FUD

Claim: CrowdStrike is a next-generation antivirus solution. You can replace your legacy EPP solution with Falcon Prevent

CrowdStrike claims to be the next-generation antivirus solution, able to replace legacy anti-virus by integrating next-gen antimalware, EDR, and managed threat hunting, all cloud-delivered by a single agent.

Enterprises need more than just an antivirus solution. Advanced machine learning, memory exploit mitigation, behavioral analysis, deception, device control, and app isolation in SES provides market-leading protection. Year after year Symantec has been awarded "Best Protection" by AV-Test (most recently March 2020). SE Labs tests show consistently more compromised systems with CS.

Claim: CrowdStrike is a cloud-native endpoint protection that can address enterprise endpoint needs.

CrowdStrike is a cloud-based solution and this brings with it limitations for many large enterprises. Security products need to be architected based on the requirements of a customer's environment. Many customers require some combination of cloud, on-prem, and hybrid deployment options. Gartner notes protection is reduced when the sensor cannot reach the cloud, making it inappropriate for networks that don't have cloud connectivity all the time.

Symantec offers deployment flexibility for sensitive divisions that cannot access the Internet. Symantec's hybrid or on-premises solutions provide a uniform and robust security methodology for heterogeneous environments. Additionally, Symantec's offline machine learning is highly effective due to larger training sets of malware and multiple protection technologies on the SES agent that CrowdStrike lacks.

Claim: CrowdStrike has unparalleled threat intelligence.

The CrowdStrike sales team brings up threat intelligence as one of the primary differentiators from other companies. They utilize the public exposure of the U.S. Democratic National Convention (DNC) breach and their involvement and the publicity associated with the event. While CrowdStrike does have a respectable Threat Intelligence value proposition it is a very expensive add-on for CrowdStrike customers to see any value from it.

Symantec offers the broadest and deepest threat intelligence in the security industry. This level of visibility spans far beyond endpoint and includes, email, network, mobile and web traffic allowing Symantec to discover and block advanced targeted attacks that would otherwise go undetected by endpoint focused vendors such as CrowdStrike. The value of Symantec backed threat intelligence is proven by superior performance in independent tests.

ADDRESSING CROWDSTRIKE STRENGTHS

CrowdStrike has strong EDR UI for alert triage and hunting.

CrowdStrike has focused on EDR functionality since its founding and has an admittedly strong EDR offering and recognition in the industry. CrowdStrike UI icons assist with alert triage graphically. Detailed endpoint telemetry is accessible in a Splunk backend for threat hunting.

That said, threat hunting requires advanced knowledge of Splunk queries and expertise to recognize suspicious events (as seen in many examples from the MITRE ATT&CK evaluation for APT29). This is why CrowdStrike focuses on selling their Managed Threat Hunting Overwatch service to deliver value to customers with the Falcon platform.

Symantec Endpoint Security Complete delivers comparable EDR with process visualization and intuitive and scalable threat hunting with the ability to query clients directly at scale. Managed threat hunting is included in SES Complete providing customers with complete EDR capability backed by human expertise at lower cost.

CrowdStrike has a lightweight client with about 40MB footprint.

Symantec integrates many technologies in the endpoint protection agent. A single client extensive capabilities leveraging ML, threat intelligence, and rule-based controls. The SEP client has been deployed for decades in large complex global environments with a track record of stability in all industries with many customized applications.

For the same level of protection with CrowdStrike, users need to augment endpoints with third-party software for IPS, app control, security policy compliance, and others. Combined with a CrowdStrike client, these impact performance and operational efficiency more than SES.

CrowdStrike has rich APIs, partnerships and integrations.

CrowdStrike only covers endpoints and so needs to make APIs and integrations available. This can involve complex manual steps that customers need to implement with various potential points of failure. For example, storing data from the cloud locally using the CrowdStrike Streaming API is a complex operation involving setting up an on-prem Linux appliance and configuring. SEDR uses Common Event Format for easy log forwarding to syslog within the SEDR UI. If customers prefer to have data retention in the cloud longer they must pay for it making it expensive either way for customers to benefit from some API functionality.

Additionally, Symantec ICDx provides a broader framework for deploying and maintaining best in breed security technologies in an XDR stack that can be leveraged across the Symantec security portfolio as well as integrations with 3rd parties, giving customers best value in security capability for security teams and lower ongoing costs for operations teams.

