SOLUTION BRIEF

Supply Chain Protection

Increasingly Vulnerable Software Supply Chains

NIST, DHS, DoD and the GSA have declared software supply chain vulnerabilities to be a substantial cybersecurity threat. For validation, look no further than the devastating SolarWinds attack that has impacted thousands of organizations.

Software development has become increasingly complex and automated, increasing dependence on vulnerable 3rd-party components. Attacks that execute at the memory level often go unnoticed, corrupting critical resources, tampering with composite elements, binaries, configuration files, and injecting libraries, or altering data files. Vendors can take months to identify and remediate known vulnerabilities, if they do at all.

Security gaps and flaws throughout the software Bill-of-Materials (SBOM) used in application production and within the related assembly and distribution processes provide bad actors with pathways to easily exploit critical applications, systems, and web services.

Software Supply Chain Attacks

A software supply chain attack occurs when a compromised 3rd-party application or software is distributed and deployed on production servers, where seemingly benign – but entirely malicious – code activates to setup backdoors, change registries, leverage trusted files and execute dangerous exploits.

Existing security tools are not sufficient to secure the supply chain, namely because the most sophisticated attacks are occurring at runtime, a notorious blind spot in organizations. Conventional tools are not instrumented to detect exploits in memory and do not provide any visibility into runtime.

VIRSEC

"Virsec understands what's happening to applications at runtime, making them self-defending against any vulnerabilities."

Sona Srinivasan
Enterprise Architect
Cisco

"Virsec virtually patches vulnerabilities in runtime memory, so nobody can exploit them."

Paul Forney
Chief Security Architect
Schneider Electric

"Virsec monitors how code executes at the lowest level and instantly detects when an adversary is trying to make it do something bad."

Michael Daly
CTO for Cybersecurity
Raytheon

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

Runtime Protection: The Missing Link

The industry has defined network security and segmentation, behavioral analysis, and monitoring IOC and user activity logs as table stakes for supply chain protection. However, these tools require a baseline, prior knowledge, and expert monitoring, and do not protect against exploits that execute at runtime. The infamous SolarWinds attack is a prime example of a remote code execution attack that occurred in runtime and went undetected for months.

If an organization only has these conventional security tools installed, it will remain vulnerable to attacks that execute at runtime, such as remote code execution exploits. The critical missing link for effective security is runtime protection. Evasive attacks that proliferate at the memory level often go undetected for days, months, or even years. Without runtime protection, organizations remain exposed and susceptible to attack.

The Virsec solution prevents the execution of corrupted software and ensures continuous runtime visibility. Virsec's advanced memory and host protection defends against the most dangerous vulnerabilities identified by MITRE and stops evasive attacks that stem from compromised applications.

Maintain Integrity

Ensure applications execute only as intended – even when compromised

Identify & Disarm Threats

Distinguish malware embedded in software packages before damage is done

Prevent Attack Spread

Monitor runtime and prevent exploits and lateral motion without requiring traffic rules, filters or investigation

Gain Deeper Visibility

Continuous awareness and visibility across each application within memory

Minimize Future Risk

Leverage controls designed to stop unknown attacks originating in 3rd-party applications and binaries

Stop Remote Code Execution Attacks During Runtime

A remote code execution attack happens when an outside agent is able to exploit a network vulnerability to remotely access and manipulate a targeted system, like what happened with the disastrous SolarWinds attack. The exploit executes at runtime, often going undetected for an untold length of time, leaving organizations exposed, weak and hemorrhaging information.

Virsec ensures application integrity at the file level with application-aware control and file integrity monitoring, providing true runtime protection. Patented AppMap® technology maps acceptable files, processes, libraries, web input, memory usage, control flow and more. Virsec instantly detects and stops any deviations, preventing attacks at the first step before damage occurs.

