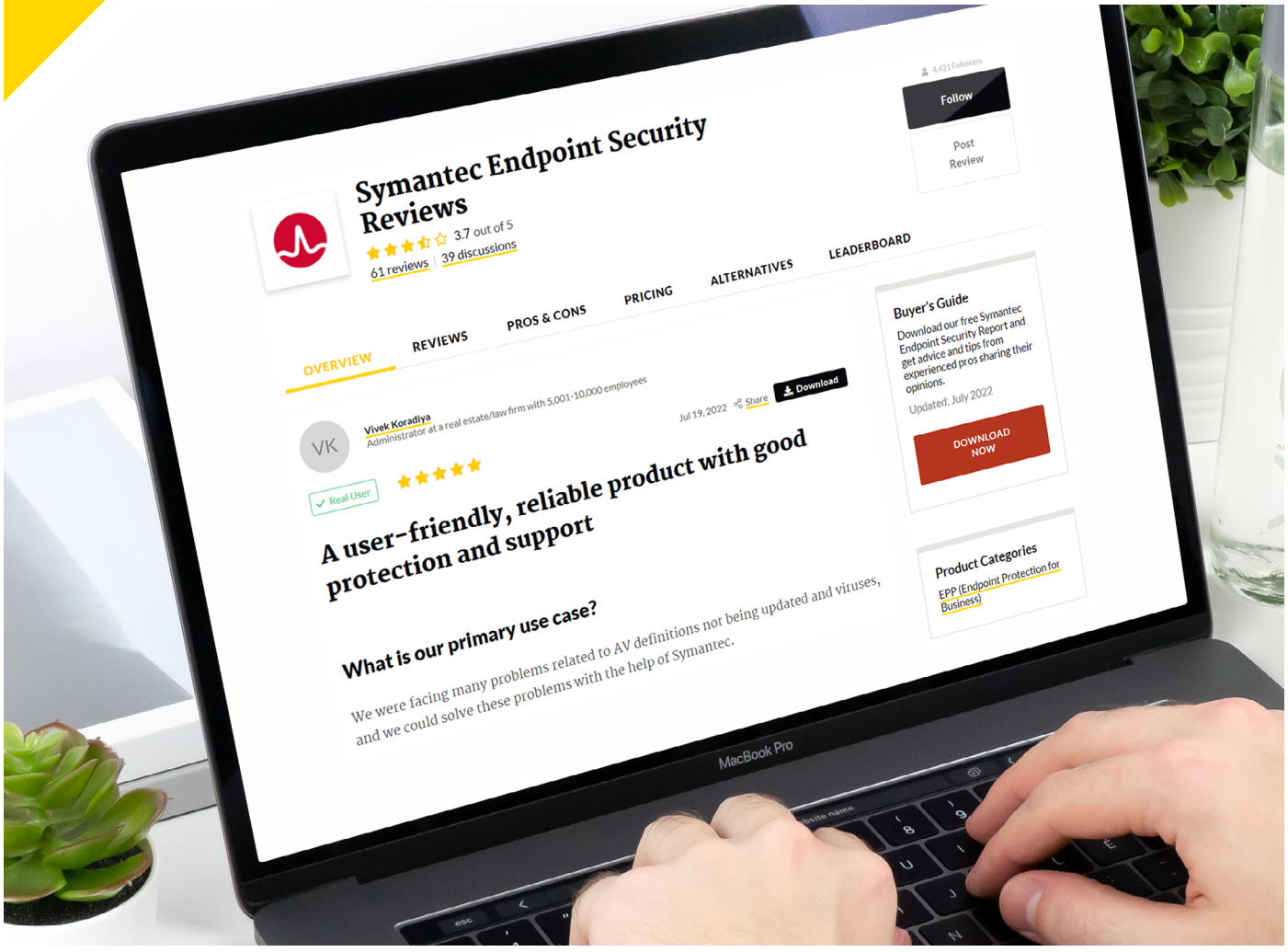
PeerPaper™ Report 2022

Based on real user experiences with Symantec Endpoint Solutions

Top 10 Key Success Factors for Threat Detection and Protection



PeerSpot

Contents

Introduction

The work of cybersecurity is almost entirely about dealing with threats, either directly or indirectly. Knowing what threats an entity is facing, and responding to them, forms the core of security operations (SecOps). Solutions that detect threats and provide protection from them are therefore some of the most critical elements of an effective security strategy.

