SOLUTION BRIEF

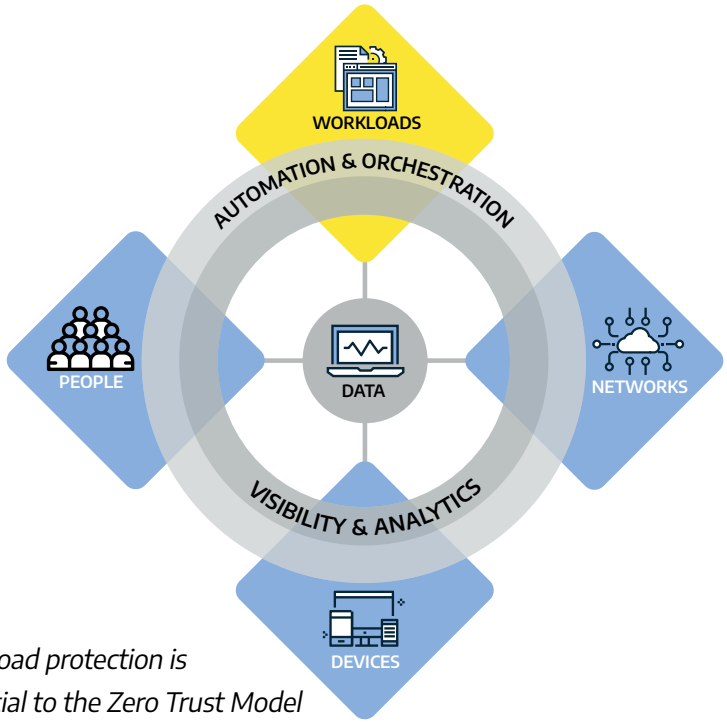
VIRSEC ZERO TRUST WORKLOAD PROTECTION

Essential Security to Stop Supply Chain Attacks

The Virsec Security Platform is the first solution to extend Zero Trust deep into the workload, guard-railing critical workloads during runtime. Virsec implements a zero trust model to effectively stop complex supply chain attacks at multiple stages.

Forrester's Zero Trust Maturity Model and Gartner's Cloud Workload Protection Guide both emphasize that the ability to secure workloads is a critical requirement for zero trust security.

Virsec secures workloads on-premises and in the cloud or containers, enabling protection to follow the workload across hybrid and disaggregated environments where zero trust is most urgently needed.



Workload protection is essential to the Zero Trust Model

VIRSEC

"When we deployed the Virsec platform, we experienced an immediate ROI, and a clear view into our entire application attack surface. Now, we have visibility and control over how our application code executes during runtime and identifies malicious behavior. This awareness is especially true for zero-day attacks, which Virsec can detect without any prior knowledge."

Principal for Cybersecurity
Broadcom

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

Enterprise Architect
Cisco

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

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."

CTO for Cybersecurity
Raytheon

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

Critical Context for Zero Trust

In a typical cyberattack, the bad actor sends maliciously crafted data that a vulnerable application unwittingly turns into code. Once this code executes, the attacker gains persistent control of the workload and can then cause arbitrary code to execute on the workload. Clearly an application workload should not blindly trust any data. Instead, it must ensure there is no attempt to slip in malicious code.

Virsec AppMapp® technology addresses the trust deficit in a vulnerable application and can readily detect, in real time, when an attacker attempts to gain control of the workload.

Because Virsec delivers workload protection with full automation at millisecond speed, it serves as an essential compensating control for vulnerabilities in runtime code – that would otherwise undermine the zero trust prerequisite for fully patched code.

As an application-aware workload protection solution, the Virsec Security Platform completes zero trust implementations by providing explicit verification that code is executing as intended, and any attempt to deviate from legitimate control flow is immediately recognized as a breach.

Coupled with monitoring and strict verification of underlying file system integrity, Virsec Zero Trust:

- Extends Software Bill of Materials (SBOM) trust by digesting, extracting, and enforcing code integrity during the Operate and Monitor lifecycle stages.
- Provides clear detection triggers instead of needle-in-haystack approaches that often misses clever supply chain attacks like SolarWinds.
- Automatically triggers protection response with highly actionable, contextual attack forensics.
- Serves as a Compensating Control for vulnerabilities in 1st party code.

