BUYER'S GUIDE

ENDPOINT PROTECTION

THE 5 MUST-HAVES AND 5 PRINCIPLES OF A SOLUTION THAT WILL PROTECT YOUR ORGANIZATION'S ENDPOINTS AGAINST ANY AND EVERY ATTACK VECTOR

Cyber Talk

CONTENTS

INTRODUCTION:
THE GROWING CHALLENGE OF ENDPOINT PROTECTION

COMPLEXITY, UNPREDICTABILITY, SOPHISTICATION

Protecting the endpoint has never been more challenging. The complexity and unpredictability of attacks and threats are continually on the rise, and threat actors are becoming more and more sophisticated in their ability to exploit vulnerabilities, breach organizations' IT infrastructures, and hack into sensitive data.

> *70% of successful cyber-attacks originate at the endpoint.*
>
> *(IDC)*

PROLIFERATION OF DEVICES, PANDEMIC-DRIVEN REMOTE WORK

On top of all the complexity and unpredictability that security professionals have been facing over the past several years, the potential attack surface has also profoundly increased.

One of the main drivers for this phenomenon comes from the fact that following the outbreak of the coronavirus, the global workforce is at home for much, if not all of the time – which means that work is happening at the endpoint.

As a result, businesses of all sizes and shapes have had to adapt at the speed of light to make significant infrastructure changes so their employees could work from home.

But that was, and still is, far from simple. Employees working from home, are often more prone to less than cautious behavior and non-compliance with corporate policy.

Furthermore, cybercriminals have been rigorously developing new strategies for exploiting this new situation so they can breach corporate networks.

> ***Of organizations that required remote work as a result of COVID-19, 70% said remote work would increase the cost of a data breach and 76% said it would increase the time to identify and contain a potential data breach.***
>
> *(Ponemon Institute)*

To illustrate the dramatic increase in the threat against the endpoint that has resulted from global work from home policies:

- In Q3 2020, Check Point Research saw a 50% increase in the daily average of ransomware attacks, compared to the first half of the year.
- Since January 2020 Covid-themed campaigns have been on the rise, coming in multiple forms, including malicious email attachments, self-propagating and modular Trojan attacks, and phishing attempts via malicious domains.
- Cyber criminals are targeting employees remote collaborating via Zoom more than ever.

ENDPOINT SECURITY MUST EVOLVE

As a result of these trends unfolding over recent months, companies and their IT and security teams must evolve their skills and methodologies to prevent such exploitations from disrupting the business and causing both financial and reputational damage.

> ***Older antivirus solutions offer insufficient protection against today's advanced threats and lack speed of response, nor do they provide the capability to show the root cause or damage done.***

(Gartner) [1]

It's no surprise then that in a study conducted in mid-2020, 39% of security professionals reported that they are not confident in the resilience of their existing endpoint protection solution, and that Gartner predicts that by the end of 2023, more than 50% of enterprises will have replaced their antivirus products.

39%

Security professionals are not confident in their existing endpoint protection

50%

Enterprises will replace their solution by 2023

[1] *Gartner, Market Guide for Endpoint Detection and Response Solutions, 2019.*

HOW TO DECIDE?

This is why cyber security researchers have set out to present security leaders with a go-to guide for understanding the **five must-haves** for any endpoint protection solution, the **five principles** of the optimal solution, and what are the **key questions** that should be asked when evaluating the options.

THE 5 MUST-HAVE ENDPOINT PROTECTIONS

A solution that can protect the organization and its ever-growing number of endpoints from any and every attack vector, while also ensuring that there is no disruption to business continuity, requires – first and foremost – the following five must-haves.

> *Security leaders are asked to protect endpoints from attacks, while also allowing access from any device to any application over any network, with minimal impact on user experience.*
>
> *(Gartner)*[2]

[2] *Gartner, Hype Cycle for Endpoint Security, 2020, July 2020*

MUST-HAVE #1:

ANTI-PHISHING CAPABILITIES

The phishing emails of today involve very sophisticated social engineering techniques that are designed to dupe employees into disclosing sensitive data and/or enabling fraudulent financial transactions.

A solution with anti-phishing capabilities enables the organization to stay ahead of cybercriminals and remove the burden of detection from the user who is targeted for manipulation.

QUESTIONS TO ASK WHEN EVALUATING ANTI-PHISHING CAPABILITIES:

- Does the solution actively prevent complex and sophisticated attacks such as zero-day phishing, impersonation, spear-phishing, and Business Email Compromise (BEC)?
- Does it perform full scans of websites and forms and deep heuristic analysis?
- Can it prevent employees from reusing corporate credential on non-corporate websites?

MUST-HAVE #2:

ANTI-RANSOMWARE CAPABILITIES

Ransomware, particularly zero-day ransomware can be very challenging to combat. By its very nature, we do not know that it exists until it strikes. And when it does, it does so without warning, leaving the security team unprepared.