Virsec defines legitimate application processes, distinguishing which libraries should get loaded whenever valid processes spawn. Virsec immediately detects and stops library injections or code that is not part of an executable or any of its dependent libraries. If tampering is detected, Virsec instantly takes precise protection actions, such as un-injecting the illicit library.

Virsec delivers unmatched visibility, control, and protection, enabling organizations to reduce the time and resources needed to meet software supply chain compliance requirements, ensuring comprehensive software supply chain protection from development to runtime.

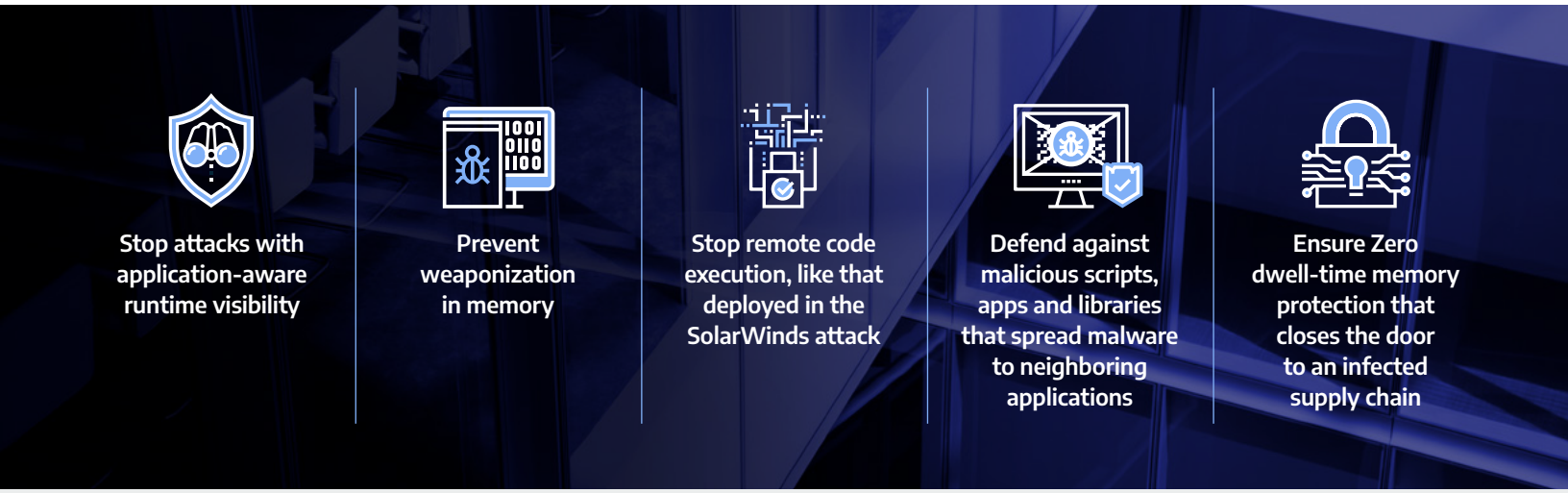
VIRSEC

Comprehensive Supply Chain Protection

The Virsec solution is uniquely instrumented to protect organizations from sophisticated supply chain attacks that use evasive memory exploits and application runtime, such as remote code execution exploits, without the need to isolate or unplug until patches are available.

Virsec solution automatically counters attacks affecting files and file systems, generating an immediate and accurate response that prevents critical assets from being altered, seized, replaced, or erased. It prevents the misuse of trusted libraries, registries, core processes and memory used to initiate lateral movement, services disruption and system breaches.

Virsec identifies and disarms attacks with unmatched accuracy. The technology is based on application-awareness that does not require timely learning, analysis of intelligence gathering and IOC, or investigations by qualified professionals.