Virsec's auto-deployment and topology extraction capabilities gives visibility at all software layers delivering **continuous compliance monitoring** that evaluates risk from vulnerabilities daily, rather than just one point in time.

Virsec Application-Aware Security

- Foundational Controls
- Only provides on-time analysis
- Focuses on hardening OS & frameworks

- EDR tools analyze after-the-fact
- Requires threat feeds, IOCs, cannot catch emerging threats

Zero Trust Workload Protection & Supply Chain Attacks

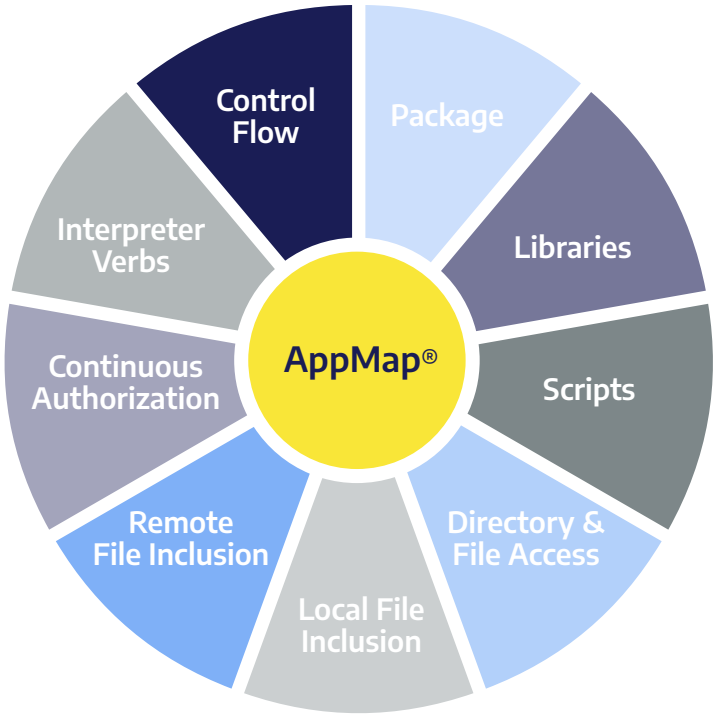
The recent attacks leveraging the SolarWinds supply chain exposed significant flaws in how conventional security tools defend against advanced malware.

Visibility Is Essential to Zero Trust

Software infrastructure incorporates hundreds of services, including authentication, authorization, DNS, email, and NTP. Each is vulnerable to supply chain attacks.

The choice for operators is to either wait for legacy indicators of compromise or threat feeds after the fact. Virsec provides the ability to use a workload-aware solution that is fully independent and executes at runtime.

Current evidence suggests that SolarWinds attack was initiated in September 2019, but indicators of compromise were not discovered until December 2020. The damage from sustained exposure is almost incalculable.



Workloads Are the New Attack Surface

The workload is the first and primary target entry point for attackers and it must be protected with the highest priority. What does it mean to be a workload-aware solution?

Workload protection must include system assurance, application control and memory protection. Code that executes during runtime can be almost undetectable, and the traditional blacklisting approach cannot possibly detect all the malware that is generated each day.

Virsec AppMap® technology works in runtime memory to give deeper insight and awareness, essential for zero trust protection. Without this visibility the workload component is simply a black box, subject to 15+ months of attacker abuse, as happened in the SolarWinds attack. Arming the workloads to defend themselves is the best protection against the most sophisticated and evasive attacks.

VIRSEC

Protect Infrastructure from Remote Code Execution Vulnerabilities

Virsec's application-aware workload protection prevents web-facing workloads from being attacked, even when it is not possible to patch them continuously to remove vulnerabilities. Conventional implementation of zero trust requires that all code be fully patched at all times. But in reality, practical issues like lead time, resources (or lack thereof) and unknown vulnerabilities makes this unachievable.

