

Virsec Automated Protection Platform



Stop cyber attacks in milliseconds. Automate protection at scale.

50+ new vulnerabilities are exposed every day that require constant patching to protect critical data systems*. These vulnerabilities pose a significant cybersecurity challenge to enterprise and public sector organizations who are spending considerable resources to defend themselves against ransomware, supply chain poisoning, zero-days, and remote code execution attacks. **It takes an average of 287 days to identify and contain a data breach resulting from these attacks.*** That's nearly a year for attackers to dwell within your network and your security teams to mitigate the damage.

These attacks unfold in seconds, yet the industry's best tools detect and respond in minutes, hours, or days. These tools are failing and security teams are overburdened by the constant scan-patch-scan cycle resulting from false alerts and remediation efforts from them. **60% of enterprises experience difficulties in retaining qualified cybersecurity professionals***, and this is a primary cause.

These traditional security tools are not bullet-proof, as evidenced by the vast number of recent data breaches and the cost. **The average total cost of a data breach in the U.S. increased from \$8.64 million in 2020 to \$9.05 million in 2021.***

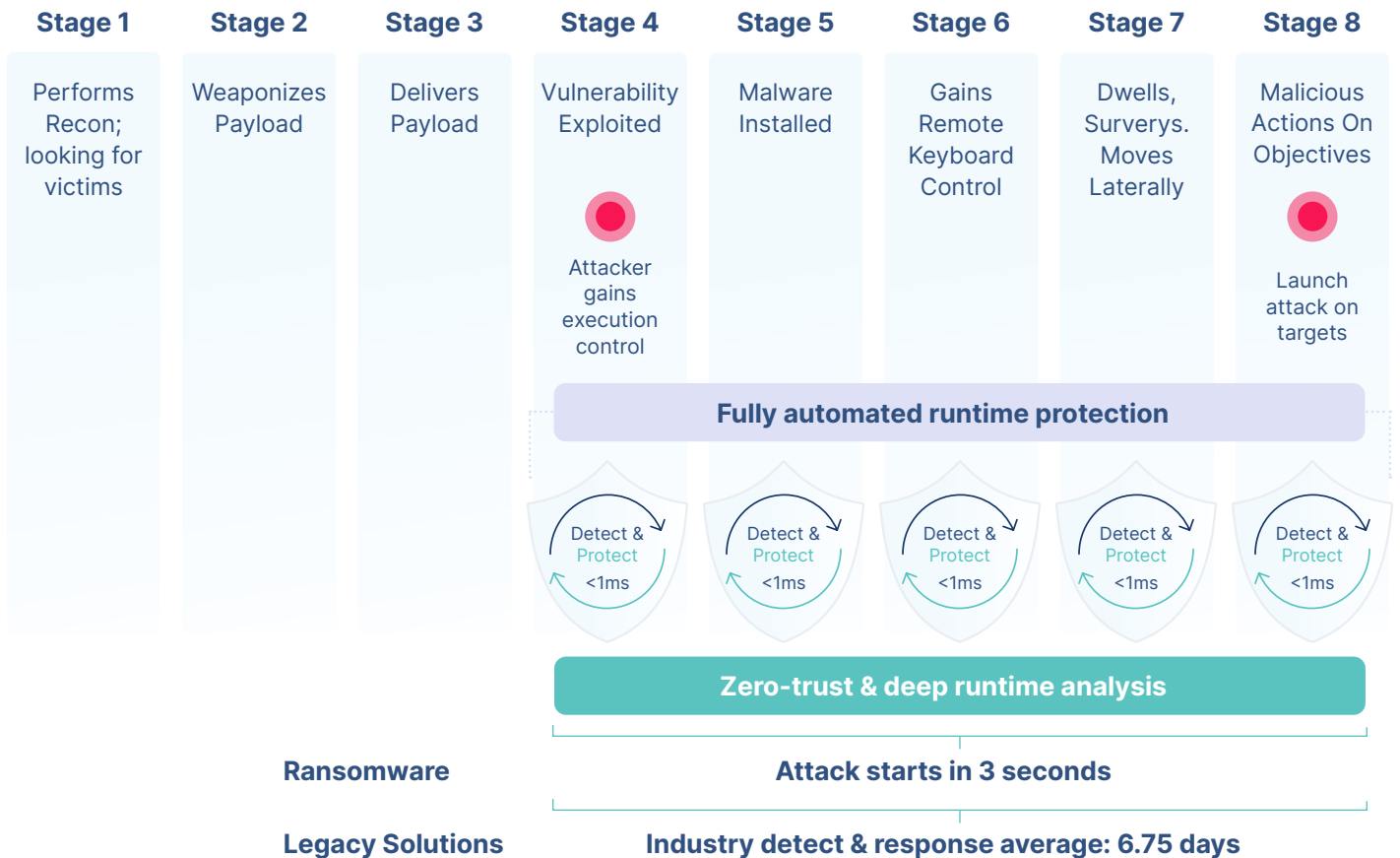
Instead of reacting to alerts, burning out your staff, and paying ransomware, it's time to ask yourself:

How long will it take you to STOP the next attack on your server workload?