SETTING CROWDSTRIKE TRAPS

- Do all of your endpoints have cloud connectivity for effective protection?
- Do you need the option to manage from the cloud as well as on-premises?
- Is having a single agent with comprehensive protection a priority?

Microsoft Endpoint Protection (1 of 3)

MICROSOFT APPROACH

Endpoint Protection and EDR are part of the OS and License Agreement.

Microsoft's Endpoint Protection components are built into Windows 10 Ent. Depending on the license entitlement (Win10 Ent E3/E5), customers get varying levels of protection. These include MS Defender, MS Defender Advanced Threat Protection and other security components.

SYMANTEC APPROACH

Symantec has the most advanced, integrated, and complete endpoint security solution for traditional and mobile devices in the cloud, on-prem and hybrid

Interlocking prevention technologies help defend against advanced attack methods and vectors; secure any device, anywhere with a high-performance, lightweight solution.

Symantec's single light weight agent's unparalleled protection across versions of Windows. Agent updates do not require updating the OS, delivering optimal TCO and up to date security.

SYMANTEC DIFFERENTIATORS – Elevator Counter Pitch to Microsoft

Symantec Endpoint Security Complete Provides Comprehensive Security with an easy to deploy Single Agent

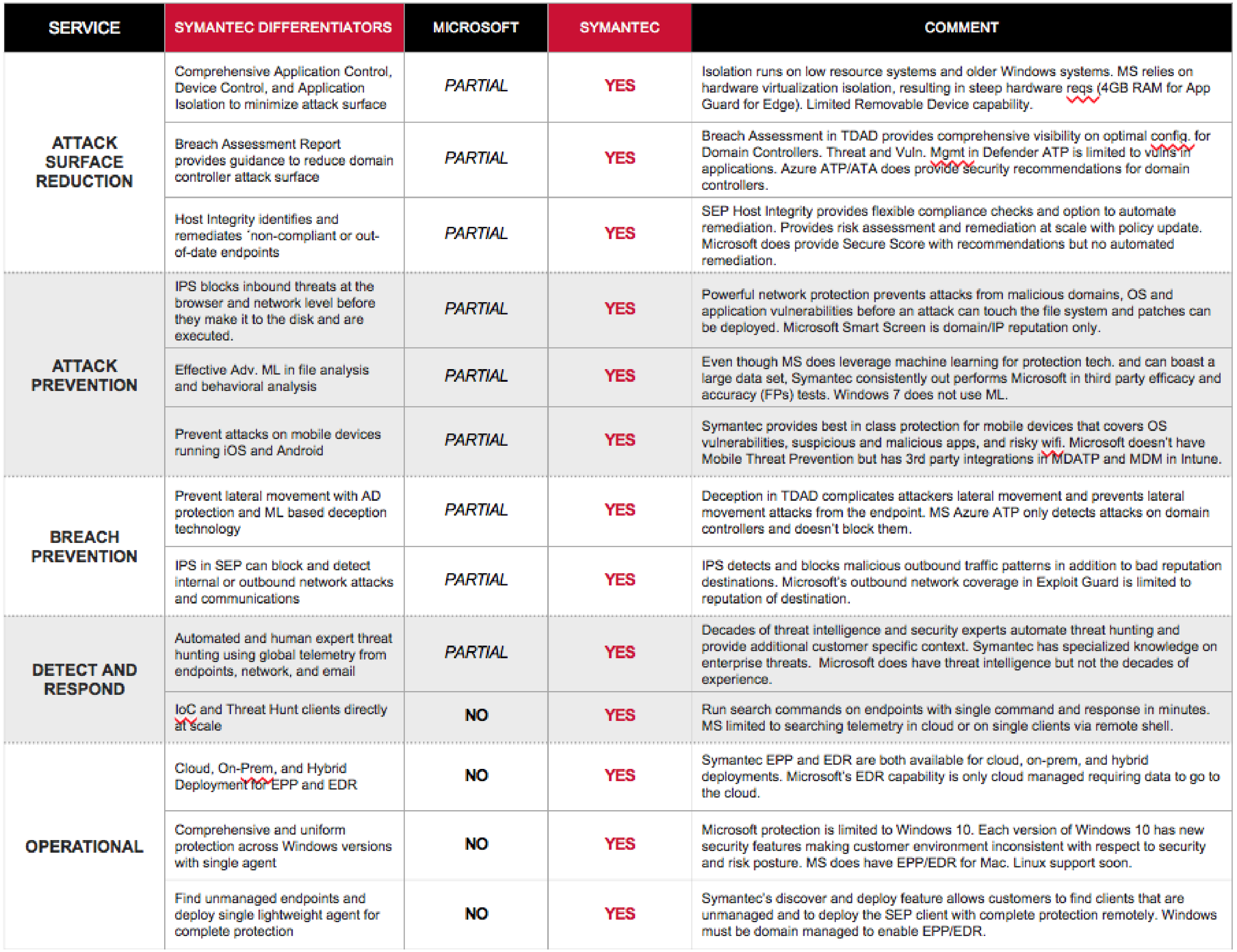
Symantec's single agent architecture combines core protection technologies like antivirus, IPS, etc., with leading-edge technologies such as EDR, adv. machine learning, memory exploit mitigation, behavioral analysis, and advanced application defenses. Symantec delivers best in class coverage for Mac, Linux, iOS, and Android.