Virsec's Zero Trust approach to code execution serves as a compensating control for both known and unknown vulnerabilities, bridging the patching gap to ensure that workloads remain fully secure at runtime.

RCE vulnerabilities can be disastrous because conventional security tools cannot detect attacks that generate attacker-influenced code directly in memory. Each week, hundreds of new RCE vulnerabilities are reported in the National Vulnerability Database (NVD), making it impractical to instantly patch these vulnerabilities or create signatures against all exploits.

The remote code execution attacks perpetrated on the end-users of SolarWinds advanced in two stages:

BACKDOOR DEPLOYMENT	LATERAL MOVEMENT
Malware delivered through SolarWinds updates opened back doors and allowed the attackers to persist in the victim enterprise and conduct malicious activities at will.	*Spread the malware to all "neighbors." The attackers also leveraged vulnerabilities in software workloads that enabled Remote Code Execution (RCE) to further exploit government and enterprise infrastructure.*

Protect Infrastructure from Corrupted Software Updates

The figure 1 diagram details the events in the SolarWinds attack and how the Virsec solution detects and stops it. The Virsec solution extends zero trust to server workloads, preventing them from executing unauthorized applications and scripts, as well as from loading unsigned and inappropriate libraries.

Even if these apps are legitimate on another server, Virsec provides zero trust compartmentalization and protection from lateral movement. Virsec effectively extends trust from point of deployment through the Operation and Monitor stages of the supply chain.

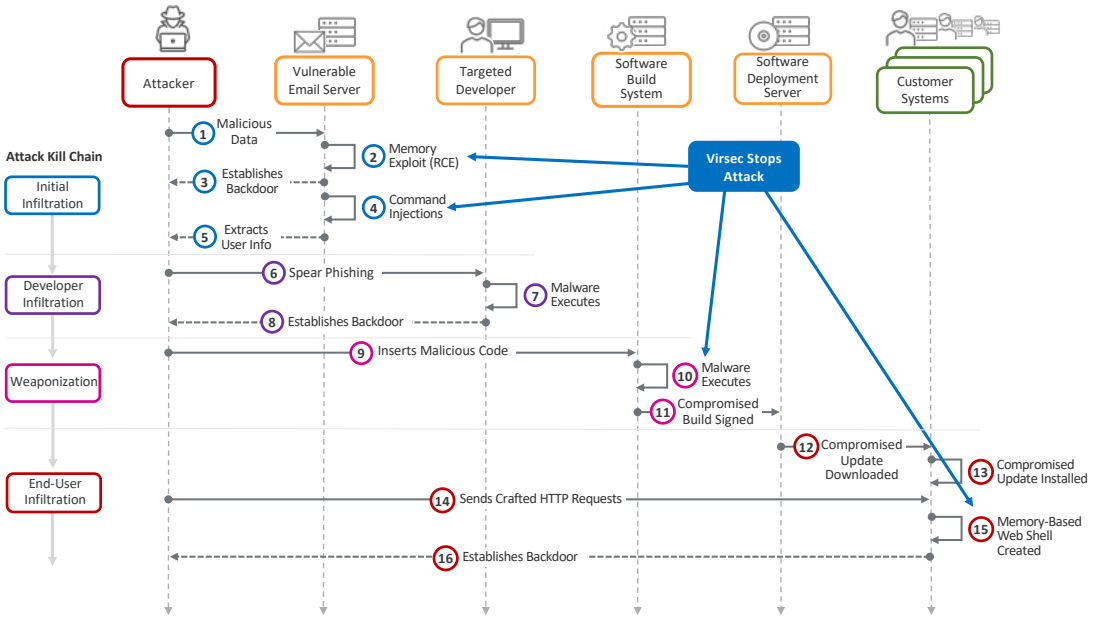


Figure 1: Virsec protection in the SolarWinds Supply Chain attacks

Virsec Security Platform

Virsec's workload protection controls are purpose-built to support Zero Trust maturity for protection against sophisticated supply chain attacks.