Virsec has redefined what is possible and provides a protection-first automated solution for server workloads that stops attacks in **milliseconds**—before the attacker can inflict any damage. Your critical server workloads remain protected, remediation response is automated, letting your teams patch for maintenance, not emergencies.

Stop attacks early in the kill chain.

It takes just 3 seconds to launch an attack, yet traditional solutions take an average of 6.75 days to detect them, leaving plenty of dwell time to inflict damage. Virsec stops threat actors early in the kill chain—within milliseconds before malware even has a chance to execute.





The only way to protect an application is to understand it from the inside out.

- Virsec maps exactly what each workload is meant to do and blocks any deviation
- Virsec automatically protects your server workloads from any type of threat—known or unknown—in milliseconds
- Full-stack application protection—from legacy and on-prem to container and cloud-native
- Server workloads—even if they're unpatched, become self-defending
- Virsec is automatically deployed to servers using Red Hat Ansible playbooks
- Customizable playbooks automate remediation response for any threats that are stopped, reducing the burden on over-taxed security teams, and driving new levels of operational efficiency

A fully automated security solution platform for your most critical server workload applications.

The Red Hat Ansible Automation Platform provides a foundation for building and operating enterprise-wide automated security protection across roles, environments, and processes. You will centralize and control your infrastructure with a visual dashboard, role-based access control, and automated remediation. This automation enables the day-to-day management of tasks with minimal demand on security operations teams, driving operational efficiency.

Virsec's Automated Protection

Scale	Automated Protection	Operations Efficiency
 <p>On-prem, hybrid, cloud/container server workloads. Linux and Windows</p>	<p>Cyber-attacks stopped in milliseconds</p> <p>External and insider threats, supply chain integrity, zero trust for server workloads</p>	<p>Protects faster than malware can execute</p> <p>Elevates task level of Security Operations personnel, with precise, immediately available forensics</p>
 <p>On-prem, hybrid, cloud/container IT environments. Linux and Windows</p>	<p>Orchestration of incident response tasks across the enterprise</p>	<p>Reduces burden on Security Operations personnel, lowering the effort of sorting through alerts and prioritizing for action</p>



“For the past year, [SHBC](#) has used the protection platform by Virsec to protect more than 100 servers from ransomware, SQL injections, and other threats. When our applications begin to deviate from their intended actions, the Virsec platform immediately detects the change and provides real-time notifications so we can remove the threats. In addition to providing a critical layer of security, the protection platform also gives our servers more power and helps them run more efficiently. Based on the success of the tool, we hope to add additional servers this year.”

ADNAN MASRI
IT Manager, SHBC

Improve your security posture and transform culture in 3 weeks.

It's time to start protecting your server workloads. With deployment on Ansible, we help you get Virsec up and running in 3 weeks. Our team of experts takes you from detecting and responding to alerts and constant patching to self-defending server workloads with fully automated remediation response. Our solution improves your security posture, team morale, and staff attrition.

WEEK 1 (1-3 DAYS)

During this phase, we'll start with discovery and map your server workload topology and then deploy our probes using pre-configured Ansible playbooks.

WEEK 2 (1-3 DAYS)

Next, we'll enable runtime protection of your identified server workloads and do any fine tuning.

WEEK 3

Now that your server workloads are protected, we'll consult with your teams to configure your incidence response automation playbooks. Examples include automation of ticketing, new firewall rules, and file and VM quarantine.

Deployment times are based on resource availability and your environment.

Post-Deployment Culture Transformation

Now that you've implemented a fully automated self-defending security platform, you'll transform your security team culture with the orchestration of incident remediation tasks across the enterprise. You'll be able to transition in/out of protect mode as needed for system management and end the patching crises.

"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."

SID PHADNIS

Principal for Cybersecurity,
Broadcom



To learn more about Virsec's Automated Protection Platform and to schedule a live demo with one of our experts, visit <https://www.virsec.com/request-demo>



*<https://www.redscan.com/news/nist-nvd-analysis-2021-record-vulnerabilities/>
*[ISACA State of Cybersecurity 2022](https://www.isaca.org/News/State-of-Cybersecurity-2022)
*<https://securityintelligence.com/news/news-vulnerabilities-25-days-remediate/>
*Cost of a Data Breach <https://www.ibm.com/downloads/cas/OJDVQGRY>