Guard Critical Software Inventories

Virsec ensures the integrity of critical application components by:

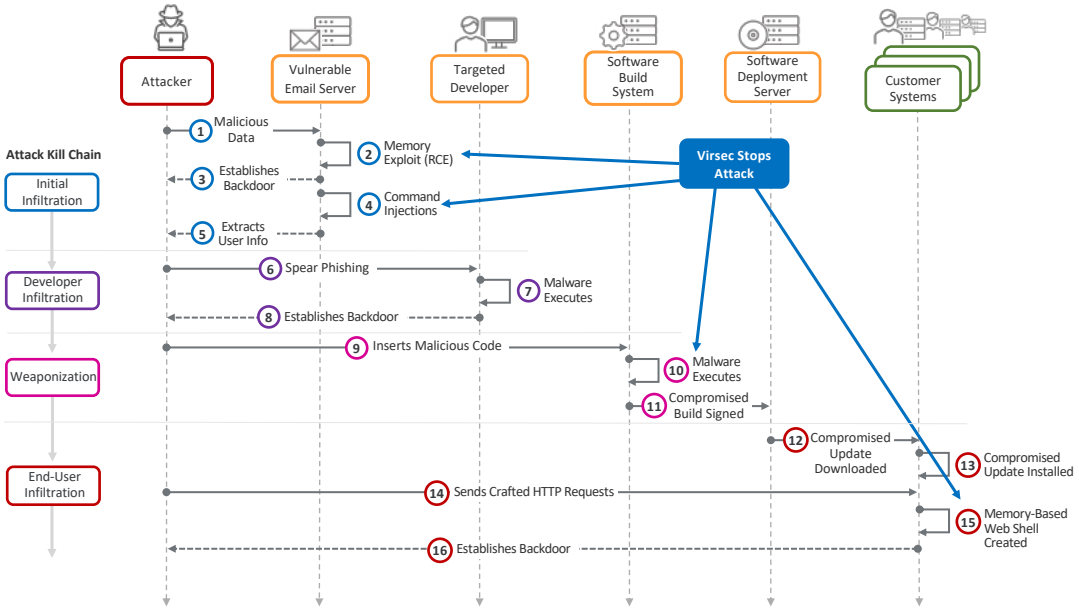
- Profiling and mapping information about each relevant file, executable, library and process from point of origin
- Continuously monitoring whether files and directories have been tampered with or corrupted during runtime
- Tracking all activity on specified files, directories, executables, scripts, configuration files, content files, and logs used within the application instance

Workloads Are the New Attack Surface

The attack surface has moved to the workloads. And wherever they reside – whether in the cloud, containers, on servers or hybrid environments – security solutions must include system assurance, application control and memory protection to ensure application-aware workload protection.

Existing security tools used to secure the supply chain are costly and time consuming, but most importantly, they are not sufficient to adequately protect against supply chain attacks. A more fundamental problem with these tools is that they are not application aware. They are unable to reliably distinguish between normal application operations and malicious operations of malware, which turns threat response into a blind guessing game.

Code that executes during runtime can be almost undetectable, and due to the pervasive and prolific nature of malicious code, organizations should assume that their networks have already been compromised. However, declaring an attack too early can significantly disrupt business operations, but performing lengthy in-depth analysis and investigation gives infiltrators plenty of time to collect their loot, cover their tracks and disappear.



Protect Legacy Applications

Almost every organization operates with a combination of applications – from COTS to custom to legacy. Unfortunately, as applications age, they become more vulnerable and require ongoing maintenance, updates and patches.

The Virsec solution protects legacy applications by identifying illicit modifications at the operating system (OS) kernel level the moment they occur – even without installed software updates. Virsec instantly identifies any deviation from a pre-determined "normal," preemptively patching systems until updates are installed.

