Elevating Endpoint Security: Why Modern Threats Need Defense Beyond EDR

by Suril Desai | November 20, 2024

Endpoint security remains a cornerstone of modern cybersecurity strategies, primarily driven by Endpoint Detection and Response (EDR) solutions. While EDR has become a widely adopted safeguard for user and server environments, it has a set of detection gaps that need to be complemented. The increasingly sophisticated tactics of adversaries demand a robust, layered approach to threat detection that transcends traditional methods. This is where cyber deception comes into play as an indispensable complement to EDR, reinforcing the defense-in-depth strategy essential for comprehensive threat protection.

Understanding the Gaps in EDR Coverage

Despite its strengths, EDR often leaves critical coverage gaps that can be exploited. Here are key scenarios where attackers take advantage of EDR design limitations:

Unmanaged Endpoints: Achieving 100% EDR coverage is nearly impossible due to factors such as legacy devices, special form-factor hardware (e.g., printers, cameras), and industry-specific equipment like medical and point-of-sale systems. Such devices are often integrated into identity stores like Active Directory (AD), making them prime targets for attackers. A startling 25% of attacks are initiated from unmanaged devices, exposing a glaring weakness in conventional EDR coverage.
Example: An attacker could compromise an unmanaged printer, use it to download malware, and escalate their reach to AD—completely bypassing the EDR's visibility.

Virtual Desktop and Virtualized Environments: Short-lived VDI sessions and third-party virtual machines present another challenge, as they often aren't compatible with EDR agents. This lack of visibility can lead to missed threats that leverage these environments to access critical data or pivot deeper into the network.
Example: Attackers may exploit non-persistent VDI images to infiltrate an organization's data and applications undetected.

Application Whitelisting: Certain applications must be whitelisted to function properly, leading to inherent visibility gaps.
Example: Attackers have exploited trusted software like SolarWinds Orion by leveraging its whitelisted status to conduct malicious activities.

EDR Evasion Tactics

Attackers have continually developed methods to bypass even well-deployed EDR systems, exploiting solution-specific vulnerabilities and adapting their strategies over time. One commonly observed tactic involves privilege escalation. Attackers use sophisticated techniques, such as DLL injection into privileged agents or services with high-level access on the endpoint, to elevate their privileges and gain local machine admin rights. With these elevated rights, attackers can reboot the device into safe mode—a state where EDR agents are not typically active—allowing them to carry out malicious activities undetected from within the safe mode environment.

Additional evasion pathways have emerged that further highlight EDR's limitations. For instance, attackers leverage "living off the land" (LOTL) techniques, which involve using legitimate system tools and processes that blend seamlessly with normal operations, making them difficult for EDR solutions to flag. Another sophisticated evasion method includes the use of signed kernel drivers. These drivers, though legitimate in appearance, are manipulated to execute malicious activities that bypass EDR detection.

An illustrative example of this approach is the Sphynx variant of the Alphv ransomware, which successfully leveraged signed kernel drivers to evade detection mechanisms. Such exploits underscore the evolving threat landscape and the need for a broader, more resilient defense strategy beyond traditional EDR.

Dear Adverts!

We are pleased to inform you that testing of basic features ALPHV / BlackCat 2.0: Sphynx is completed. All affiliate plus when creating a new configuration will be offered the opportunity to choose a version. To maximize the non-detectable binary time, the software will only be available for active affiliate plus.

The code, including encryption, has been completely rewritten from scratch. By default all files are frozen. The main priority of this update was to optimize detection by AV/EDR, the following steps were taken to achieve this goal:

- A new technique has been added to mask the encryption process similar to file archiving. When you activate this feature, you can also configure the masking strategy. Currently only zip masking mode is available, the list will be expanded.
- The --access-token startup key has been removed. Now any of the generated keys in launch_keys.txt file can be used for launching files, e.g:

```
C:\alphv.exe 195ToGOF -oAC --AUC -X99odn4 -pdTvb -ewi -vyJtKOOTxBdQ7Ql9

./alphv dm -5 -sEsx -QafOuyRY -Tn3588c5 -fb80noL0X -yUT
```

- When creating the configuration, it is now possible to define a readme distribution strategy. This is a red rag for any antivirus, which is not always possible to disable. Therefore we recommend to make several configurations. In the first build, disable readme distribution completely and encrypt user workstations and/or less visited servers, and in the second build, encrypt and distribute readme.
- Also, it is now possible to define a strategy for renaming encrypted files.
disabled: do not rename (do not add an extension),
all: rename everything (add .xyzwz extension),
onlyunknownextensions: only rename unknown extensions. It is recommended not to rename files when AB is enabled.

