virsec™

Buyer's Guide
Zero-Trust Application Workload Protection

Introduction: Protecting Application Workloads

Modern workloads for most organizations typically comprise hundreds of systems executing across multiple clouds, on-premises, VMs, and containers. Protecting this dynamic and complex environment is increasingly more critical as advanced attacks target these crown jewels. Traditional EPP/EDR solutions designed for protecting end-user clients are not well-suited for servers.

Zero-day attacks have become a great cause for concern as unpatched systems are increasingly targeted by cybercriminals as they are often the most vulnerable. **Remote Code Execution (RCE)** is a common attack vector used here as existing cybersecurity tools have failed to adequately guard against it.

Many popular solutions rely heavily on detecting and responding to breaches after they have happened, resulting in high dwell times and giving attackers plenty of opportunity to inflict catastrophic damage. These solutions are also very noisy, creating a high volume of false positive alerts and drowning security teams in tedious work that takes away their focus from high-priority issues.

According to Gartner,

"Enterprises that use an EPP offering designed for end-user-supporting devices are putting enterprise data and applications at risk."[1]

Assets Affected by Security Breaches

The 2021 Verizon Data Breach Investigations Report shows that attacks on servers dominate compared to those on user accounts and client devices. Furthermore, the report also shows that attacks on web application servers outpace any other asset type.

Hence, securing server workloads in the cloud, multi-cloud, or on-premises has become a very high priority for most organizations.

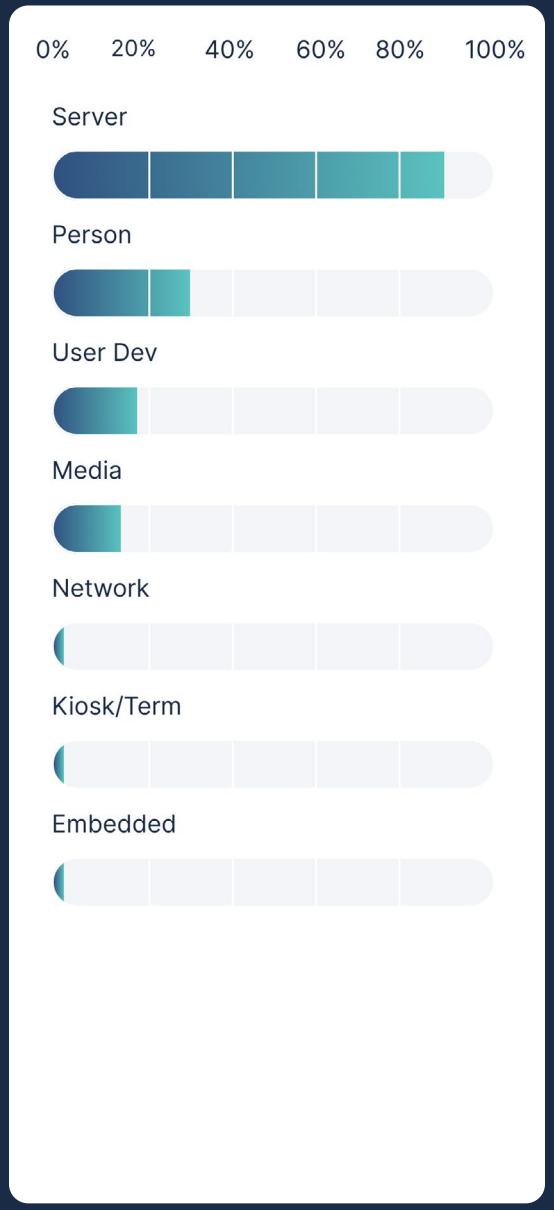


Figure 22. Assets in breaches (n=4,384)