A single agent allows security teams to easily add security technology independent of an organizations business platform in Windows 10. MS Defender is part Windows 10 Enterprise and Windows Server 2016/2019 requiring security teams to align with business stakeholders before being able to deploy updates to security technology.

SES Complete leverages decades of telemetry across endpoint, email, and network for quality EDR alerts.

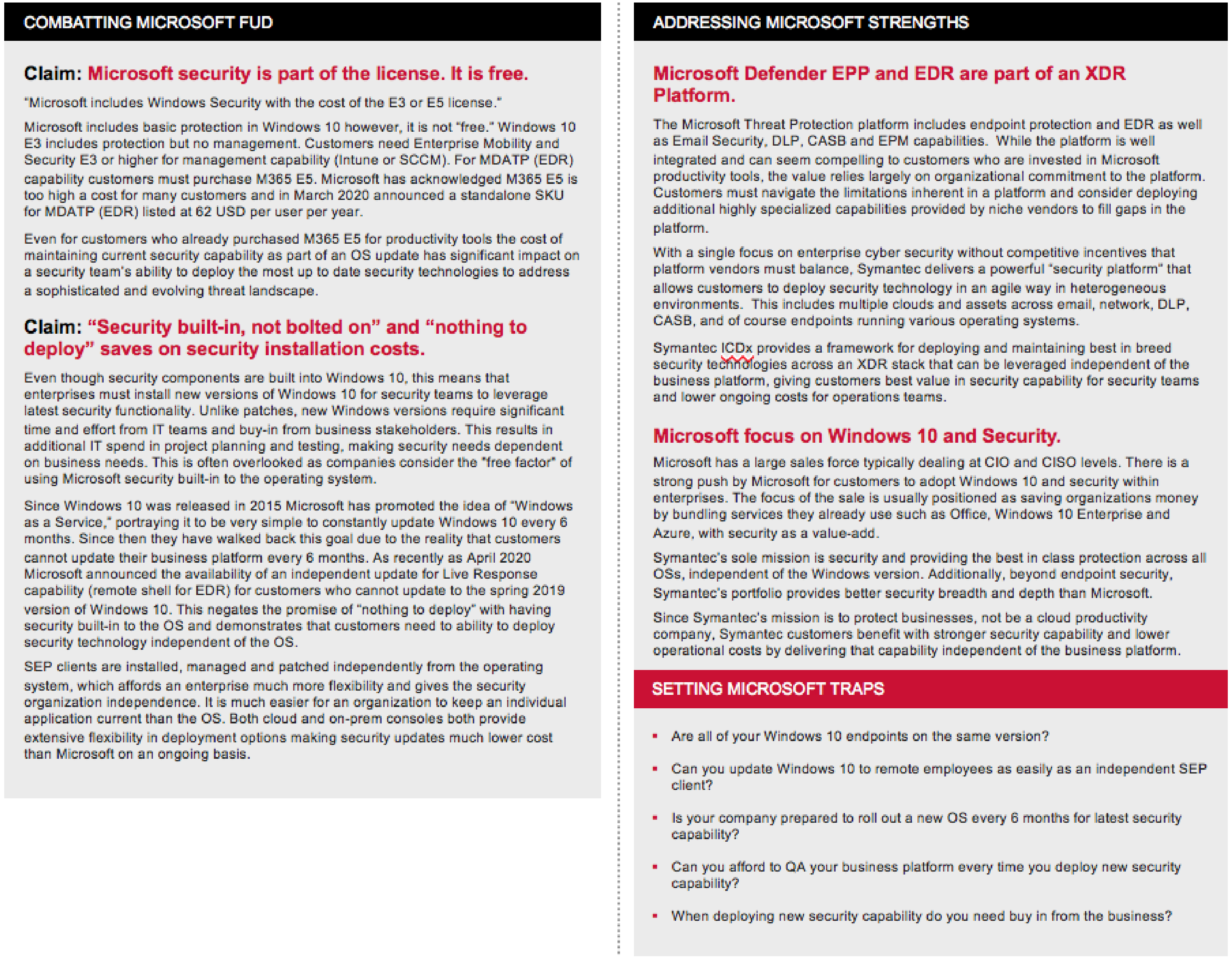
Symantec leverages deep security expertise based on decades dedicated to generating security telemetry across control points to deliver high quality EDR alerting. Rather than overwhelming analysts with logs, SES Complete leverages on client analytics to generate actionable security telemetry and reduce time to respond to incidents. Security experts who supplement event enrichment and customer specific context and recommendations.

