CLOSE THE GAPS FROM SUPPLY CHAIN POISONING WITH VIRSEC

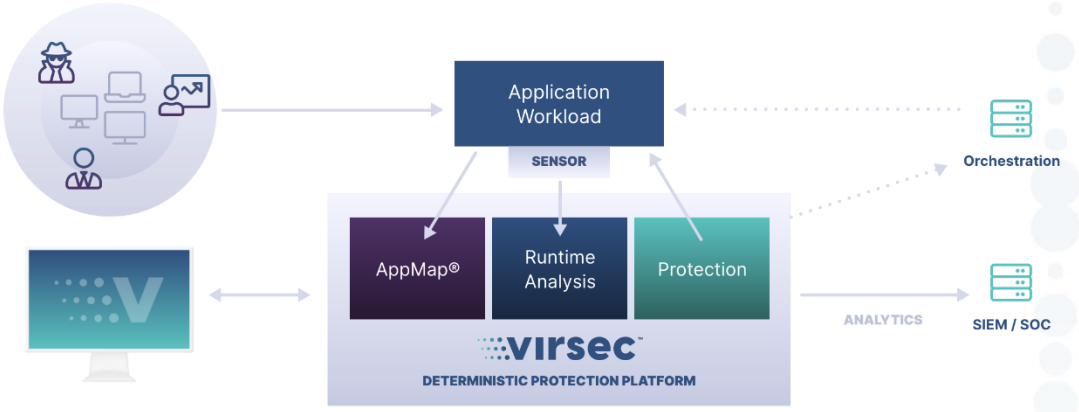
The world runs on software, yet, until now, there was never a way to achieve 100% protection of that software while it is running, wherever it is running. The only way to fully protect software is by fully mapping and understanding what it is supposed to do and immediately stopping what it is not. Virsec's Deterministic Protection Platform (DPP) eradicates software threats in real-time before they can cause any harm, making security response obsolete.

Software Supply Chain Attacks are Gaining Traction

Software supply chain attacks have been front and center in the minds of many IT security leaders within some of the world's largest organizations. Many organizations feel that they cannot do more to prevent these attack types, and they cannot afford this to continue as they place themselves at enormous risk and peril. Supply chains are particularly vulnerable because modern software is not written from scratch: instead, it involves many off-the-shelf components, such as third-party APIs, open-source code, and proprietary code from software vendors. If an application includes one compromised dependency component, the entire application is then vulnerable. Furthermore, every other application that uses that same component is also vulnerable, so the number of impacted software can grow exponentially.

Additionally, software is often reused. Therefore, a vulnerability in one application can live on beyond the original software's lifecycle. Software that lacks a large user community is particularly vulnerable because a large community is more likely to expose a vulnerability faster than a project with few followers. Supply chain attacks are on the rise because as enterprises have become better at hardening their environments, malicious attackers have turned to softer targets and have found more creative ways to make their efforts challenging to detect and most likely to bypass existing security controls. Below are some of the most prevalent types of supply chain attacks:

- Upstream attacks target a system that is "upstream" from users, such as through a malicious update, which then infects all the users "downstream" who download it. An example of this is what happened with the SolarWinds supply chain attack.
- Midstream attacks that target intermediary elements such as software development tools.
- Dependency confusion or hijacking attacks exploit private internally created software dependencies by registering a dependency with the same name but with a higher version number on a public repository. The false reliance is likely to be pulled into the software build instead of the developer's intended dependency. This is possible if a developer does not properly scope his software dependencies.
- Stolen SSL and code-signing certificate attacks compromise the private keys used to authenticate users of secure websites and cloud services.
- CI/CD infrastructure attacks introduce malware into the development automation infrastructure. An example of this is by cloning legitimate GitHub repositories.
- Open-source software attacks introduce code into builds that propagate downstream to those who use the open-source libraries.

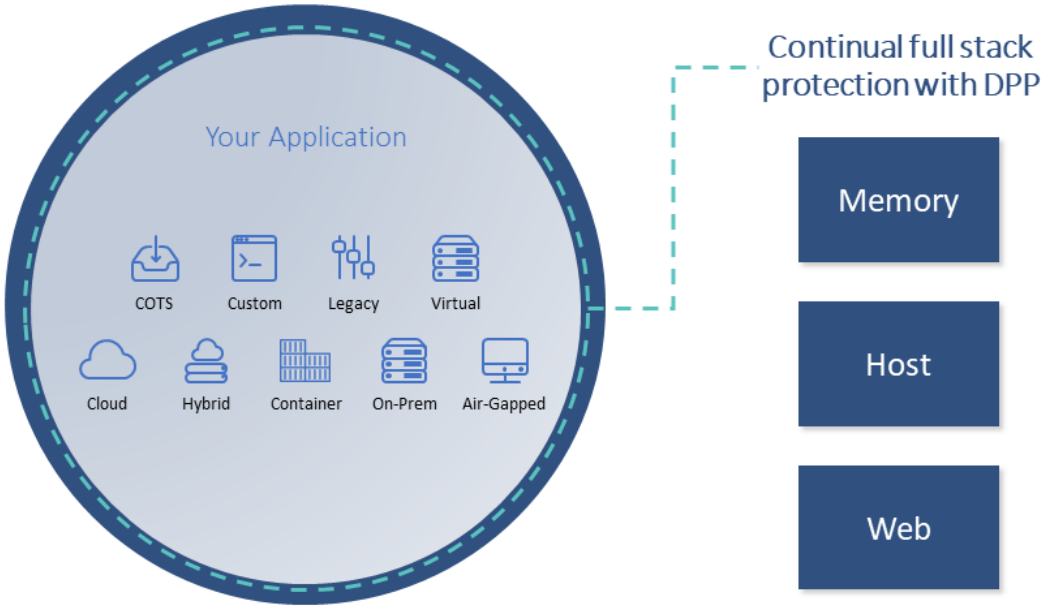


virsec

Prevent a Supply Chain Attack with Virsec Deterministic Protection Platform (DPP)

Supply chain attacks are increasingly becoming a business-critical issue impacting crucial relationships with partners and suppliers. Supply chain attacks are hard to detect. This is partly because even though a piece of software is validated, that doesn't mean that software is secure today. Organizations need to mitigate the supply chain risks that make them vulnerable to attacks. This requires employing effective protection solutions. The following are some recommendations for how organizations can increase their supply chain security and avoid becoming a victim:

- **Employ solutions that fully protect your software:** Virsec Deterministic Protection Platform (DPP) establishes a foundation for achieving complete application protection. It provides deep visibility and full-stack control across the runtime infrastructure with a deterministic approach to threat detection. It focuses on core application components, with real-time detection and protection actions that harden vulnerable software, assuring that your application only runs as it should and that no malicious code can ever execute.
- **Fully understand application execution:** With its deterministic approach, only trusted execution is enforced by DPP. DPP ensures zero adversary dwell time because DPP provides the complete contextual understanding of all software during runtime without triggering false positives and delays associated with human response.
- **Identify and Stop Attacks during Runtime:** Depending on security controls that rely on Indicators of Compromise (IOCs) alone is risky. It is essential to realize that any security control that needs a threat intelligence feed can only protect a system after the same attack has been discovered somewhere else. DPP optimizes runtime memory protection with out-of-box application behavior sequencing controls that detect even the most sophisticated defense evasion tactics. It stops these attacks in real-time, stopping malicious exploits before they can cause any damage to the victims' system.



Learn more| Click here for more information about workload protection with Virsec