Security managers have a range of choices for threat detection and protection solutions. Some of the most common of them focus on threat detection and protection at the endpoint, which is one of the primary battlegrounds in defending the enterprise from increasingly advanced threats. What makes for a good threat detection and protection solution? In this paper, real users of Symantec endpoint solutions weigh in with the top 10 key success factors for threat detection and protection. They focus on capabilities such as machine learning, firewalls inside endpoints, fast response, automation and more.

Threat Detection and Protection Overview

The terms “threat detection” and “threat protection” tend to get used together, so much so that people may conflate their meanings. Although threat detection and threat protection are related, and usually work together in a cybersecurity context, they are not the same process. Threat detection is about monitoring an IT environment and picking up evidence that a threat is present. For example, a virus may have a unique digital signature. If a threat detection solution sees that signature, it will know the virus is present.

Threat protection is about taking action to prevent a detected threat from causing harm. A threat protection solution will block detected threats. It may quarantine them. The solution might wipe, and re-image machines affected by a threat that’s been detected.

Threat detection and threat protection don’t do much good on their own. Detecting a threat and not doing anything about it is a risky waste of time. Conversely, a threat protection solution will not know what to do without alerts about threats that have been detected. For these reasons, the two technologies almost always operate in tandem.

Improved threat detection and protection

Endpoint Security Use Cases Featuring Symantec Endpoint Solutions

PeerSpot members are putting Symantec endpoint solutions to work across a variety of use cases. For example, a Senior Network Engineer who uses Symantec Endpoint Security at a government agency uses the solution primarily for antivirus protection, anti-malware protection, and personal firewall protection. A Security Technical Consultant who uses Symantec Endpoint Security at Prosoft Information Systems, a software company, said, "Our primary use case of Symantec End-User Endpoint Security is for malicious websites and malware attacks."

A thin client for servers, coupled with a full package for the users' systems, are the ways that Georgetown University uses Symantec Endpoint Security. Advanced threat protection is how a tech services company employs Symantec Endpoint Detection and Response. According to their Head of Corporate Desktop Services, "The product gives us an edge when it comes to antivirus. We use a cloud connector, and the solution is locally deployed, taking data live from the cloud and syncing." A Chief information security officer who uses Symantec Endpoint Security Complete at a transportation company uses the solution to protect their Active Directory environment and file servers.

> **"The product gives us an edge when it comes to antivirus."**
>
> **Read review »**

"Symantec Endpoint Detection and Response is primarily applied to endpoints in the banking and telecom sectors," said the CTO of ABM Info. Tech, a tech services company. He added, "If you want to protect yourself from zero-day threats, one option is to have Endpoint and the EDP, and if you don't want to have that combination, EDR [endpoint detection and response] is the best way to detect any exfiltration into the network, and then to respond accordingly."

Fast response and blocking

Top 10 Key Success Factors for Threat Detection and Protection

Symantec users identified 10 key success factors for threat detection and protection. These range from the ability to block executables to scanning without affecting the network. Automation matters, as does fast response and blocking. Users like having a firewall in the endpoint, as well, among other criteria.

#1 – Threat Detection and Protection Capabilities

Core threat detection and protection capabilities are, not surprisingly, one of the key success factors. That is the basic mission, after all. Symantec users spoke to this functionality in their reviews, with ABM Info. Tech's CTO, for example, saying, "The detection vulnerability is very effective. It distinguishes Symantec Endpoint Detection and Response from its competitors."

> **"The detection vulnerability is very effective. It distinguishes Symantec Endpoint Detection and Response from its competitors."**
>
> Read review »

> **"We no longer have to deal with day-to-day threats, and we can focus more on work."**
>
> Read review »

"We no longer have to deal with day-to-day threats, and we can focus more on work," said a Director for Cybersecurity Solutions who uses Symantec Endpoint Security at a tech services company. "Whenever there are some problems, our operations don't stop. So, we can continue our work knowing that there is a good security solution protecting us."