Microsoft Endpoint Protection (2 of 3)



SERVICE	SYMANTEC DIFFERENTIATORS	MICROSOFT	SYMANTEC	COMMENT
ATTACK SURFACE REDUCTION	Comprehensive Application Control, Device Control, and Application Isolation to minimize attack surface	*PARTIAL*	YES	Isolation runs on low resource systems and older Windows systems. MS relies on hardware virtualization isolation, resulting in steep hardware reqs (4GB RAM for App Guard for Edge). Limited Removable Device capability.
	Breach Assessment Report provides guidance to reduce domain controller attack surface	*PARTIAL*	YES	Breach Assessment in TDAD provides comprehensive visibility on optimal config. for Domain Controllers. Threat and Vuln. Mgmt in Defender ATP is limited to vulns in applications. Azure ATP/ATA does provide security recommendations for domain controllers.
	Host Integrity identifies and remediates ´non-compliant or out-of-date endpoints	*PARTIAL*	YES	SEP Host Integrity provides flexible compliance checks and option to automate remediation. Provides risk assessment and remediation at scale with policy update. Microsoft does provide Secure Score with recommendations but no automated remediation.
ATTACK PREVENTION	IPS blocks inbound threats at the browser and network level before they make it to the disk and are executed.	*PARTIAL*	YES	Powerful network protection prevents attacks from malicious domains, OS and application vulnerabilities before an attack can touch the file system and patches can be deployed. Microsoft Smart Screen is domain/IP reputation only.
	Effective Adv. ML in file analysis and behavioral analysis	*PARTIAL*	YES	Even though MS does leverage machine learning for protection tech. and can boast a large data set, Symantec consistently out performs Microsoft in third party efficacy and accuracy (FPs) tests. Windows 7 does not use ML.
	Prevent attacks on mobile devices running iOS and Android	*PARTIAL*	YES	Symantec provides best in class protection for mobile devices that covers OS vulnerabilities, suspicious and malicious apps, and risky wifi. Microsoft doesn't have Mobile Threat Prevention but has 3rd party integrations in MDATP and MDM in Intune.
BREACH PREVENTION	Prevent lateral movement with AD protection and ML based deception technology	*PARTIAL*	YES	Deception in TDAD complicates attackers lateral movement and prevents lateral movement attacks from the endpoint. MS Azure ATP only detects attacks on domain controllers and doesn't block them.
	IPS in SEP can block and detect internal or outbound network attacks and communications	*PARTIAL*	YES	IPS detects and blocks malicious outbound traffic patterns in addition to bad reputation destinations. Microsoft's outbound network coverage in Exploit Guard is limited to reputation of destination.
DETECT AND RESPOND	Automated and human expert threat hunting using global telemetry from endpoints, network, and email	*PARTIAL*	YES	Decades of threat intelligence and security experts automate threat hunting and provide additional customer specific context. Symantec has specialized knowledge on enterprise threats. Microsoft does have threat intelligence but not the decades of experience.
	IoC and Threat Hunt clients directly at scale	NO	YES	Run search commands on endpoints with single command and response in minutes. MS limited to searching telemetry in cloud or on single clients via remote shell.
OPERATIONAL	Cloud, On-Prem, and Hybrid Deployment for EPP and EDR	NO	YES	Symantec EPP and EDR are both available for cloud, on-prem, and hybrid deployments. Microsoft's EDR capability is only cloud managed requiring data to go to the cloud.
	Comprehensive and uniform protection across Windows versions with single agent	NO	YES	Microsoft protection is limited to Windows 10. Each version of Windows 10 has new security features making customer environment inconsistent with respect to security and risk posture. MS does have EPP/EDR for Mac. Linux support soon.
	Find unmanaged endpoints and deploy single lightweight agent for complete protection	NO	YES	Symantec's discover and deploy feature allows customers to find clients that are unmanaged and to deploy the SEP client with complete protection remotely. Windows must be domain managed to enable EPP/EDR.