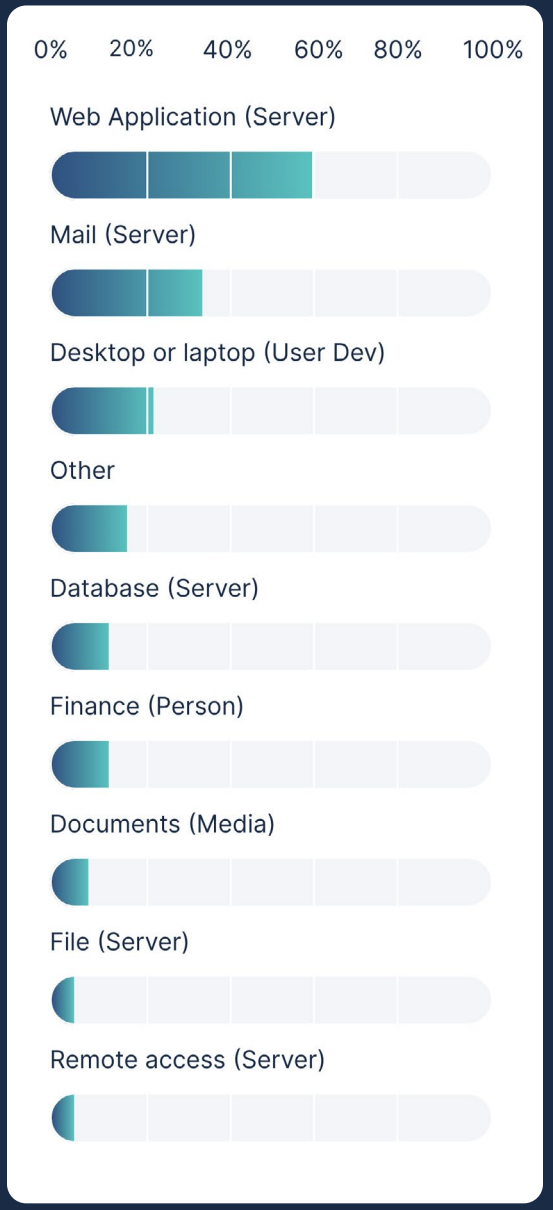


Figure 24. Top asset varieties in breaches (n=2,796)

