SIX CAPABILITIES TO
BOOST YOUR ENDPOINT PROTECTION

Introduction

Endpoint protection has reached a critical tipping point. Before the COVID outbreak, 70 percent of cyberattacks targeted endpoint devices.[1] Now, with employees working remotely from home offices, endpoint devices are seen as 'soft targets' by cyberattackers.

> Laptops, tablets, mobile phones, or other wireless endpoints (i.e., IoT) connected to the corporate network will grow to 30 billion devices by 2023.[2]

Now, may be the time to assess your endpoint protection and ask these questions:

- How are we securing endpoints today?
- What is our level of success in defending against malware and phishing and ransomware exploits?
- How have we altered/updated our endpoint security since the pandemic lockdown?
- With the economic instability due to the pandemic, what could a massive data breach impact your organization?

In this guide, we highlight six endpoint threat prevention capabilities (engines) that are essential to protecting your organization against the most menacing threats. By implementing these capabilities, you'll take steps to elevate your endpoint protection.

[1] "Cybercrime: The Credential Connection," IDC

[2] "The Future of Endpoint Protection, 2019-2024," by Chris Sherman, Forrester Research, Inc. January 24, 2019 https://www.forrester.com/report/The+Future+Of+Endpoint+Protection+2019+To+2024/-/E-RES137971

6 Capabilities

To Secure Your Endpoints

CAPABILITY 1

Anti-Phishing: "But that email looked so real!"

How do you rate your anti-phishing capabilities? Does your endpoint security suite include effective protection against phishing attacks? And what about advanced zero-phishing, or those attacks never seen before?

With organizations suffering multiple breach attempts daily, your employees' private information and credentials can be compromised by cybercriminals. It's no secret that socially engineered phishing can make dangerous emails look legitimate. Even with periodic training and coaching, phishing continues to be the attack method of choice for cybercriminals. Sixty percent of CISOs in one survey said phishing was a top cause for largest financial losses and it's predicted to be a higher risk over the next two years.[3]

What should you do to prevent phishing

Your endpoint solution needs an effective anti-phishing engine to detect and block access to known phishing sites, and actively prevent against complex and sophisticated attacks.

Key questions to ask when evaluating your anti-phishing capabilities

- Does your current solution prevent employees from reusing their corporate credentials on non-corporate websites? Using corporate credentials on other apps and websites broadens the threat surface.
- Does your solution include full scanning for of websites and forms and deep heuristic analysis to defend against zero-day phishing, impersonation, spear-phishing, and Business Email Compromise (BEC)?
- Does your solution perform a reputation scan and include similarity algorithms, such as visual textual similarity to well-known sites?

[3] "Driving Cybersecurity Performance," ESI ThoughtLab, June 2020 https://econsultsolutions.com/esi-thoughtlab/driving-cybersecurity-performance/

CAPABILITY 2 | Anti-Ransomware: "I only clicked once!"

How does your organization stack up against sophisticated ransomware attacks? Is it just human nature for curiosity to cloud judgement when accessing emails and websites?

The impact of a zero-day ransomware attack can be financially devastating. In 2019 alone, the cost of ransomware to enterprises (led by government agencies, healthcare providers, and educational institutions) is estimated to have exceeded $7.5 billion.[4] And it's expected to grow to a staggering $20 billion by 2021.[5]

Zero-day ransomware is lethal because your users simply don't know it's dangerous until it's too late. Click a bad link and systems can be penetrated through multiple entry points, including the web, emails, or removable media devices.

The Newhall School District in Los Angeles County suffered a ransomware attack, forcing the shutdown of distance learning for 6,000 elementary school students.[6] "This obviously came at a difficult time for us since we're 100% digital learning," said Newhall Supt. Jeff Pelzel.

Greg Lindner, the county Office of Education's chief technology officer said "about two-thirds of attacks take place through email and phishing scams, while downloads and hacking are also involved."

What you should do to prevent ransomware attacks

A high-performance anti-ransomware engine monitors changes to files on user drives and identifies ransomware behavior such as non-legitimate file encryption. Once such behavior is detected, smart snapshots of the attacked system will help block the attack and recover encrypted files automatically, regardless of the encryption used.

Key questions to ask when evaluating your anti-ransomware capabilities

- What are you currently do to protect against ransomware?
- Has your current solution included behavioral analysis to form stronger prevention?
- Does you endpoint protection include automatic blocking and recovery of encrypted files?

[4] "20 Ransomware Statistics You're Powerless to Resist Reading," by SSL Store, hashedout, February 27, 2020 https://www.thesslstore.com/blog/ransomware-statistics/

[5] Ibid.

[6] "Ransomware Attacks Halt Some Online Learning in L.A. County, by Andrew J. Campa, Los Angeles Times, September 16, 2020 https://www.govtech.com/public-safety/Ransomware-Attacks-Halt-Some-Online-Learning-in-LA-County.html

CAPABILITY
3

Content Disarm and Reconstruction (CDR): "I trusted my partner!"