> *In the US alone there has been a 98% increase in ransomware attacks during Q3 2020.*
>
> *(Check Point Research)*

To complicate matters even more, it can penetrate the organization through multiple entry points, including the web, emails, and removable media devices. An endpoint protection solution with advanced anti-ransomware capabilities will enable the organization to mitigate the risk and avoid the damage of a successful attack.

QUESTIONS TO ASK WHEN EVALUATING ANTI-RANSOMWARE CAPABILITIES:

- Does the solution protect my organization against sophisticated zero-day ransomware attacks?
- Does it include an anti-ransomware engine that monitors changes to files on user drives and identifies ransomware behavior such as illegitimate file encryption?
- Can it block an attack and recover encrypted files automatically?

MUST-HAVE #3:

CONTENT DISARM AND RECONSTRUCTION (CDR)

On the one hand organizations can't afford to disrupt productivity by inspecting every file that is attached to incoming emails.

On the other hand, they can neither take the risk of allowing files to be downloaded to users' PCs and laptops without first inspecting them.

This is why an endpoint security solution must include an automatic file sanitization capability, also known as Content Disarm and Reconstruction (CDR) or Threat Extraction.

QUESTIONS TO ASK WHEN EVALUATING CDR CAPABILITIES:

- Does the solution help the security team make sure that all incoming files are safe without disrupting employee productivity?
- Can the solution remove exploitable content from documents by sanitizing them from potentially harmful elements, cleaning them, and delivering 100% sanitized versions within seconds?

MUST-HAVE #4:

ANTI-BOT CAPABILITIES

Bots present a formidable security threat. They are often used by hackers in an Advanced Persistent Threat (APT) attack against a particular individual or organization.

Bots connect to the organization's command and control servers, where the hacker controls the bot remotely and instructs it to execute illegal activities.

Such bot attacks can cause data theft – of personal, financial, intellectual property, or organizational data. To prevent these attacks, the endpoint protection must include the requisite anti-bot capabilities.

QUESTIONS TO ASK WHEN EVALUATING ANTI-BOT CAPABILITIES:

- Can the solution automatically detect and contain bot-driven infections before sensitive data is exposed?
- Does it continuously monitor outgoing traffic and identify the communications that occur with the command and control servers to detect infected machines?
- Can the solution block infected traffic, remediate the attack, and isolate the compromised machine to prevent the potential spread of a lateral infection?

MUST-HAVE #5:

AUTOMATED POST-BREACH DETECTION, REMEDIATION, AND RESPONSE

While traditional endpoint detection and response (EDR) solutions can detect suspicious behaviors, they typically have very few out-of-the-box rules nor can they perform automatic remediation.

> *Automation is a major differentiator where security staff are scarce and there is a need for rapid detection of advanced persistent threats and to provide the fastest remediation of these.*
>
> *(Gartner)*[3]

Lacking automation means that the risk of attack residuals is greater, not to mention that manual processes are time consuming and can potentially lead to greater impact.

QUESTIONS TO ASK WHEN EVALUATING AUTOMATION CAPABILITIES:

- Can the solution automatically analyze, contextualize, and remediate incidents?
- Can the solution automatically determine if what just happened was a real attack, how the hacker got in, what the impact on the business is, and how the systems should be cleaned?

[3] *Gartner Market Guide for Endpoint Detection and Response Solutions, Paul Webber, Prateek Bhajanka, Mark Harris, Brad LaPorte, December 2019.*

THE 5 PRINCIPLES OF THE OPTIMAL ENDPOINT PROTECTION SOLUTION

PRINCIPLE #1:
A PREVENTION-FIRST APPROACH

There is no doubt that preventing an attack saves an organization a lot time and money. The cost of a malware attack, for example, is estimated to reach to $2.6 million per company, on average. And it doesn't end at cost and time. There is also always the risk of damage to brand equity and customer trust.

Needless to say, prevention of a network breach will always trump detection and remediation.

QUESTIONS TO ASK
TO ENSURE THAT THE SOLUTION TAKES A PREVENTION-FIRST APPROACH:

- Can it perform preemptive protection with **anti-phishing** capabilities, including for unknown phishing sites, **anti-ransomware, CDR, exploit prevention**, and **anti-bot** capabilities?
- Can it operate in **prevention mode** (in addition to detection mode), in cases where the threat is clear and the risk is high?
- Does it **notify and provide users with information** and knowledge in case of a detected cyberthreats?

PRINCIPLE #2:
AI-DRIVEN MULTILAYERED SECURITY

Today's security reality is complex, characterized by many layers. There are millions of strains of unknown malware and many sophisticated evasion techniques. This means that stopping today's most dangerous attacks requires inspecting more than one layer.

> *91% of cybersecurity professionals are concerned that hackers will use artificial intelligence (AI) in cyberattacks against their company that are more sophisticated and harder to detect.*
>
> *(TechRepublic)*

However, traditional solutions, including antivirus, sandboxing, and legacy endpoint protection products, offer limited inspection and lack the sophistication required for such complexity.

