Whitepaper

Virsec Security Platform (VSP)

Executive Summary

Virsec leverages patented Trusted Execution™ technology to protect high-value enterprise applications deployed in the data center, or in public and hybrid clouds, from highly sophisticated attacks including memory corruption, code injection, credential theft, supply chain and other sophisticated attacks. Virsec effectively creates and enforces guardrails around the application as it executes. These guardrails ensure that applications only execute as intended and restrain bad actors from corrupting memory as a precursor to hijacking control of the application and subsequent stealing or destroying high-value enterprise data.

Conventional cybersecurity tools are designed to extract markers from incoming network traffic as well as system calls made by the application. These runtime marker sequences are compared to known and catalogued attack techniques. When bad actors vary techniques beyond what has been previously catalogued, their attacks are highly likely to succeed. For most enterprises, it is a massive logistical challenge to constantly keep updating heuristic and behavioral signatures of deployed security solutions and to keep patching their applications as soon as possible or risk being attacked.

VSP breaks this logistic nightmare by monitoring applications instead of attack techniques. VSP's approach of creating application guardrails ensures that protected applications execute only what the developer and not the bad actor intended. This approach relieves enterprises from reactive patching. Even unpatched applications protected by VSP cannot be abused.

US-CERT tracks vulnerabilities in publicly available applications through its National Vulnerability Database (NVD). The single largest individual category of vulnerabilities are **buffer errors** (~15%) which results in attacker controlled machine code being directly executed thereby allowing attackers to take over servers and perform their malicious activity. In the last two years, the count for buffer error vulnerabilities in the NVD has shot up from ~750 to ~2,250 – a three-fold increase. The single largest group of vulnerabilities (~55%), in the NVD are **injection-style vulnerabilities** in interpreted code. These include SQL Injection, Cross-Site Script Injection, Command Injection, Code Injection etc. This group of vulnerabilities facilitate attacker controlled interpreted code being injected into memory. Later this attacker-controlled code is executed by downstream interpreters thereby allowing attackers to take over servers.

There is wisdom in the phrase "you cannot fix what you cannot see." Conventional security products treat the process memory of the application as a black box. Owing to this blind spot, they lack a reliable way of detecting or responding when application memory is corrupted or manipulated. VSP addresses these shortcomings by granularly monitoring the application's control flow, and contextually sanitizing user input for interpreter syntax.

VSP complements deep memory protection with additional capabilities including:

- Whitelisting server executables to control which ones can spawn a process. This prevents unknown executables such as traditional **file-based malware** from launching rogue processes.
- Monitoring script files targeted at legitimate interpreters like PowerShell and others from spawning processes using bad-actor controlled scripts thereby protecting against **fileless malware** attacks.
- Monitoring files for malicious alterations as they arrive through the supply chain.

VSP not only protects targeted applications against the most sophisticated vulnerabilities within milliseconds but it can also generate granular and highly correlated forensics and threat feeds. These in turn help with diagnostics, compliance and improving effectiveness of traditional signature-based security products already in place. Increased visibility from VSP forensics helps to eliminate the number of man-hours spent in chasing after the barrage of false positives generated by conventional cyber solutions like Web Application Firewalls (WAFs) and Host Based Intrusion Prevention (HIPS) solutions.

Virsec delivers this highly deterministic, timely and reliable security response even when patches are not yet available or not yet deployed. VSP does not require access to source code and leverages standards-based orchestration tools for large scale deployments.

Many of Virsec's customers view VSP as a compensating control that dramatically improves the enterprise's cyber-risk posture without costly and reactive intervention. With Virsec, enterprises no longer have to trade risk for business continuity.

Key Benefits

1. **Technology Advantage:** A key technological differentiator between Virsec Security Platform (VSP) and other application layer security solutions is:

    a. Conventional security tools focus on stopping known bad input, such as malformed data and files, by filtering through a knowledgebase consisting of signatures and heuristic rules further embellished by AI and ML. Despite these enhancements, these solutions often fail when presented with non-conventional data and file variants and techniques not already embodied in their knowledgebase.

    b. Instead VSP focuses on ensuring that the code of applications running on a server or workstation always executes the developer's intent and not the attacker's intent.

2. **Targeted Attack Protection:** Sophisticated cyber criminals and nation states are now resorting to attacks that Weaponize at Run Time (WRT). This means that instead of starting new, malicious processes like conventional malware does, the typical WRT attack targets one or more 0-day vulnerabilities in the application's code base to seize control from an existing legitimate process in order to execute the attacker's intent. These attacks are indefensible when using conventional cyber security technologies. VSP is the only cyber security technology that deterministically prevents such targeted attacks without needing any signatures.

3. **Full Attackable Surface Protection:** VSP protects compiled (including third party software where no source code is available), interpreted or business logic, and micro code in CPUs used for speculative execution acceleration. In addition to protecting code, VSP also protects the file system against unauthorized changes in real time.

4. **Millisecond Dwell Time:** Failure to detect attacks in a timely fashion allows the attacker to dwell for extended periods of time. Unlike conventional security controls, VSP can thwart Conventional, Scripted and WRT Malware in real time at the initial infiltration stage itself thereby reducing the window of opportunity for the attacker to milliseconds. Early remediation results in not having to deal with the steps required to purge the attacker's wares across the connected digital infrastructure.

5. **Compensating Controls and Application Hardening:** Enterprise IT operations are challenged by dilemma and difficulty presented by patching vulnerable applications. Not deploying patches in a timely manner opens the door to WRT attacks. Even attackers with the skill set of script kiddies can now easily extort the enterprise. VSP hardens the application such that it cannot be attacked even if vulnerabilities exist and patches are not deployed.

6. **Risk Reduction for Enterprise:** VSP provides detailed attack forensics, which not only helps reduce pressure on SECOPS Analysts but also helps DEVOPS quickly remediate vulnerable code thereby reducing risk to the enterprise.

7. **Value Add For Existing Security Controls:** VSP's Protection Engine can feed highly granular attack metadata into adjacent security tools such as IPS/ NGFW/ WAF etc. thereby improving their efficacy going forward.

8. **Facilitating Digital Transformation:** VSP works seamlessly for applications found in the various IT & OT tiers; especially for enterprises in the defense and industrial control sector where cyber attacks occur on software which must operate in environments with no Internet connectivity.

9. **Vertical and Infrastructure Agnostic Protection:** VSP protects server workloads running on physical, virtual or containerized compute instances found in the cloud, data centers or hybrid environments of large ICS, Govt & Defense, Technology, Healthcare customers globally.

10. **Out of the Box Deployment and Runtime Experience:** VSP automatically extracts high granularity telemetry from process memory and the file system of each host it protects without requiring any code changes or complicated installation and deployment.