Undoubtedly, each feature deserves to be described in a separate article, but we'll leave the work to our favorite antivirus analysts, and for you We'll just list the most important changes.

- The process of interaction with the network has been completely redesigned. Network orbs search and encryption algorithm has been improved.
- Completely redesigned process impersonation logic for encrypting network files without rights.
- System resource usage has been architecturally redesigned. Encryption speed has increased many times over.
- Support for Glibc 2.5+, which was released in 2006, has been added for *nix. This means that it is now possible to encrypt very old *nix-like systems. Including ESXI<=5.0.
- The -v / -ui keys have now been merged. If you want to monitor the encryption process, you have to add to the command line the -v key, e.g:

```
C:\alphv.exe 195ToGOF -oAC --AUC -X99odn4 -pdTvb -ewi -vyJtKOOTxBdQ7Ql9 -v

./alphv dm -5 -sEsx -QafOuyRY -Tn3588c5 -fb80noL0X -yUT -v
```

Otherwise, the locker process will go into a backgrounder.

- Test simplified the configuration editing interface. In case of urgent need, we will return the ability to point config

The Case for a Layered Defense Strategy

The concept of layered defense as part of a defense-in-depth approach to cybersecurity has been universally accepted by both industry and academia. This strategy is grounded in the fundamental insight that no single layer is sufficient to defend against all possible attack vectors.

Adversaries continually exploit the coverage gaps within existing security layers, such as targeting unmanaged endpoints, to access critical assets. Advances in AI have further complicated this landscape, enabling attackers to deploy increasingly sophisticated and automated tools that can pinpoint and exploit weaknesses not covered by traditional EDR solutions. These AI-driven tools make it easier for adversaries to navigate defenses with precision and stealth.

In this asymmetric battle, where defenders must protect against a wide array of evolving threats while attackers need only find one vulnerability, it is essential for cybersecurity teams to adopt a multi-layered defense strategy. While EDR forms a solid foundation, it is primarily focused on detecting “known bad” and must be reinforced by independent detection layers that can detect evolving and unknown threats. This approach must combine various strategically chosen detection methods to counteract modern threats effectively. Building these additional layers that function independently is vital to avoid overlapping vulnerabilities and ensure that gaps present in one method are not replicated in another.

These independent detection methods, including technologies like cyber deception, are necessary to create a comprehensive defense system that can better withstand the adaptive strategies employed by attackers.

