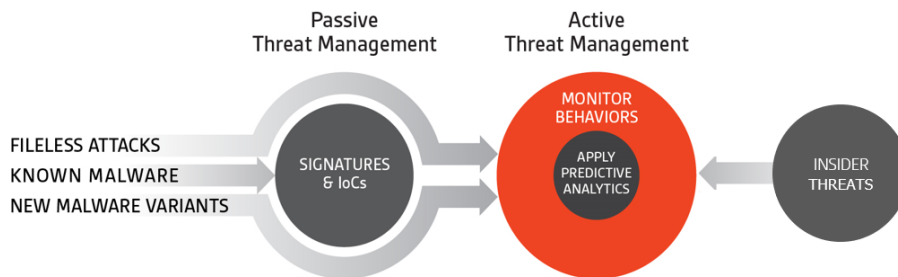


Security Brief

The Evolution of Threat Detection Technologies

Digital DNA is an in-memory threat detection technology introduced by CounterTack in 2009 and patented in 2014. It is the only in-memory detection technology available for endpoint security solutions. Digital DNA is in high demand and licensed by leading security vendors including Symantec, Rapid7 and Digital Guardian.



The New Normal

Endpoint security solutions like AV and Next Gen AV are important components of any security strategy. However, they are Passive Threat Management solutions. They scan files on disk against Signatures and Machine Learning models to detect and prevent malware attacks. Their vendors are engaged in a never ending game of cat and mouse with cybercriminals who continuously devise new malware variants to penetrate these solutions. AV and Next Gen AV do not capture fileless attacks.

In the new normal, Security Teams, both large and small, need to incorporate Proactive Threat Management into their security strategies. They need to look to new detection and response solution based on dynamic behavior monitoring and predictive analytics..

Digital DNA—The Cornerstone of Predictive EDR

Digital DNA is the cornerstone of CounterTack's Predictive EPP solution. It is the most reliable technology for detecting new malware and fileless attacks. It enables CounterTack Predictive EPP to detect the most threats, without relying on signatures or IoCs. Digital DNA provides the insight behind accurate and actionable predictive analytics.

AV and NextGen AV are passive threat management solutions

They are ineffective at detecting new malware variants and fileless attacks.

Security teams need to incorporate Proactive Threat Management into their security strategies

The Evolution of Threat Detection Technologies



What You Need At a Glance:

- Antivirus scan for malicious files using Signatures
- Next Gen Antivirus adds machine learning to scan for malicious files.
- Legacy EDR solutions rely on threat intelligence (IoCs)
- Signatures, machine learning and IoCs are static technologies
- They are ineffective at detecting new malware variants and fileless attacks

Antivirus. Antivirus scans for malicious files using Signatures. However, hackers understand Antivirus techniques and continuously create new variants to bypass them. Antivirus vendors struggle to keep up. Antivirus is still relevant because it catches around 60% of today’s malware. It is ineffective at catching 49% of today’s threats – fileless attacks.

Next Gen Antivirus. Next Gen Antivirus extends threat coverage with machine learning. Vendors continuously analyze malware samples and build models that scan and parse files, and then match features to detect new malware. Next Gen AV needs to keep machine learning models up-to-date. It doesn’t detect fileless attacks.

Application Containerization. Application containerization is a limited solution for browsers or applications like MS Office. It monitors applications in a sandbox. If it detects a malicious event it will remediate it. It works off of signatures and white listing. Application containerization effectivity is limited to what’s going on in the sandbox.

Threat Intelligence. Threat intelligence is the staple of legacy EDR solutions that rely primarily on Incidents of Compromise (IoCs). IoCs are Signature-like. They look at OS events, filenames, CnC hosts and more to extrapolate a pattern indicating malicious activity. IoCs need to be continuously updated to be effective.

Signatures, Machine Learning and IoCs are static technologies. The endpoint solutions that rely on them are engaged in a never ending game of cat and mouse to keep pace with today’s threats. They are ineffective at detecting new malware variants and fileless threats. They are post-breach solutions. They can’t discover threats until they carry out their behaviors.

Behavior-based. Many EDR solutions claim to be behavior-based. True behavior-based solutions look for techniques that hackers use to carry out attacks. They look at processes, network connections, file and registry changes, and the pattern of those activities. Behavior-based solutions are effective because they don't look at files or rely on threat intelligence.

In-Memory Threat Detection. Advanced EDR solutions are evolving to predictive threat detection. Malware must run in memory to carry out an attack. In-memory threat detection looks at processes running in-memory and reverse engineers them to identify malicious behaviors and predicting what the attack is trying to do. It is the most reliable technology for detecting new malware, fileless and insider attacks.



CounterTack Predictive EDR is the only endpoint solution featuring in-memory threat detection – Digital DNA. With Digital DNA it **detects** suspicious behavior that other threat detection technologies can't. It is the only solution that **predicts** what these behaviors can do. Digital DNA provide the visibility Security Teams need to adopt more agile and proactive threat management strategies to **prevent** attacks.

What You Need At a Glance:

- Behavior-based detection looks at processes, n/w connections, file and registry changes, and more
- In-Memory Threat Detection looks at processes running in memory
- The most reliable technology for detecting new malware, fileless and insider attacks
- CounterTack Predictive EDR is the only endpoint solution featuring in-memory threat detection
- It detects the most threats, predicts what they can do, and enables prevention of advanced attacks.

100 Fifth Avenue
Waltham, MA 02451-1208
855.893.5428
www.countertack.com

800 Rene-Levesque Blvd W,
Suite 1860
Montreal, Quebec H3B 1X9
514.287.7427
www.gosecure.ca