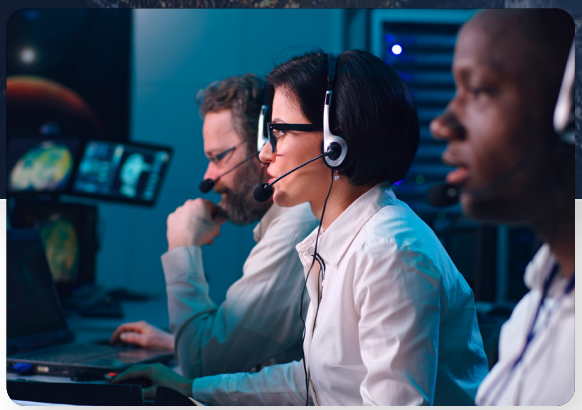
Virsec Security Platform

Stop Tomorrow's Zero-Day Attacks Today



Zero Trust Protection for Application Workloads

Radically strengthen your security program, stop attacks in milliseconds, and eliminate dwell time with Virsec's precise, continuous workload protection.

Virsec continuously protects application workloads, stopping known and unknown attacks—including zero-days. Virsec Map technology precisely maps what's expected (or not), only allowing trusted apps, files, and processes to run. Further, Virsec Enforce stops malicious code before it can run, protecting workloads at every moment. Battle-tested against the top government red-teamers and trusted by leading Fortune 100 companies, Virsec has repeatedly proven a protection-first model is not just possible, it is the next frontier for hybrid cloud workload protection.

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

Virsec Security Platform (VSP)

Virsec Security Platform (VSP) is a cybersecurity solution that continuously protects applications and host workloads against advanced cyber threats and neutralizes zero-day exploits with zero dwell time (milliseconds).

VSP aligns with zero trust architectural approaches and presents a portfolio of mitigating security controls that automate the runtime execution of authorized processes, libraries and dependencies for Windows or Linux Host OS workloads.

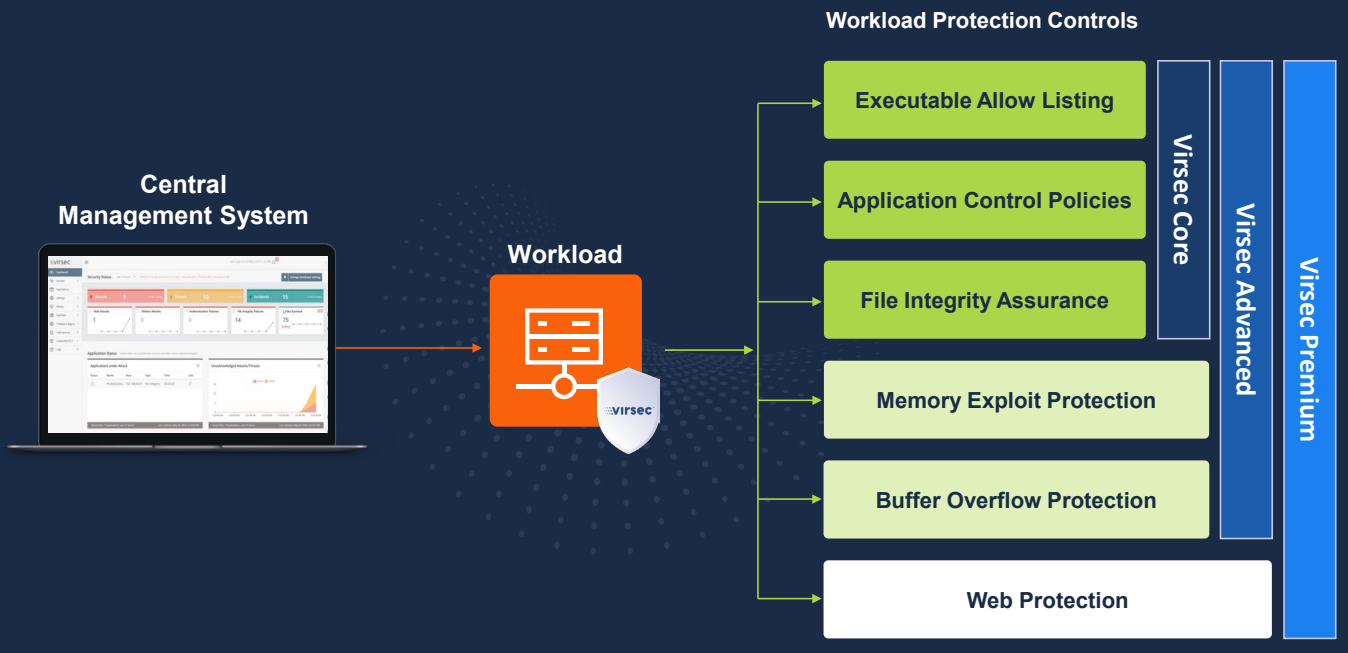
Gartner

"Enterprises using endpoint protection platform (EPP) offerings ... for server workload protection are putting enterprise data and applications at risk."