For a Sr. Consultant, Cyber Security who uses Symantec Endpoint Security Enterprise at a tech services company, what stood out was the solution's proactive threat protection and the spyware protection features, which go beyond basic threat detection. In their case, this is effective even without EDR.

A System Administrator who uses Symantec Endpoint Security at a consultancy praised the solution's ability to detect signature-based viruses. An IT Specialist who uses Symantec Endpoint Security at an educational organization valued the solution for ransomware protection, general malware protection and network exploitation protection.

#2 – Blocking Executables

Executable files can wreak havoc on end user's systems and they often get clicked on by mistake. For these reasons, blocking executables is a key success factor in threat detection and protection. According to a Threat Intelligence and Forensics Investigation Specialist at IBM Thailand, "There are times when Symantec Endpoint Detection and Response tags an executable as malicious when it is trying to get executed on the machine. In this case, it prevents the execution and it gives you a process view of things where you can look into what has happened and whether it is a genuine process trying to access some system activities, or it's a malicious one."

This user added that, depending upon the process, the solution gives the user a clear identification of the executable. He said, "We can do the containment from the interface itself and isolate the machine from the network. The process review on network isolation is good."

"We can do the containment from the interface itself and isolate the machine from the network. The process review on network isolation is good."

Read review »

#3 – Firewall in the Endpoint

PeerSpot members found that having a firewall in the endpoint improved threat detection and protection. As a Managing Director who uses Symantec Endpoint Security Complete at Rubik Infotech Pvt. Ltd, a security firm, put it, "One feature I found most valuable in Symantec Endpoint Security Complete is the firewall feature on the endpoint. The firewall feature helps users handle virus outbreaks."

An Operations Manager who uses Symantec Endpoint Security at Telescope Digital, a tech services company, concurred, saying, "I like the additional features that come with it. The firewall feature and the encryption feature that they throw in are good as well." Figure 1 depicts this feature.

Figure 1 - A built-in firewall in the endpoint can stop threats before they even infect users' devices.

#4 – Scanning Without Affecting the Network

Security must strike a balance with system performance and other operational considerations. A solution for threat detection and protection cannot affect user experience by slowing down the network or users' devices. The Head of the Cyber and Information Research Centre at the Council for Scientific and Industrial Research, an educational organization, spoke to this issue when he said, "The most valuable feature of Symantec Endpoint Detection and Response is its ability to conduct large scans on the endpoints without affecting the network."

"The most valuable feature is that I don't feel that it is there," is how a manager who uses Symantec Endpoint Security at a comms service provider described his experience with the solution. "It works in the background and doesn't interfere with my daily work. All the scans are done in the background." An Engineer who uses Symantec Endpoint Security at a manufacturing company stated, "It does not slow down the computer like other solutions.

Real-time scanning is a related, sought-after feature. A Project Manager who uses Symantec Endpoint Security at a law firm put it like this: "The product is a good antivirus in terms of the fact that it can do real-time scanning and scheduling. We can plan scans for the weekend. We can also control it on the server for all the clients it manages." In their case, the solution gets real-time updates of virus definition files from the internet. If there is any malware attack or something, it can immediately download them and apply the relevant definition to the clients.

> **"It works in the background and doesn't interfere with my daily work."**
>
> Read review »

> "The main benefit for us is that the protection occurs a lot more quickly than it used to."
>
> Read review »

#5 – Fast Response and Blocking

Effective threat detection and protecting depends on fast response and blocking. As a System Analyst who uses Symantec Endpoint Security explained, it is the solution's response time that is most valuable. "It is very quick," he said. The blocking features in Endpoint Protection are good. Problematic patterns can be blocked across the 11,000 workstations we have throughout India. If you apply a blocking policy, it will take effect within about 30 minutes across all machines."

The tech services company's Head of Corporate Desktop Services likewise noted, "If there are any issues, it's immediately reported to the appliance which is connected to the cloud. The main benefit for us is that the protection occurs a lot more quickly than it used to."

