SOLUTION BRIEF

ENDPOINT VS. SERVER WORKLOAD SECURITY

EDR/EPP Security Tools Cannot Protect Servers and Application Workloads

EDR/EPP tools provide important protections for enterprise endpoints. But it is important to note that they are designed to protect only what they're named after – endpoints. Using attack signatures, behavioral analysis and AI/ML data analytics, they monitor user endpoints in real time and watch for malicious activity. Endpoints include devices such as laptops, smart phones, hand-held tablets and PCs, as well as devices like routers and modems.

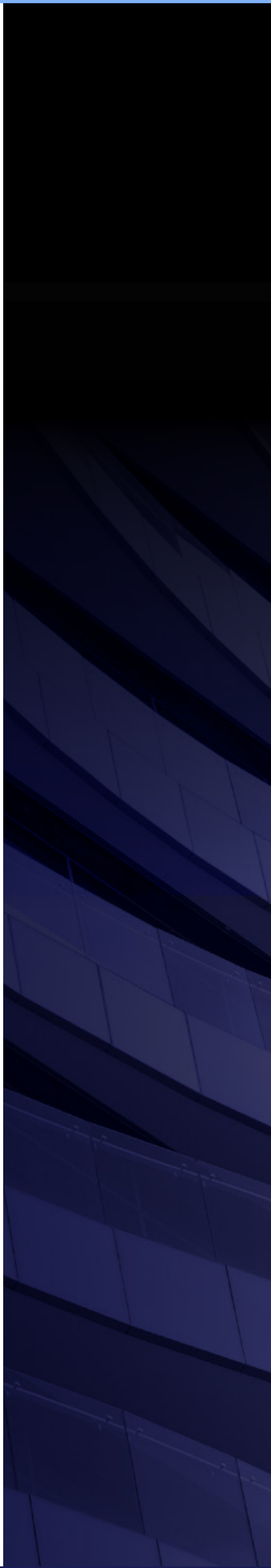
When enterprises try to rely on EDR/EPP solutions deeper inside their networks where their critical application and server workloads reside, the results have been poor. Attackers are well aware of endpoint security limitations, which is why they favor applications and server workloads as a primary focus.

70 Percent of Attacks Target Server Workloads

Verizon's annual Data Breach Investigation's Report (DBIR) highlighted this significant threat in their annual report, noting 70 percent of attacks target server workloads.

Server workloads and applications are more connected and have a far greater attack surface than endpoints. The expanded attack surface increases risk beyond what physical data centers and servers used to pose. Businesses with hybrid cloud operations carry additional responsibility of protecting virtual servers, containers and cloud workloads.

When it comes to applications in these environments, endpoint tools cannot distinguish normal functions from abnormal ones. They cannot look at application behavior or analyze tool files, programs and processes running in memory.



Lack of EDR/EPP Visibility Into Applications Is a Fatal Flaw

The complex technology required for gaining visibility inside applications and server functions was never meant to be part of EDR/EPP solutions core design. Enterprises in general and EDR/EPP tools specifically lack visibility into all of these areas, which presents vulnerable blind spots primed for attack.

This fatal flaw of application blindness is pervasive. All vendor varieties of EDR/EPP tools missed the infamous SolarWinds attack that went on for over a year. It's a classic case of the wrong tool for a critical job.

Remote code execution (RCE) exploits – like that which targeted the SolarWinds infrastructure – and other application-targeting techniques don't exhibit the patterns that endpoint tool signatures, artificial intelligence and machine learning abilities are looking for. Advanced RCE attacks will continue and numerous common applications, from email applications to authentication systems to performance tools, remain vulnerable.

Five Reasons EDR /EPP Solutions Cannot Protect Application Workloads

There are five key areas where EDR and EPP technology isn't suited to analyze behavior in applications, on servers or processes that occur during runtime.

1

Applications on Server/ Workloads are fundamentally different than those running on devices.

Applications running on your servers and workloads and those running on devices and laptops are fundamentally different. Users, purposes and performance requirements for these applications are also different and therefore require different means of protection.

2

Exploits targeting servers and workloads are also f undamentally different.