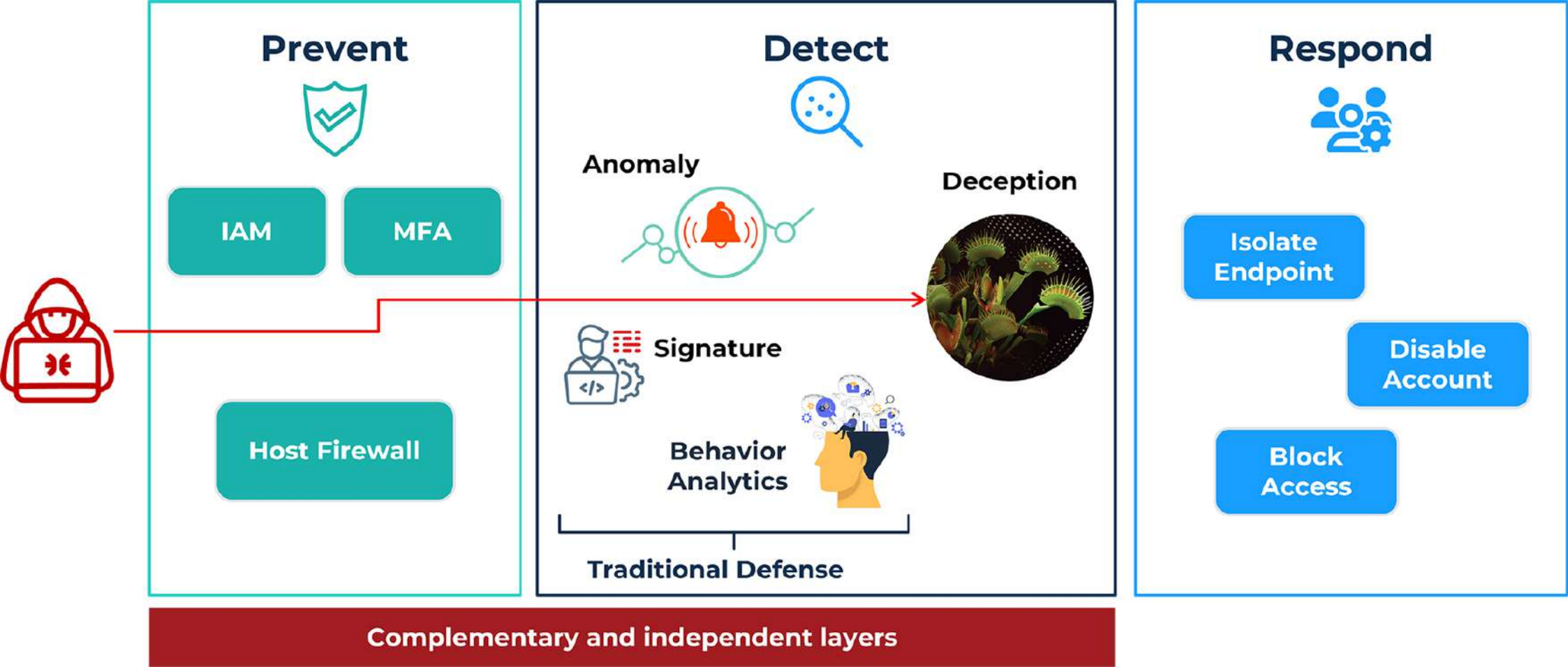
The Role of Cyber Deception

Cyber deception is based on the concept of predicting the goals of the adversary, strategically placing traps, and closely monitoring any interactions with these traps. Unlike conventional security measures, deceptions are not part of legitimate workflows. Any engagement with them is a clear indication of malicious intent, providing an early warning that enables swift defensive action.

Deception-based threat detection stands apart from the methodologies employed by EDR solutions, which often rely on anomaly-based detection, behavior-based analysis, or signature matching to identify TTPs (tactics, techniques, and procedures) associated with malicious activity. Deception shifts the focus to the attackers' objectives, laying out traps that are designed to draw adversaries in. Deception-based detection is agnostic to the attacker TTPs, providing visibility to threats that evade TTP-centric detection approaches.

Because deception-based detection operates independently from EDR's detection mechanisms, it serves as an essential complementary layer that extends detection coverage to include unknown threats, evolving threats and mitigates the gaps found in existing security layers that are focused on known threats. This independence is crucial to ensuring that the same gaps are not shared across multiple layers, enhancing overall defense effectiveness.

Incorporating deception technology alongside EDR allows defense teams to achieve broader visibility into threats that EDR might miss. This combination can significantly accelerate the detection window, reducing the Mean Time to Detect (MTTD) and preventing adversaries from gaining a foothold and escalating their attacks. By leveraging deception as part of a comprehensive defense-in-depth strategy, organizations can protect critical assets more effectively and maintain a proactive stance against advanced cyber threats.


Prevent
IAM
MFA
Host Firewall
Detect
Anomaly
Deception
Signature
Behavior Analytics
Traditional Defense
Respond
Isolate Endpoint
Disable Account
Block Access
Complementary and independent layers

Sample Attack Scenario: Deception-Enabled Defense

Consider a scenario where an attacker gains initial access to an environment and begins reconnaissance to identify unmanaged endpoints to target. The attacker performs enumeration against the enterprise catalog, such as Active Directory (AD), and identifies a printer. Exploiting a known vulnerability, the attacker mounts an attack against this printer and uses LDAP queries from the domain-joined printer to elevate privileges and gain domain dominance. This type of attack would go undetected if the defense team relied solely on EDR, as there would be no EDR agent installed on the unmanaged endpoint (the printer).

However, with deception technology, defense teams can deploy a decoy printer designed to attract the attacker's interest by giving it an enticing hostname, such as "exec-team-printer," and registering it within the AD catalog. When the attacker performs reconnaissance, this decoy printer appears in the output and draws the attacker's focus. Any attempt to exploit the decoy triggers an immediate, high-fidelity alert, giving the defense team early visibility into the threat. The team can then respond promptly to isolate the attacker and prevent the attack from propagating further.

This example demonstrates the effectiveness of cyber deception as a critical component of a defense-in-depth strategy. By deploying deception alongside EDR, organizations enhance their ability to detect and respond to threats that would otherwise evade traditional endpoint security measures. Deception expands visibility, accelerates detection, and provides a proactive means of protecting critical assets against sophisticated adversaries.

Conclusion

As the cyber threat landscape continues to evolve, relying solely on EDR is insufficient for comprehensive protection. By integrating cyber deception into the defense-in-depth framework, organizations can achieve the necessary layered security approach. Deception not only enhances threat visibility but also accelerates the detection process, effectively reducing the Mean-time-to-Detect (MTTD) and preventing adversary breakout to protect critical assets.