Microsoft Endpoint Protection (3 of 3)



COMBATTING MICROSOFT FUD

Claim: Microsoft security is part of the license. It is free.

"Microsoft includes Windows Security with the cost of the E3 or E5 license."

Microsoft includes basic protection in Windows 10 however, it is not "free." Windows 10 E3 includes protection but no management. Customers need Enterprise Mobility and Security E3 or higher for management capability (Intune or SCCM). For MDATP (EDR) capability customers must purchase M365 E5. Microsoft has acknowledged M365 E5 is too high a cost for many customers and in March 2020 announced a standalone SKU for MDATP (EDR) listed at 62 USD per user per year.

Even for customers who already purchased M365 E5 for productivity tools the cost of maintaining current security capability as part of an OS update has significant impact on a security team's ability to deploy the most up to date security technologies to address a sophisticated and evolving threat landscape.

Claim: "Security built-in, not bolted on" and "nothing to deploy" saves on security installation costs.

Even though security components are built into Windows 10, this means that enterprises must install new versions of Windows 10 for security teams to leverage latest security functionality. Unlike patches, new Windows versions require significant time and effort from IT teams and buy-in from business stakeholders. This results in additional IT spend in project planning and testing, making security needs dependent on business needs. This is often overlooked as companies consider the "free factor" of using Microsoft security built-in to the operating system.

Since Windows 10 was released in 2015 Microsoft has promoted the idea of "Windows as a Service," portraying it to be very simple to constantly update Windows 10 every 6 months. Since then they have walked back this goal due to the reality that customers cannot update their business platform every 6 months. As recently as April 2020 Microsoft announced the availability of an independent update for Live Response capability (remote shell for EDR) for customers who cannot update to the spring 2019 version of Windows 10. This negates the promise of "nothing to deploy" with having security built-in to the OS and demonstrates that customers need to ability to deploy security technology independent of the OS.

SEP clients are installed, managed and patched independently from the operating system, which affords an enterprise much more flexibility and gives the security organization independence. It is much easier for an organization to keep an individual application current than the OS. Both cloud and on-prem consoles both provide extensive flexibility in deployment options making security updates much lower cost than Microsoft on an ongoing basis.

ADDRESSING MICROSOFT STRENGTHS

Microsoft Defender EPP and EDR are part of an XDR Platform.

The Microsoft Threat Protection platform includes endpoint protection and EDR as well as Email Security, DLP, CASB and EPM capabilities. While the platform is well integrated and can seem compelling to customers who are invested in Microsoft productivity tools, the value relies largely on organizational commitment to the platform. Customers must navigate the limitations inherent in a platform and consider deploying additional highly specialized capabilities provided by niche vendors to fill gaps in the platform.

With a single focus on enterprise cyber security without competitive incentives that platform vendors must balance, Symantec delivers a powerful "security platform" that allows customers to deploy security technology in an agile way in heterogeneous environments. This includes multiple clouds and assets across email, network, DLP, CASB, and of course endpoints running various operating systems.

Symantec ICDx provides a framework for deploying and maintaining best in breed security technologies across an XDR stack that can be leveraged independent of the business platform, giving customers best value in security capability for security teams and lower ongoing costs for operations teams.

Microsoft focus on Windows 10 and Security.

Microsoft has a large sales force typically dealing at CIO and CISO levels. There is a strong push by Microsoft for customers to adopt Windows 10 and security within enterprises. The focus of the sale is usually positioned as saving organizations money by bundling services they already use such as Office, Windows 10 Enterprise and Azure, with security as a value-add.

Symantec's sole mission is security and providing the best in class protection across all OSs, independent of the Windows version. Additionally, beyond endpoint security, Symantec's portfolio provides better security breadth and depth than Microsoft.

Since Symantec's mission is to protect businesses, not be a cloud productivity company, Symantec customers benefit with stronger security capability and lower operational costs by delivering that capability independent of the business platform.