Given the above, it stands to reason that attackers would use different methods in going after applications and workloads. Their methods are stealthier and have no trouble getting by endpoint tools – i.e., the same tools designed to protect endpoints are not equipped to handle exploits that target applications and workloads.

3

The blacklisting model is old and doesn't scale.

Blacklisting has been around for a long time but it's become obsolete because it can no longer keep up with today's threats. In the infinite universe of potential malware, finding everything bad and blocking it before an attack happens is not realistically possible. It's an approach that by definition always runs behind current threats.

4

Reactive security models always fall behind.

Most security tools operate in reactive mode. When EDR tools see something suspicious, they might run some algorithms to try to analyze the activity. If external analysis determines that the activity is bad, the hope is next time the tools will be able to stop it. But that is too slow for organizations. It puts them always in reactive mode – too little, too late. Aware they are always being tracked, attackers are constantly morphing and changing their techniques to escape detection.

5

Advanced exploits today bypass EDR security tools.

All of these areas together demonstrate the ways in which EDR solutions cannot protect applications and systems from the kinds of obfuscated code used in advanced attacks. The failure to address this risk can be catastrophic, as we recently saw in the December 2020 SolarWinds attack.

Virsec Security Platform Blocks Attacks That EDR/EPP Tools Miss

Virsec stops attacks at multiple critical stages of the kill chain, preventing downstream damage.

