Eliminate Panic Patching

Improve Security and Reduce Operational Stress

Unpatched vulnerabilities are the most prominent attack vectors exploited by ransomware groups.

Every time a new security patch is issued by a vendor, IT and Security teams must rush to deploy the patch across several server workloads. As the volume and velocity of patches increases, competing priorities place the IT Operations, SOC and triage teams in constant high-pressure situations. This rushed unplanned manual patching is disruptive to the business, error prone and overrides the planned release cycles. It also does not allow for proper patch testing and validation.

Cybercriminals have become very adept at finding unpatched systems rapidly after a vulnerability is disclosed. Applications and workloads have become the most common entry point for inserting malware into an environment. Organizations must defend themselves by going beyond panic patching. Virsec Security Platform (VSP) offers a continuous runtime protection solution that protects workloads even while they have not been patched.

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

Challenges for Patching in a Timely Manner

1

Volume

Demands too many to staff, leaving known vulnerabilities unassigned

2

Resources

Updating thousands of servers take time, staff and maintenance windows

3

Critical Processes

Taking systems offline causes business disruption

4

Policies

Many hoops to jump through to get the right staff to deploy the right patch to the right workload

5

Legacy or Out-of-Support Applications

Commercial applications, no vendor support for packages or applications or the in-house development team is no longer available

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

Virsec Security Platform

Virsec Security Platform (VSP) automatically maps what your server applications are supposed to do, then stops any deviations in milliseconds, preventing attackers from leveraging vulnerabilities to take control and run malicious code. VSP is a proven technology that enables leading government and commercial organizations worldwide to protect workloads essential to business at runtime against ransomware and other known and unknown threats before there is business impact, even systems left unpatched.

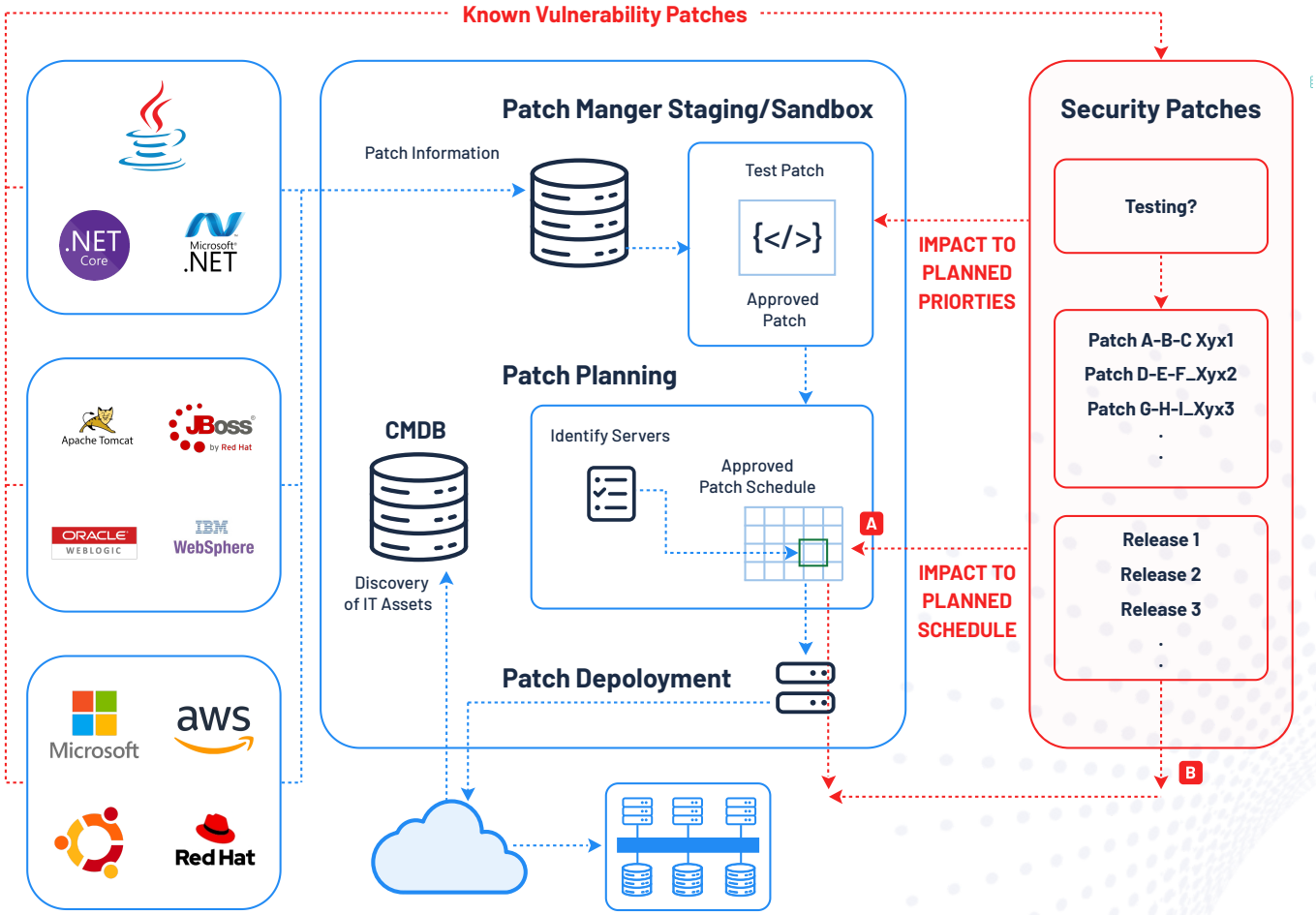
Virsec is differentiated from 'detection and response' solutions which rely on analysis after a breach has occurred. Instead, VSP uses deterministic techniques that proactively protect against ransomware and malware exploits with Virsec Map, which defines the executable allow list of what is authorized (system integrity) and Virsec Enforce which dynamically enforces that the software executes as expected (runtime protection).