To outwit today's sophisticated cybercriminals, the endpoint protection solution must be driven by artificial intelligence and be able to inspect every layer of the attack surface, going beyond traditional detection methods such as signatures and rules.

QUESTIONS TO ASK
TO ENSURE THAT THE SOLUTION OFFERS AI-POWERED MULTI-LAYERED SECURITY:

- **Does it include AI engines that perform a static analysis** of files and executables for identifying unknown malware before it is executed?
- **Does it leverage a collaborative knowledge base** for gaining access to real-time, dynamic security intelligence to deliver the knowledge and insights?
- **Does it have a behavioral analysis** engine for collecting behavioral indicators from devices, with the ability to correlate such indicators?
- **Does it apply behavioral heuristics, rules, and machine learning models** for optimizing malware identification and classification?

PRINCIPLE #3:
POST-INFECTION REMEDIATION AND RECOVERY

Unfortunately, regardless of how comprehensive the security solution may be, one cannot assume that the organization won't get hit with a cyberattack. Everyone gets compromised at one point or another.

Accordingly, it is critical to be prepared with state-of-the-art post-infection remediation and recovery capabilities.

> *77% of more than 3,600 security and IT professionals polled indicating they do not have a cyber security incident response plan.*

(ComputerWeekly)

QUESTIONS TO ASK TO ENSURE THAT THE SOLUTION ENABLES POST-INFECTION REMEDIATION AND RECOVERY:

- **Does the solution perform automatic quarantining** of infected machines, to prevent the attack from spreading by lateral movement across the corporate network?
- **Does it constantly monitor and record** endpoint events? This should include affected files, processes launched, system registry changes, and network activity
- **Does it perform automatic remediation and sterilization** of the entire cyber kill chain, for restoring the device to the last clean point?
- **Does it include advanced incident response** algorithms and deep analysis capabilities of the raw forensic data?
- **Does it enable full recovery** of ransomware-encrypted files?
- **Does it perform proactive threat hunting** with a mechanism for recording endpoint events for long-term retention?

PRINCIPLE #4:

A CONSOLIDATED SECURITY AND THREAT INTELLIGENCE ARCHITECTURE

As complicated as ensuring security can be, the task becomes all the more complex when multiple solutions from multiple vendors must be managed.

> *By 2022, 60% of organizations that leverage endpoint detection and response (EDR) capabilities will use the endpoint protection solution from the same vendor or managed detection and response services.*
>
> *(Gartner)* [4]

It is no surprise then, that in a recent survey 99% of security professionals agree that using solutions from multiple security vendors introduces unnecessary challenges. And 69% agree that prioritizing vendor consolidation would lead to better security.

QUESTIONS TO ASK TO ENSURE THAT THE SOLUTION HAS A CONSOLIDATED ARCHITECTURE:

- Is it tightly integrated with the **network?**
- Is it tightly integrated with the **cloud** infrastructure?
- s it tightly integrated with the **mobile security** infrastructure?

[4] *Gartner Market Guide for Endpoint Detection and Response Solutions, Peter Firstbrook, November 2018.*

PRINCIPLE #5:
UNIFIED AND CLOUD-BASED MANAGEMENT

An endpoint protection solution that serves as a single, unified agent streamlines processes, simplifies management, and reduces the total cost of ownership (TCO).

> *By 2025, cloud-delivered EPP solutions will grow from 20% of new deals to 95%*
>
> *(Gartner)*

Furthermore, the benefits of the cloud are well known – from elasticity, to flexibility, scale, and speed. There is no argument that cloud is the way to go.

QUESTIONS TO ASK TO ENSURE THAT THE SOLUTION HAS UNIFIED AND CLOUD-BASED MANAGEMENT:

- Does the solution unify endpoint protection (EPP), EDR, VPN, NGAV, data protection, and web-browsing protection?
- Does it offer cloud-based **provisioning** and **monitoring** of devices and policies?
- Does it ensure full redundancy?
- Does it offer **flexible deployment** options for both cloud and on-prem?

IN SUMMARY

As we have seen, the domain of endpoint protection is one that is fraught with complexity and challenge. There have never been more endpoints to protect, and the techniques of cybercriminals have never been more sophisticated.

Overcoming the challenge requires a new approach to the task, with a solution that includes 5 must-have capabilities:

- Anti-phishing
- Anti-ransomware
- Content Disarm and Reconstruction (CDR)
- Anti-bot
- Automated post-breach detection, remediation, and response

The optimal solution must also be driven by the following 5 principles:

- A prevention-first approach
- AI-driven multilayered security
- Post-infection remediation and recovery
- Unified and cloud-based management
- Consolidated security and threat intelligence architecture

By pulling together these powerful capabilities and taking this modernized approach to endpoint protection, security teams can be confident that they are taking the most robust approach to securing the enterprise with sophistication that outwits even the most sophisticated cybercriminals.