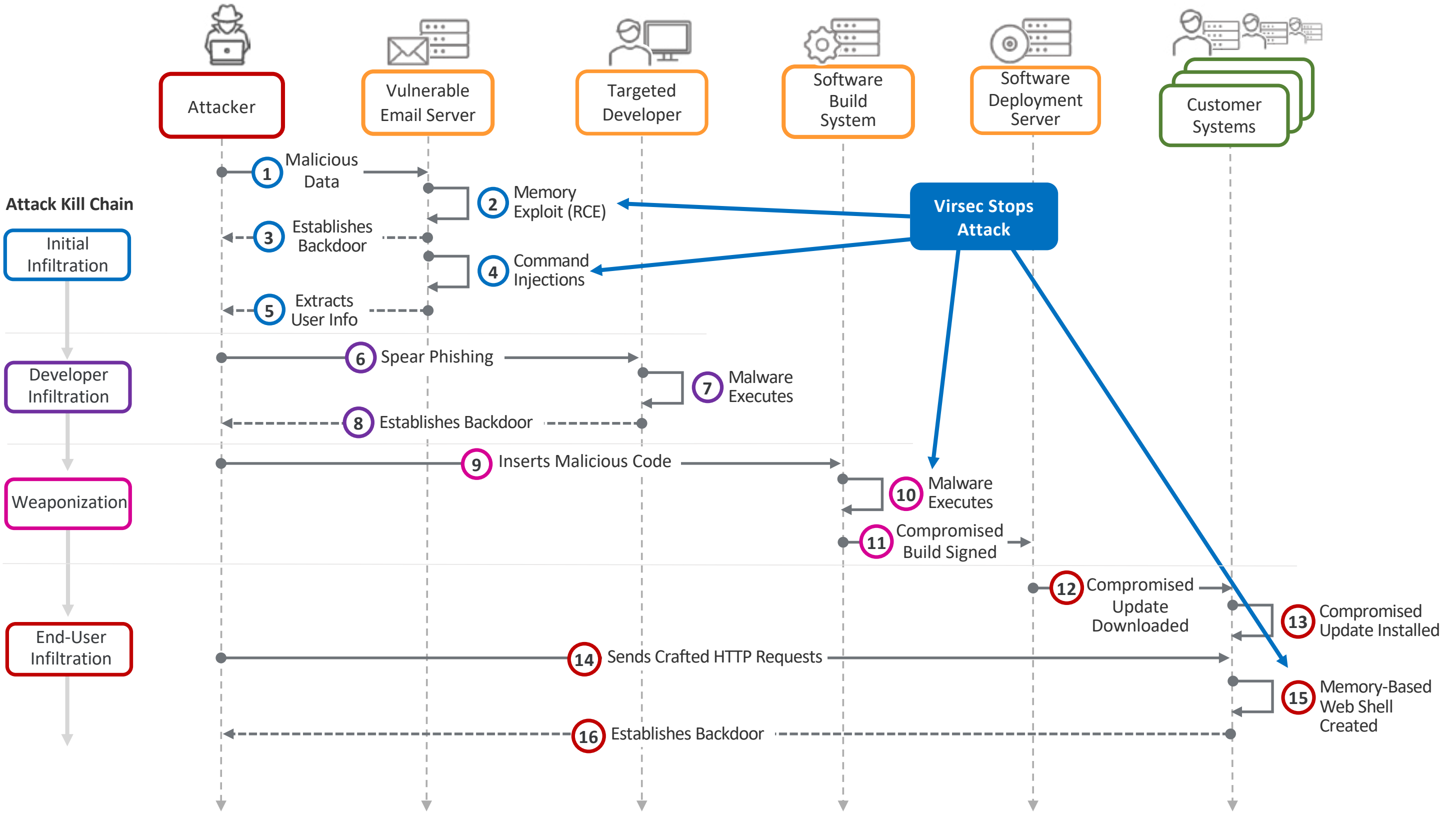


Figure 1: Multiple infiltration steps where Virsec stops advanced attacks

The Virsec Security Platform (VSP) provides a far more effective, accurate and practical approach to protecting server workloads and applications than EDR technology are equipped to provide. Unlike solutions that rely on heuristics or behavioral rules to detect attacks, VSP uses a deterministic, code-based approach to detect and protect against these types of advanced cyberattacks, with no signatures, no tuning and no noise.

“Do not use an offering designed to protect end-user endpoints and expect it to provide adequate protection for server workloads.”

Neil Macdonald, Gartner

Virsec AppMapp® Technology

Virsec's patented AppMap® technology maps acceptable files, processes, libraries, web input, memory usage, control flow and more. The Virsec Security Platform monitors actual code execution, instantly detecting and stopping any deviations from normal, and preventing attacks at the first step before damage occurs.

Rather than trying to blacklist everything that is possibly bad or focus on system behavior that can change and evolve, Virsec enforces what is good and allowable. This ensures that applications never get derailed, regardless of threats, vulnerabilities, or patch status. Trying to chase after an infinite number of malicious actions is an impossible task that only becomes more unachievable every day.

Virsec leverages three highly differentiated and deterministic approaches:

Control Flow Integrity (CFI)

protects pre-compiled code used in application servers and frameworks as well as runtime libraries

Byte Code Instrumentation (BCI)

protects interpreted code used by the business-logic in web-based applications

Centralized Application Control Repository (CACR)

allows only known developer-provided executables and libraries to run and blocks execution of unknown file-based or fileless malware

Advanced Protection for Advanced Attacks

Today's security battleground has shifted to application workloads, and organizations need full runtime visibility and protection – down to the memory, host and web layers. Traditional security tools, such as endpoint security, should still be used to guard the perimeter. But it is important to realize their significant limitations.

The Virsec Security Platform protects from within and provides a far more effective, accurate and practical approach to protecting server workloads and applications than EDR technology. Rather than rely on heuristics or behavioral rules to detect attacks, Virsec uses a deterministic, code-based approach to detect and protect against advanced cyberattacks and does not generate false positives.