Gartner's 2020 Market Guide for Cloud Workload Protection Platforms

Virsec Zero Trust Protection Capabilities

virsec



Solving Your Toughest **Cybersecurity Challenges**

Protecting server workloads is uniquely different from securing client endpoints and requires an additional set of capabilities to stop malware and nation-state attacks before they wreak havoc. Most organizations struggle with the growing threat of ransomware crippling critical workloads, advanced threats from zero-day and supply chain poisoning, the unrelenting and tedious cycles of panic patching, and the exposure from out-of-support systems. Virsec solves these challenges with the highest security efficacy and lowest operational costs to:

PROTECT LEGACY AND OUT-OF-SUPPORT APPLICATIONS AND WORKLOADS

Reduce vulnerable attack surface by securing workloads even if they are no longer receiving security updates, and without needing access to the source code.

PROTECT AGAINST RANSOMWARE BREACHES

Proactively prevent advanced attacks from exploiting breaches and corrupting server workloads.

ELIMINATE PANIC PATCHING

Shift from a reactive to a proactive approach to patch management, applying patches on your schedule thus allowing for a thorough test and deployment process.

INCREASE OPERATIONAL EFFICIENCIES

Reduce costs and improve productivity of security program by eliminating alert fatigue, lowering performance overhead, and simplifying operations.

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

The Virsec **Value Promise**

Eliminate Zero-Day Threats

Stops known and unknown, zero-day, memory, fileless, file-based attacks from infecting workloads in milliseconds.

Take Attacker Dwell Time to Zero

Stops an attack before it starts with automatic threat interdiction that ensures zero dwell time and helps put an end to long-term data damage and loss.

Embrace Zero Noise

VSP eliminates false positives, vastly reducing analyst intervention across all environments.

References

BROADCOM

ANDY NALLAPPAN, CHIEF TECHNOLOGY OFFICER

"Conventional tools will not help us protect what matters most to our business. To do that, we have selected Virsec because **they start with runtime protection from the inside.** They are truly leading the way to more advanced cyber protection."

Raytheon

JOHN DESIMONE, VICE PRESIDENT, CYBER

"It's essential to make sure that mission-critical applications only do the right thing. This requires what Virsec delivers—**having visibility into the full application stack** and ensuring that only the right code executes."

inspirage

NORM MESSENGER, CHIEF SECURITY OFFICER

"We need real-time visibility into all of our systems to meer all our customer's security needs. We use CrowdStrike for our end points, but for critical servers we need the **application awareness that only Virsec provides."**

Customer **Snapshot**

ENTERPRISE

InfoArmor, BROADCOM, TATA, Bloomenergy, FREEDOMPAY, Bottomline, Raytheon Technologies, GE Healthcare

COMMERCIAL / SMB

GroundProbe, GreenLight Biosciences, Karnataka Bank, LUMICELL, Independence Contract Drilling, Godrej, inspirage, Vivriti Capital, QDB, Boston Red Sox

PUBLIC SECTOR

भारत सरकार Government of India, U.S. Department of Energy, Government of Fujairah, Alabama A&M University, Homeland Security, SVCW, Gwinnett, Sahuarita Arizona

virsec™

To learn more about the Virsec Security Platform and to find out how to start protecting your mission-critical server workloads, visit us at **www.virsec.com**

At Virsec we know a protection-first cybersecurity model is possible. By making server workloads self-protecting, we offer continuous protection, stopping known and unknown attacks—including zero days. With our revolutionary, patented technology, we secure software from the inside at runtime, precisely mapping what the app can do and stopping malicious code before it can run. Battle-tested against 200+ of the top government red-teamers and trusted by several Fortune100 companies, Virsec has repeatedly proven a protection-first model works. Virsec is headquartered in San Jose, California, with offices worldwide. For more information, please visit **virsec.com**.