The Virsec Security Platform (VSP) patented technology is delivered via the following three application-aware components:

Achieve Zero Trust Workload Protection

The Virsec Security Platform provides Zero Trust throughout the software supply chain and workload operational lifecycle. Protect enterprises from sophisticated remote code execution or sophisticated supply chain attacks against on-premises, cloud, hybrid, or container-based workloads.

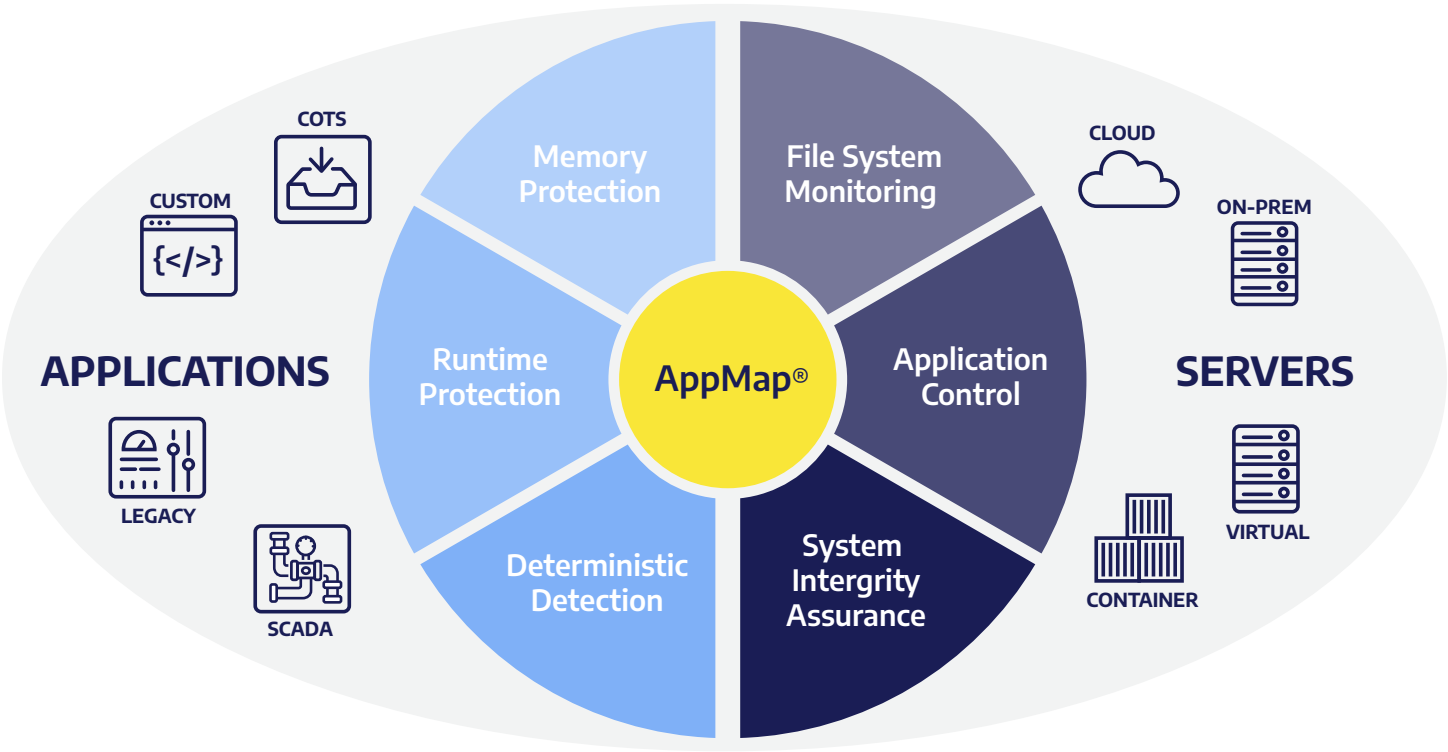
For more details, please visit www.virsec.com

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



VIRSEC

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

Partners & Customers