#6 – Automation

Automation is critical for ensuring the right threat detection and protection outcomes. In this context, Telescope Digital's Operations Manager remarked, "I like the way it allows you to automate things when you're using it with Active Directory." The government agency's Senior Network Engineer praised Symantec Endpoint Security for its automated updating. "They send out updates on a regular basis," he shared. "All that we have to do is to set it up on our server to download it, then it is distributed to the individual endpoints." Figure 2 shows what this process looks like.

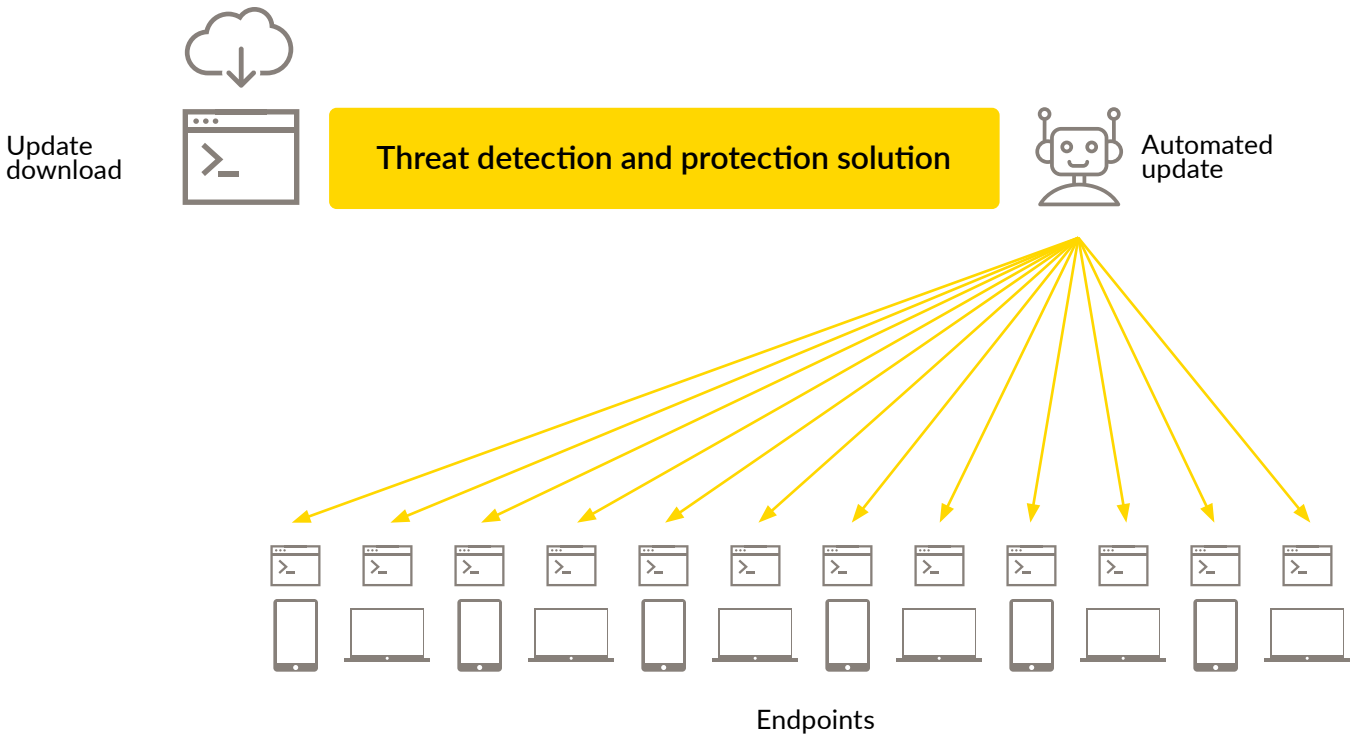


Figure 2 - Automation enables rapid updating of security settings without requiring staff member time.

#7 – Simple to Deploy and Manage

A threat detection and protection solution should be simple to deploy and easy to manage. Security teams are already stretched thin. They don't want to spend extra time dealing with complex systems. "It just works," is how a Corporate IT Manager at a pharma/biotech company described Symantec Endpoint Security. He added, "We have a console, and I can see it at a glance. I don't have any problems with it at all. I can push the client out. All the antivirus updates are managed from a single central point, and it just works."