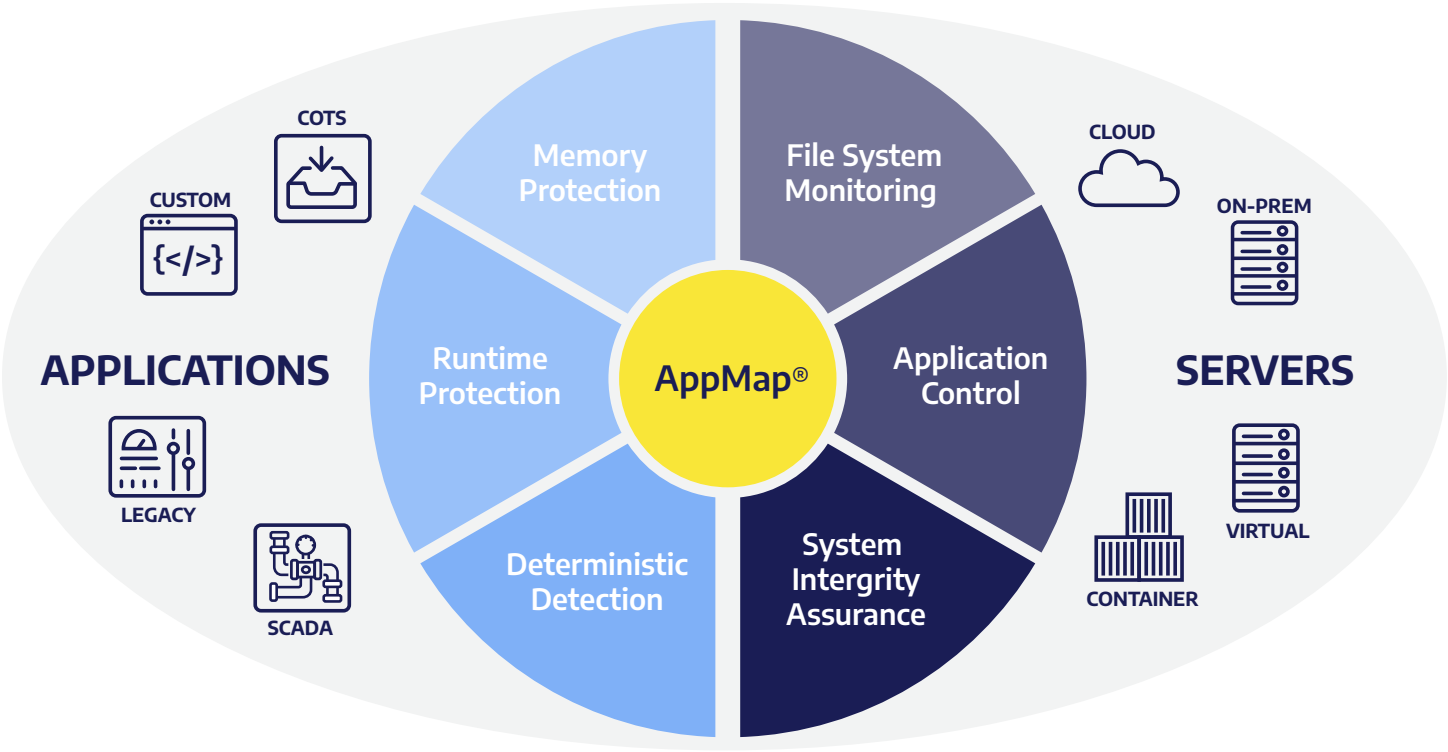
Virsec eliminates the risk posed by disclosed or undisclosed vulnerabilities being exploited during lengthy patching cycles. By mapping and monitoring actual code execution, the Virsec solution instantly identifies when an application is about to be targeted and stops attacks in their tracks. Virsec ensures precise Compensating Security Controls that eliminate the risks of vulnerabilities being used to abuse web applications, third-party code, and legacy systems.

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.

"Virsec virtually patches vulnerabilities in runtime, so nobody can exploit them."

Chief Security Architect, Schneider Electric

Recognition

Cyber Catalyst · CRN · Cyber Defense Magazine Global Awards 2019 Winner · Gartner · Cyber Security Excellence Awards Winner 2020 · MITRE · Info Security Products Guide 2020 Global Excellence Gold · Ovum

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

VIRSEC