Can you assure that all incoming files are safe and do not impact employee productivity? Are your partners practicing stringent endpoint protection with all interactions with your employees?

What you should do to trust incoming files

In our fast-paced world, and one now disrupted by the COVID outbreak, all incoming emails with attached files inspection should be mandatory practice. These include files entering the network through the web or removable devices. Downloading uninspected files to user desktop PCs and laptops significantly increases the chances of a successful exploit. Content Disarm and Reconstruction (CDR) provides an automatic file sanitization capability.

Key questions to ask when evaluating your CDR capabilities

- Do you have proactive and rapid sanitization capability to remove exploitable content from documents?
- Are you 100% sure that files are clean?
- Is your solution transparent to employees so it does not impact productivity?

CAPABILITY 4 | Anti-bot: "What the heck is a bot?"

Can you automatically detect and contain "bot-related" infections before sensitive data is exposed? How familiar are you with malicious bot attacks?

Bots, those software programs on the internet that perform repetitive tasks, are used to steal personal, financial, intellectual property, or organizational data. SPAM emails attack resources in denial of service attacks or execute bandwidth consumption that harms productivity.

What you should do to prevent malicious bots

Ensure your anti-bot scheme detects infected machines by continuously monitoring outgoing traffic and identifying communications with command and control (C&C) servers. When an infection is detected, your endpoint security solution blocks traffic, remediates the attack, and isolates the machine to prevent lateral infection spread.

Key questions to ask when evaluating your anti-bot capabilities

- Does your endpoint security solution include anti-bot capabilities that detect infected machines using continuous monitoring of outgoing traffic?
- Are you able to identify the communications that occur with your command and control servers?
- How reliable is your current detection, blocking and remediation capabilities to effectively protect against malicious bots?

CAPABILITY
5

Automated post-breach detection, remediation, and response: "The threats are constant!"

Can your endpoint security solution automatically visualize and analyze incidents, contextualize them, and remediate them? Are you relying on manual remediation?

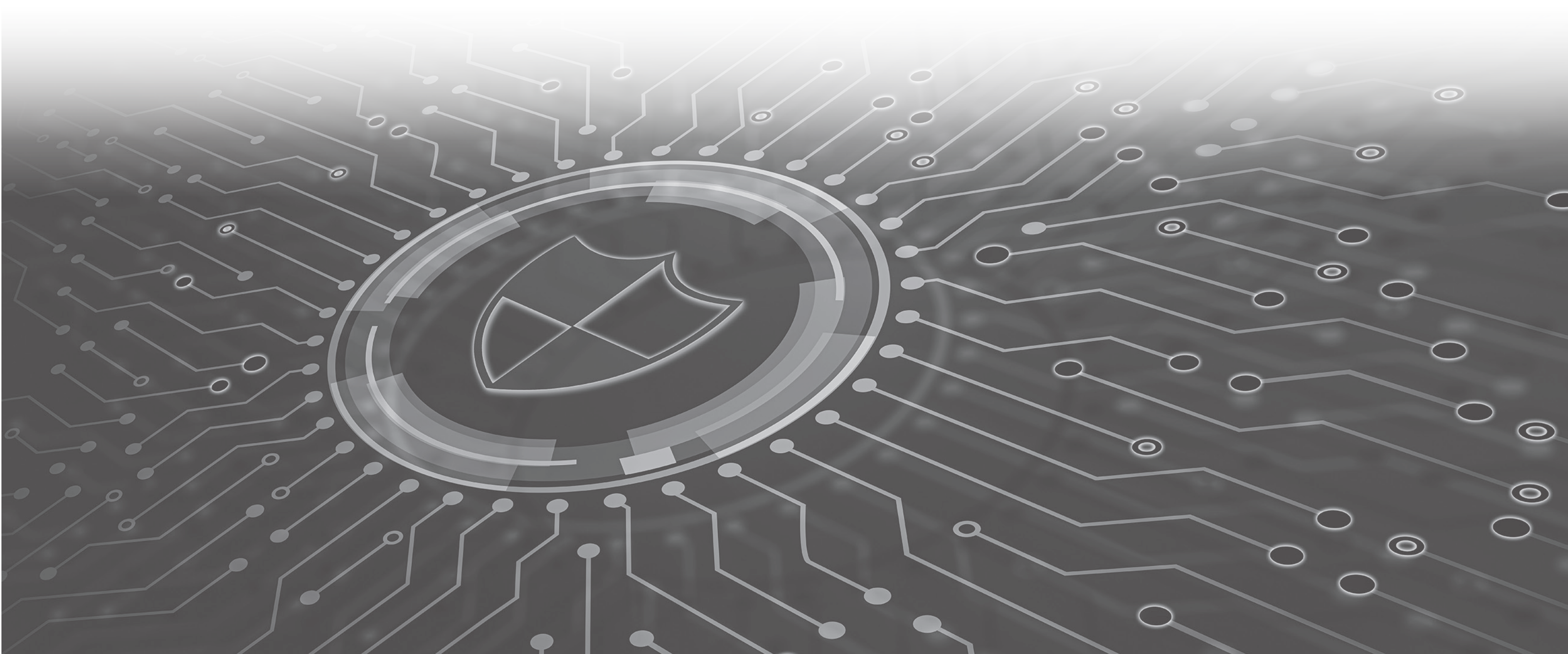
Traditional endpoint detection and response (EDR) solutions can detect suspicious behaviors, but, with few out-of-the-box rules, they do not support automatic remediation. With manual remediation, you run the added risk attack residue that were not cleaned. This process can be time-consuming, and can often require a highly trained analyst.