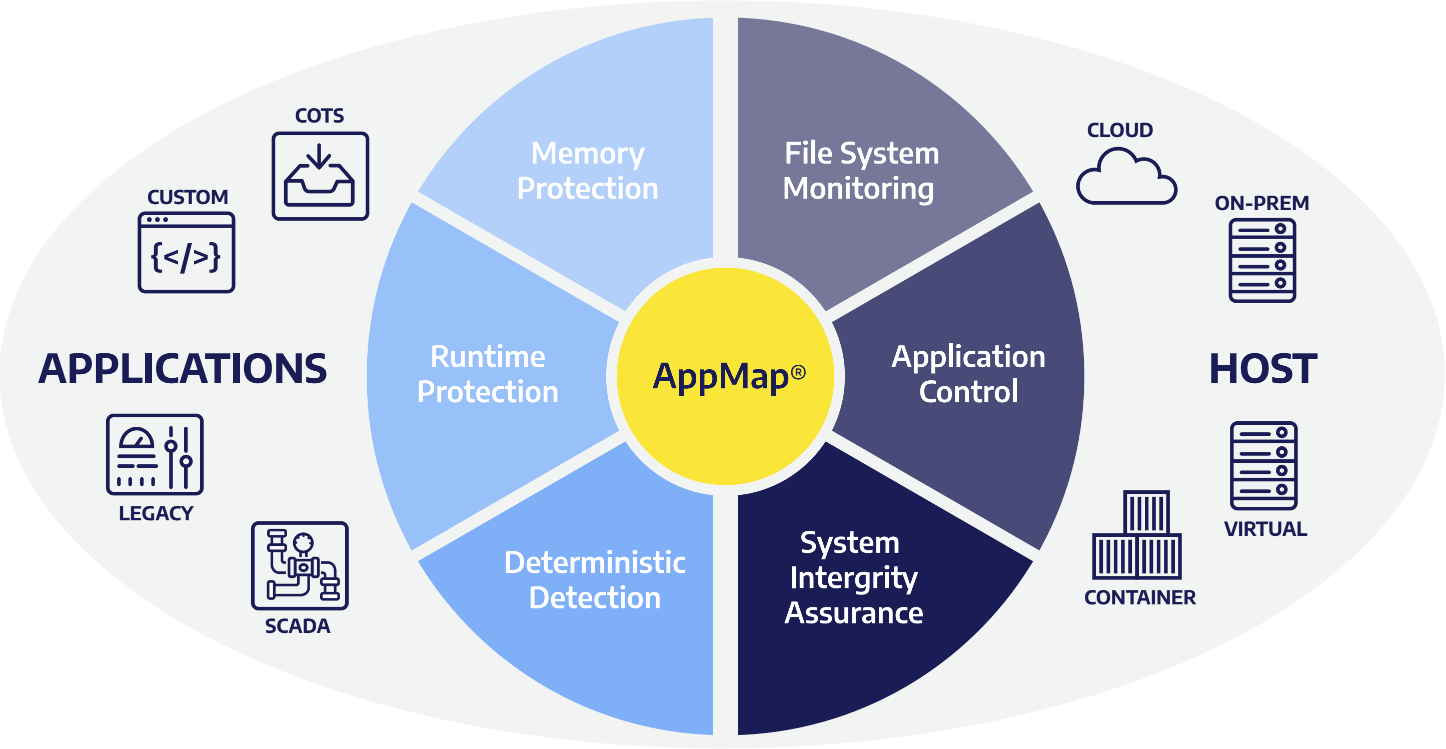
Virsec provides unique application-aware protection at runtime, defending all applications, on any platform, in any environment.

Application-Aware Workload Protection

Virsec provides application-aware workload protection against the widest range of evasive cyberattacks – known and unknown – and secures applications from the inside. Virsec protects all your applications, including custom, COTS, third-party, legacy, SCADA and more. And the Virsec solution protects across any platform, including on-prem servers, virtual, cloud, hybrid, container, and edge.

ANYWHERE	ANYTHING	ANYTIME
On-prem, public/private cloud, hybrid, container	*Custom, legacy, COTS and air gapped applications*	*Deploys in minutes, protects continuously in real-time*

> *"Do not use an offering designed to protect end-user endpoints and expect it to provide adequate protection for server workloads."* Gartner



Server & Application Workload Protection

Application-Aware Mapping Technology

No Signatures, No Tuning, No Noise

Zero Dwell Time

Full-Stack Runtime Protection

Securing the World’s Most Critical Applications

Virsec is deployed globally protecting mission-critical applications and infrastructure in industries including financial services, healthcare, government, defense, power, oil & gas, transportation, telco, technology, and more.

Recognition

Cyber Catalyst

CRN

Cyber Defense Global Awards · Cyber Defense Magazine 2019 Winner · Cutting Edge Digital Footprint Security

Gartner

Cyber Security Excellence Awards · Winner 2020

MITRE

Info Security Products Guide 2020 Global Excellence Gold ★★★★★

Ovum

Partners & Customers

Tech Mahindra

NCUA

Raytheon Technologies

Godrej

Schneider Electric

YOTTA

du

AVEVA

BROADCOM

inspirage

etisalat

GDIT

• 226 Airport Parkway, San Jose, CA 95110 • VIRSEC.COM

VIRSEC