VSP continuously monitors file systems, registry, scripts, and processes to ensure system integrity of applications and workloads. It verifies applications are reputable and trusted. This facilitates the automatic detection of DLL injection attacks, and misuse of legitimate software components and tools, without requiring rules and signature updates. Virsec also continuously addresses high-risk and critical Common Vulnerabilities and Exposures (CVEs) and Common Weakness Enumeration (CWEs) and zero-day events without manual efforts or need for expertise, allowing teams to easily deliver on security commitments with less overhead. Furthermore, VSP provides advanced web controls against all OWASP attacks and deep runtime visibility into data flowing through your business logic, validating HTTP & SQL input and responses for precise detection.

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

Proactive vs Reactive Patching

With Virsec Advanced configured in protection mode, organizations can eliminate panic patching and instead, conduct patch releases within their normal maintenance windows and processes. This is akin to having a 25th hour in the day, giving you more time to process the security patch in a structured way with proper testing and release management planned out in advance. With Virsec the risk of unforeseen effects is minimized, and IT and Security teams can have more assurance in what they deploy and when they deploy. Precious resources can now be focused on higher value tasks that enable and grow the business versus always being on defense.



For further information please see www.virsec.com.

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

Optimize Workload Protection Strategy

Take the complexity out of workload protection with a single solution that provides continuous runtime protection at depth across all vulnerable server applications. Identify known and unknown attacks and evasive threats like process or DLL injections under a single integrated solution that provides additional advanced web application protection capabilities and precise zero-day defense.

Improved Security

- Virsec provides a protection-first security posture by controlling application system integrity to only execute as intended and blocking any unknown or known bad functions.
- Reduce risk of your most vulnerable workloads – unpatched systems actively targeted by cybercriminals.

Cost Reduction

- Reduction or no interruptions to business services and applications - allows for continued ROI on existing applications and their supporting infrastructure
- Eliminates the immediate need to panic patch – reduce rescheduling and resource challenges
- Reduction in investigating false positives

Maintenance

- Allows for continued use of implemented known maintenance and troubleshooting processes and utilization of IT staff's established knowledge.

User Experience

- Maintain consistent user experience within established processes and methodologies.

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.

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