Symantec Endpoint Protection 14 (SEP)

For further help and advice contact the Exclusive Networks team on: Symantec_uk@exclusive-networks.com or follow #thinkyouknowsymantec for the latest news and events.

SYMANTEC ENDPOINT PROTECTION 14

Every day, we face different and increasingly complex challenges as we try to keep organisations secure. More devices, broader geographies, increased endpoints, an ever changing network perimeter and increasingly aggressive and sophisticated cyber-attacks.

SEP 14 provides one of the most highly rated endpoint protection solutions offering:

- Prevention
- Detection
- Response
- Deception
- Adaptation

Symantec SEP 14 does this by blending core technologies with new, leading edge technologies like advanced machine learning and memory exploit mitigation. At the same time, Symantec has lightened the client in SEP 14 by more than 73%, making it easier to deploy and manage.

TARGET MARKET

Primary Audience:

Enterprise-size Organisations (1,000 employees and above)

This audience desires the best in class protection against advanced threats as well as the need to maximise ROI across all security investments and have the budget to do so.

- Aviation and Hospitality
- Enterprise
- Finance
- Healthcare
- Manufacturing and Design
- Oil and Gas
- Education
- Government
- Entertainment

THE BUSINESS NEED

- Advanced threats are difficult to defend against and the endpoint is the last line of defence
- There is a concern about the massive growth of ransomware
- Businesses need to defend against fileless and stealthy attacks
- There is a desire to manage multiple technologies including: anti-malware, advanced malware protection, EDR, app control, exploit prevention and deception
- There is a need for easy-to-manage technologies that can integrate with other technologies to improve overall security

SEP 14's single lightweight console and high-performance agent **reduces network bandwidth usage by 70%.**

Symantec is currently securing more than **270,000 customers, with 125 million end-points.**

By **2021**, cyber-attacks are expected to cause **$6 trillion in damages worldwide.***

* Source: https://www.scmagazine.com/mobile-security-stats/slideshow/3370/#1

WHO SHOULD YOU BE TALKING TO?

- ✓ **Network Admin**
- ✓ **IT Manager**
- ✓ **IT Director**
- ✓ **Network Manager**
- ✓ **CISO**
- ✓ **VP/Director of Information Security**

Symantec Endpoint Protection 14 (SEP)

For further help and advice contact the Exclusive Networks team on: Symantec_uk@exclusive-networks.com or follow #thinkyouknowsymantec for the latest news and events.

DISCOVERY QUESTIONS

- What endpoint security tools are you using to block advanced threats such as ransomware and zero-day exploits? (SEP)
- What is the process your team currently follows for protecting against unknown threats, ransomware, zero-day mutating and targeted attacks? (SEP)
- How does your team monitor the security of your endpoints?
  - Are you aware of malware getting through?
  - Does your endpoint solution allow you to automate a response? (ATP: Endpoint)
- How do you currently determine an attacker's intent? (Deception)
- How do you currently ensure that application vulnerabilities are not exploited to attack your network and endpoints? (Hardening)

OVERCOMING OBJECTIONS

☒ **Objection:** "I need next-generation endpoint threat protection."

☑ **Response**: Could you tell me what you think "next-gen" means?

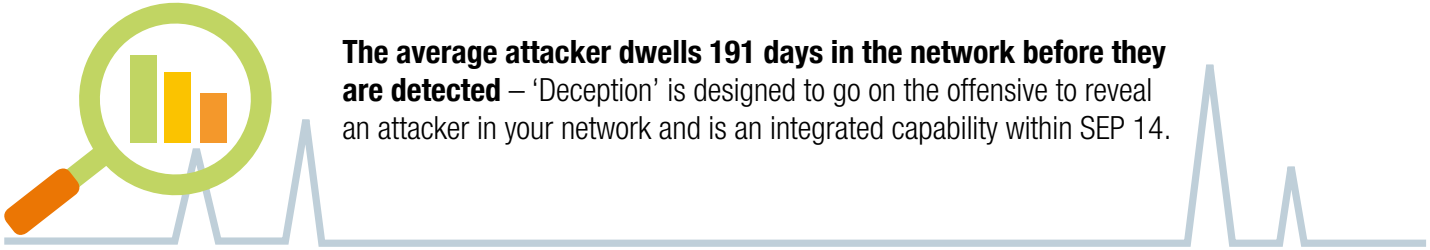
SEP 14 is the most comprehensive endpoint protection available combining essential and next-gen technologies.

☒ **Objection:** "I can get Cylance for machine learning then Microsoft for free antivirus, which is good enough."

☑ **Response:** Microsoft is not free, the cost of architecting, configuring and managing, combined with remediation time from outbreaks creates a higher cost of ownership.

☒ **Objection:** "Endpoint protection products consume too much of my bandwidth."

☑ **Response:** SEP 14 reduces bandwidth consumption by 70% which means less impact to the network and the endpoint (reducing performance related Help Desk calls).



The average attacker dwells 191 days in the network before they are detected – 'Deception' is designed to go on the offensive to reveal an attacker in your network and is an integrated capability within SEP 14.

How does SEP compare to the competition?

McAfee Together is power.

What the Competition Says:

"McAfee Security Connected and centralised management reduce complexity and improve operational efficiency."

How to Block the Competition:

Security Connected is made up of many components that need to be purchased, installed, configured and maintained which increases operational complexity.

TREND MICRO

What the Competition Says:

"Symantec endpoint solutions require multiple consoles to run the solution."

How to Block the Competition:

At this time Symantec management of solutions can be spread across multiple consoles depending on the efficacy, protection, and granularity offered by Symantec are industry leading.

CROSS-SELL OPPORTUNITIES

- ✓ **Advanced Threat Protection (ATP)**
- ✓ **Global Intelligence Network (GIN)**
- ✓ **Incident Response Service**
- ✓ **IT Management Suite**
- ✓ **Managed Security Services**
- ✓ **Content Analysis and Malware Analysis**
- ✓ **Web Security Service**