BLOKWORX

STACK vs. STACK

ENDPOINT SECURITY

EDR + DEFENDER *VS.* LIMACHARLIE + DEEP INSTINCT

Positioning your security stack for prevention and threat protection

OVERVIEW

MSPs have recently asked us if Microsoft Defender paired with an EDR is sufficient for security. They like maximizing their investment in the licensing they're already paying for (Microsoft), and the number of alerts coming from the EDR makes them feel like they're proving value to clients.
The question is: ***Are the cost savings when paired with an EDR providing adequate protection?*** We reviewed the basic functionality, third-party testing, and conducted our own efficacy testing to best answer this question for our Partners.

TAMPERING/DISABLING

Anti-tampering is designed to prevent modifications to the setting or configuration of the security product, most importantly to prevent the ability to disable said security. Windows Defender and Deep Instinct can be disabled in very different ways, demonstrating stratified security postures:

You can leverage Microsoft's own commands against its solution to disable it using at least two methods:

- PowerShell Leveraging Set-MpPreference
  - LOLBAS/LOLBIN files bypass Defender with "valid" cert which then launch their payloads to impair defenses
- Leveraging sc or net commands to alter settings/disable services

Deep Instinct can only be disabled in the one method:

- Disable via a console protected with login/password and 2FA

EDR CAPABILITIES

We firmly believe that EDR is a solid addition to your security stack, if the rest of the stack is equally capable and synergizes well. In this comparison, we'll look at a channel-leading EDR solution often chosen to pair with Windows Defender and compare it to MAED+EDR services (powered by Deep Instinct and LimaCharlie) offered by BLOKWORX.

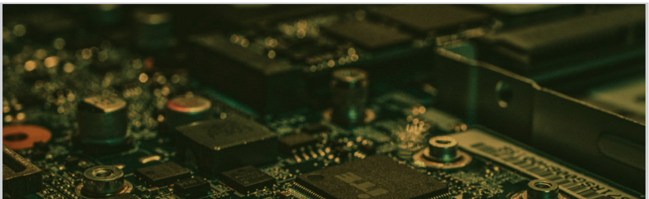
HANDLED NOT HOMEWORK

Both EDR solutions do specifically what they say they will, they detect and respond to threats on machines. However, in most cases, the other EDR will not remediate. It will also not prevent before an item is detonated (that's the detection part). Instead, it will assign homework to the end customer.

The channel-leading EDR sends out e-mails outline items found in the environment with "next steps" mostly comprised of "you need to take this action on the machine," meaning the questionable object is still on the machine and could be leveraged. BLOKWORX solution both prevents and remediates without client intervention.

QUALITY OF LIFE IMPROVEMENTS

The BLOKWORX solution is capable of detection and response, but has other quality of life improvements built in. This helps monitor a completely independent endpoint solution (no reliance on the Windows registry or built-in services) to ensure the agent is healthy, provides the ability to fix broken agents without the need to put hands on the machine, and even the ability to collect performance data (procmon) also without placing hands physically on the machine.



THIRD-PARTY TESTING

How does Windows Defender compare directly to Deep Instinct? Unit 221B conducted third-party testing to determine the efficacy of the products. Their baseline machine was a fully updated and patched version of Windows 10 with Defender to mimic a real-life scenario if an enterprise was under attack.

THE TEST

- 100 diverse samples of malware
- 65 of the samples had detections by other vendors, while 35 were undetected by others
- File could not be corrupt
- File size under 1MB (to ensure file was not ignored based on size limitations)

RESULTS

SYSTEM A - WINDOWS 10 w/out DEEP INSTINCT

- Windows Defender automatically deleted 5 files
- Windows Defender automatically prevented 0 attacks on attempted execution
- 6,677 security events logged on the machine

SYSTEM B - WINDOWS 10 with DEEP INSTINCT

- Deep Instinct automatically deleted 68 files
- Deep Instinct automatically prevented 32 attacks upon attempted execution
- 4,030 security events logged

deep instinct™

Deep Instinct prevented the file from being extracted in 68 of the 100 files. The remaining 32 files were prevented on attempted execution.

Defender prevented 5 files, while 95 were not prevented nor terminated by Defender.

Deep Instinct also generated 2,647 less security events than the Defender-only machine. This means that 2,647 false positives/events not needing attention did not appear causing unnecessary panic/alert fatigue/remediation action.

DEEP INSTINCT HIGHLIGHTS

100% UNKNOWN ATTACKS PREVENTED

96.4% CUSTOMIZED ATTACKS PREVENTED

99.8% TOTAL EFFICACY

Testing conducted by
Unit 221B

FURTHER TESTING

Parallel third-party testing doesn't exist for Defender, so we conducted efficacy testing with a machine running Defender and a popular EDR, and a machine running Deep Instinct and LimaCharlie.

1 Defender had all settings enabled (Real-Time protection, Cloud-based protection, Tamper protection), and Deep Instinct carried BLOKWORX standard MAED policy.

2 We ran a powershell designed to pull components into memory and compile/execute a payload (Agent Tesla) which is a RAT (remote access trojan).

3 Defender did not pick up on the attack and did not alert on it. The EDR also had no idea the file(s) existed on the machine, nor that a trojan was actively running on the device.

4 Deep Instinct prevented the attack before the files could compile or attempt to write to the machine, successfully preventing a foothold with built-in persistence.

CONCLUSION

In summary, we cannot in any way suggest that EDR+Windows Defender is comparable to the level of security you receive with LimaCharlie + Deep Instinct (the solution provided and supported by BLOKWORX).

In short, they operate in completely different realms - one is prevention-based and one is detection-based. Are cost savings really going to be justifiable in the event of a critical incident? You'll have to make that decision, but we're proud to say our stack prevents events other solution miss, as evidenced by rigorous data and testing, reported here.