SETTING MICROSOFT TRAPS

- Are all of your Windows 10 endpoints on the same version?
- Can you update Windows 10 to remote employees as easily as an independent SEP client?
- Is your company prepared to roll out a new OS every 6 months for latest security capability?
- Can you afford to QA your business platform every time you deploy new security capability?
- When deploying new security capability do you need buy in from the business?

Customer Stories

Large Multinational Bank

- **Customer Challenges**
  - Financial regulations and internal audit requirements for application whitelisting by 2018
  - McAfee solution “did not work”
- **Why We Won**
  - App Isolation & App Control for suspicious and vulnerable apps; had the needed workflows
  - Single endpoint agent – big plus
  - Broader contract negotiation
  - Great trust relationship with Symantec
- **Competitors**
  - McAfee (lacked legacy application support, had performance issues)

$2M deal

130K endpoints

Large Multinational Oil Company

Customer Challenges

- Heavy resource consumption on the McAfee endpoint
- Too much endpoint complexity with McAfee (EP, AP, TIE) and FireEye HX; need a simple, integrated endpoint solution
- McAfee lost customer trust when it fell out of the Gartner MQ leader quadran
- Wannacry infection in May 2017 was not detected by McAfee

Why We Won

- Our platform proposal delivers significant opex and capex savings, reduces complexity, and increases agility for incidents response
- Superior detection efficacy and better technology
- SEP is significantly less resource intensive on the endpoints (vs. McAfee)
- Our leadership position in the Gartner MQ and McAfee's drop-off
- Our integrated EDR features were comparable to the existing FireEye HX deployment

41K seats of SEP 14 + EDR (now included in SES Complete)

Deal size:

$700K over three years

Competitors

- Displaced McAfee (ePO, ETP, ES and TIE), FireEye (HX, EX, NX), and Cisco IronPort

Large Healthcare Company

Customer Challenges

- Too little visibility into endpoint activity
- Zero day and ransomware detection
- Understanding of what users are doing and if there are any data leaks
- Need confidence that malware had not spread across the estate when a compromise was detected

Why We Won

- Single agent - simple to add EDR (ATP: Endpoint)
- True security partner, MSS monitoring ATP and performing incident investigation
- No additional load on healthcare endpoints
- Endpoint visibility with SEP 14 + EDR (ATP: Endpoint)
- CISO on Symantec Healthcare Advisory Board
- Deal included 30,000 DLP seats

30K seats of SEP 14 + EDR (now included in SES Complete) + Virtual Appliances [3yrs]

30K seats ATP: Network +
2 8800 appliances [3 yrs]

ATP deal size:
$866K over three years

Competitors

- No competitors - Existing SEP and BCS for endpoint customer

Large Healthcare Company

Customer Challenges

- Too many vendors, required one vendor to solve multiple security needs
- Fulfill current and future requirements with vendor technology, not 3rd-parties
- Looking for mature and proven products for endpoint, web, email, DLP
- One solution provider to deliver technology, implementation, support and educational services

Why We Won

- Broader security portfolio than Cisco
- Proven products across endpoint, web, email and DLP
- Competitive total acquisition cost for entire bundle of products and services
- Established Symantec as trusted partner over many executive briefings, technical reviews and consulting projects

Competitors

- ATP: Network displaces FireEye and Snort IPS (Cisco/IronPort)
- SEP + ATP: Endpoint across enterprise displaces Microsoft SCEP
- Email Security.Cloud and ATP: Email displaces Proofpoint

40K seats of SEP 14 + EDR (now included in SES Complete)

60K seats ATP: Network +
20 8800 appliances

60K seats ATP: Email

ATP deal size:
$809K over three years

Thank You

BROADCOM®

BROADCOM®

connecting everything®

Symantec
A Division of Broadcom

Thank you for downloading this Symantec guide! Carahsoft is the reseller for Symantec Fed and Sled solutions available via Navy BPA, DIR-TSO, The Quilt, and other contract vehicles.

To learn how to take the next step toward acquiring Symantec's solutions, please check out the following resources and information:

For additional resources:
carah.io/Symantec-resources

For additional BlackBerry solutions:
carah.io/Symantec-remote-solutions

To set up a meeting:
symantecteam@Carahsoft.com
703-871-8539

For upcoming events:
carah.io/Symantec-webinars

For additional FED and SLED solutions:
carah.io/Symantec-solutions

To purchase, check out the contract vehicles available for procurement:
carah.io/Symantec-contracts

carahsoft.

For more information, contact Carahsoft or our reseller partners:
CAmarketing@carahsoft.com | 703-871-8539