Very user-friendly

For a Manager IT & Infrastructure staffer at an energy/utilities company Symantec Endpoint Security is "very user-friendly." He elaborated, saying, "The interface and functions are very simple for everyone to understand." Simplicity is what counted for a Principle Consultant who uses Symantec Endpoint Security Enterprise at Infosec Ventures, a tech services company.

For a Sr. Officer - Quality Assurance at a tech services company, it was Symantec Endpoint Security's administrator console that is easy to manage. He said, "Deploying patches, definition updates and report is simple."

#8 – Application and Device Control

Symantec users want application and device control. A Technical Manager who uses Symantec Endpoint Security at Mignet Technologies, a tech services company explained, "Device control is most valuable." For context, he added, "Symantec is providing all such features in the basic plan, whereas when we last checked, such a feature was not available in the basic plan of Malwarebytes."

A Sr. Admin who uses Symantec Endpoint Security at Aon Corporation, an insurance company, similarly noted, "The application and device control are valuable features, and the live update is another one. We have a schedule to check every four hours for the live update." An IT Security Specialist who uses Symantec Endpoint Detection and Response at TT Systems LLC, a tech services company, also remarked, "The most important feature is Application and Device Control. You can customize it to help stop attacks, and we have done that many times in our different environments."

It just works

"Machine learning is the number one feature of Symantec Endpoint Security Enterprise."

Read review »

#9 – Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) and Machine Learning have roles to play in threat detection and protection. There is so much data to analyze in the process that it's impossible for people to keep up. Machines are also often far better at spotting suspicious patterns in device logs and other data streams that indicate the presence of a threat.

A Sr. Professional Services Engineer who uses Symantec Endpoint Security at a software company spoke to the point, saying, "All the features are great with the core being antivirus, spyware, Artificial Intelligence and Advanced Machine Learning, and capabilities like reputation analysis based on their huge footprint, firewall, IPS and device control are very useful at protecting the environment."

He went on to say, "With Symantec adopting the AI and many of the new protection features like file-less attacks and other modern technologies, it's very attractive and makes a big difference." For a Project Manager & Tech Lead at iConnect IT Business Solutions DMCC, a tech services company, machine learning is the number one feature of Symantec Endpoint Security Enterprise.

#10 – Frequent Updating

The rapidly evolving nature of threats makes it imperative that a threat detection and protection solution frequently update itself. This capability mattered to an Industrial Automation Analyst at a mining and metals company. To him, the ability to frequently get virus signature updates is one of Symantec Endpoint Security's most important features. A Network Administrator at a financial services firm had a comparable comment. He felt that one of the most valuable features Symantec Endpoint Security is its antivirus database, which is current and updated daily.

Automated updating

Conclusion

Cybersecurity teams must be aware of threats that can harm the digital assets they are on duty to defend. Once identified, these threats must be mitigated—thereby protecting the organization's sensitive data, applications, networks and so forth. For many, this process starts at the endpoint. As PeerSpot members explain in reviews of Symantec endpoint solutions, there are 10 key success factors for effective threat detection and response. The best solutions will enable their realization. These include having a firewall present in the endpoint itself, fast response, automation, artificial intelligence and more. As these factors come together in a solution, the security team gains the ability to detect the presence of threats and act on them before they can cause damage to their organization.

About PeerSpot

PeerSpot (formerly IT Central Station), is the authority on enterprise technology. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

About Broadcom

Broadcom is a leading provider of enterprise security solutions worldwide leveraging the breadth and depth of expertise in both hardware and software security. Broadcom offers a broad portfolio of embedded security solutions, industry-leading mainframe security and payment authentication software, and a best-in-class suite of integrated Symantec cyber security software. From software to silicon, security solutions from Broadcom are widely deployed and used in networks across the globe. With such unparalleled and industry-unique offerings plus an extensive foothold in enterprise security, Broadcom is best equipped to address today's constantly evolving challenges of protecting data and digital infrastructure from multifaceted threats while enabling enterprises to navigate risk and thrive in a fast-changing world.