What you should do to make endpoint protection more effective

Robust attack diagnostics and visibility allow system administrators and incident response teams to effectively triage and resolve attacks. This greatly reduces the time needed for analyzing incidents, while freeing up to teams to focus on other more critical tasks.

Key questions to ask when evaluating your automated security capabilities

- Does your endpoint security solution automatically and thoroughly remediate the entire cyber kill chain?
- Do you use forensics to automatically monitor and record endpoint events, including affected files, processes launched system registry changes and network activity?
- Once an attack has been detected, can the infected device can be automatically quarantined to prevent lateral infection-spread and restore the endpoint to a safe state?



CAPABILITY
6

Mobile phone security: "Are employee phones really vulnerable to cybercrime?"

Do employees use their own mobile phones (BYOD) to access your network? Are they protected like your other endpoint devices?

More than ever before, employee mobile phones have become an essential tool with the emergence of virtual offices. The shift from office to home has meant employees transferring desktop and laptop computers to their new set up. Mobile phones, especially those with network access, however, can be easily overlooked when it comes to security.

Malware attacks against mobile devices — and Android handsets in particular— have skyrocketed. Hackers increasingly turned their attention to attacking smartphones with credential-theft, surveillance, and malicious advertising.[7]

What should you do protect mobile devices?

Accurate threat detection and efficient response are critical components of preventing advanced attacks on smartphones and tablets. Traditional anti-virus and app reputation solutions can identify known threats, but they can't detect zero-day malware or vulnerabilities in networks, operating systems, and apps.

Key questions to ask when evaluating your mobile phone security

- What are you doing to secure employee network-connected mobile devices?
- Are you using a behavioral approach to analyze threats across your network, operating system, and apps?
- Are you getting on-device network protection to prevent phishing, access to malicious websites, detect bot-infected devices, plus URL filtering?

[7] "Mobile malware attacks are booming in 2019: These are the most common threats," by Danny Palmer, ZDNet, July 25, 2019 https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/

Your Next Step

Seek a comprehensive endpoint protection for these times

Protecting your networks, users, partners, and third-party suppliers requires endpoint protection that can secure your organization against prevalent and dangerous cyberattacks.

SandBlast Agent from Check Point Software is a comprehensive security for endpoint devices, protecting users wherever they're located and wherever they go. It offers the capabilities discussed here, plus includes innovative technologies such CPU-level sandbox, threat extraction, and deep behavioral analysis and forensics and machine learning to deliver the high catch rates (100% for HTTP and email malware, and evasions and low false positives (0.8%) .[8]

Check Point SandBlast Agent Earns AA Product Rating in NSS Labs 2020 Advanced Endpoint Protection Test. Get the details of this definitive endpoint protection test.

SandBlast Agent has become an industry standout as an effective endpoint security solution that automatically and completely remediates the entire cyber kill chain to shorten response time. It has been designed with innovative threat prevention technologies, insightful visibility, and response capabilities, and a comprehensive endpoint protection in a single solution.

Further validation of SandBlast Agent comes from customers. According to the latest Gartner Peer Insight research, nearly 90% of Check Point's users recommend products to their colleagues. The below reflects how customers view SandBlast Agent:

> *"The Check Point SandBlast Agent protected our organization's intellectual assets. There were numerous incidents where when users download the attached file from email or form any other files Check Point SandBlast identifies these threats. It removes those threats but preserves those files intact. No matter what anti-filter software used if the file bypasses the rule Check Point SandBlast catches the threats in the files and provides detail information of the file that has been quarantined. We have been using this product for more than 2 years and happy with the software."*
>
> – Systems Administrator, Manufacturing, June 7, 2020

> *"We are using the agent to prevent users from download and opening documents in their browser before they have been properly scanned or striped of bad elements. We have notice a lot less malware alerts in our system as those elements are striped out from any download. Additional, we find employees reaching out to us more about phishy attachments which shows they are on guard more often about what they are downloading."*
>
> – Systems Administrator, Systems Integrator, May 29, 2020

> *"Check Point Sandblast Agent was for us the best suited Advanced Endpoint Protection. It was deployed quickly within our world-wide organization. The management console has an intuitive user interface and is easy to use."*
>
> – Senior Security Analyst, March, 2020

Want more information to solve your endpoint security challenges? Go to Endpoint Protection and Threat Prevention website, or request your demo.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com

© 2020 Check Point Software Technologies Ltd. All rights reserved.