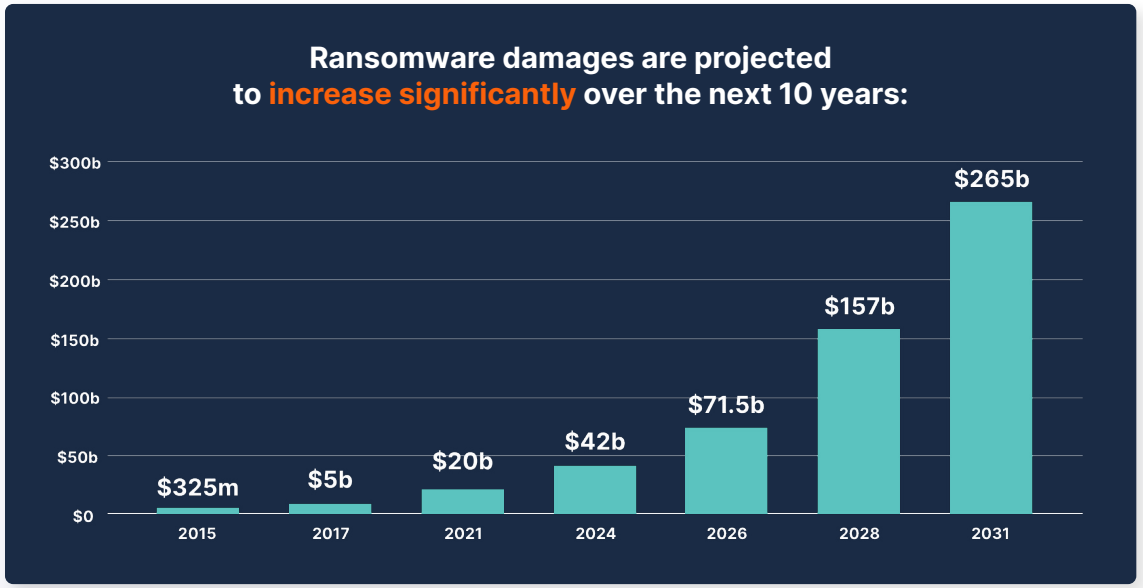
Typical Uses Cases

Use Case 1

Protect Against Ransomware Breaches

Ransomware has become one of the most prevalent attack types globally, doubling in frequency annually (Verizon DBIR 2021). 37% of global organizations said they were victims of a ransomware attack in 2021 (IDC 2021 Ransomware Study).

Ransomware demands were up by 144% in 2021.[2]



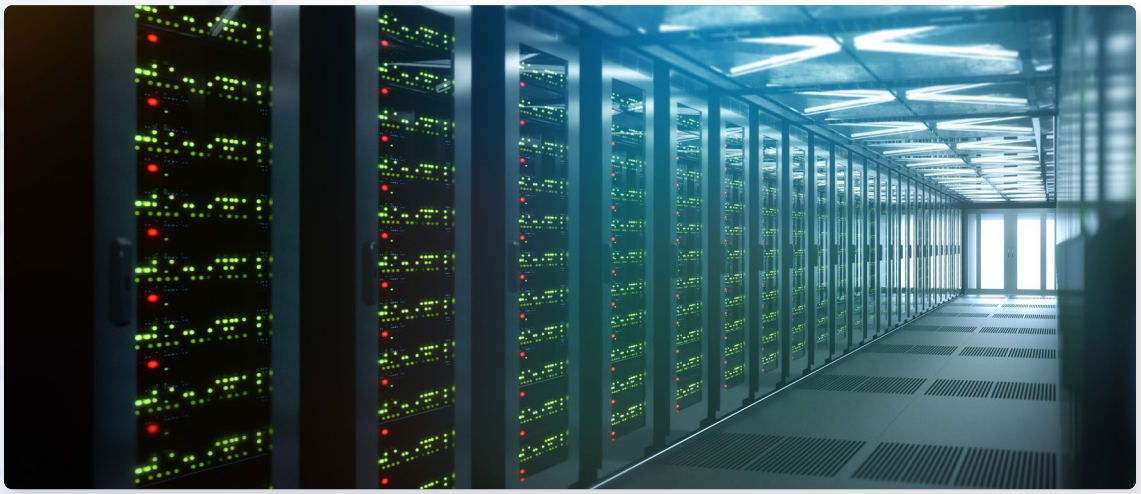
Nearly 80% of organizations that pay ransoms are hit again with another ransomware attack. Nearly 46% of the attacks were from the same group that executed the first attack.

8% of organizations manage to retrieve their data after paying a ransom.

29% of organizations recieved less than half of their data.

2 https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2022-unit42-ransomware-threat-report-final.pdf

Use Case 1



Ransomware typically infiltrates through common attack vectors including exploiting unpatched vulnerabilities, remote desktop access, phishing, and credential abuse. Ransomware-as-a-service (RaaS) has become a well-established criminal market, making it easy for attackers to access exploit services.

Adversaries have gotten much faster at exploiting new vulnerabilities, with attacks surfacing merely hours after a new vulnerability is announced. Per SANS, unpatched vulnerabilities are some of the biggest and first attack vectors adversaries use.

Fileless malware, frequently used by attackers, easily evades traditional detection and response solutions, often by deploying malicious code directly into memory. Use of Living-off-the-land binaries (lolbins) is another technique used successfully to evade detection.

After infiltrating a victim's systems, attackers increasingly exfiltrate data before encrypting it to create "double extortion," which is a threat to publicly release stolen information and crippling business systems.

Ransomware groups have increased their impact by targeting cloud infrastructures to exploit known vulnerabilities in cloud applications, virtual machines, and VM orchestration software (CISA Report, 2021).

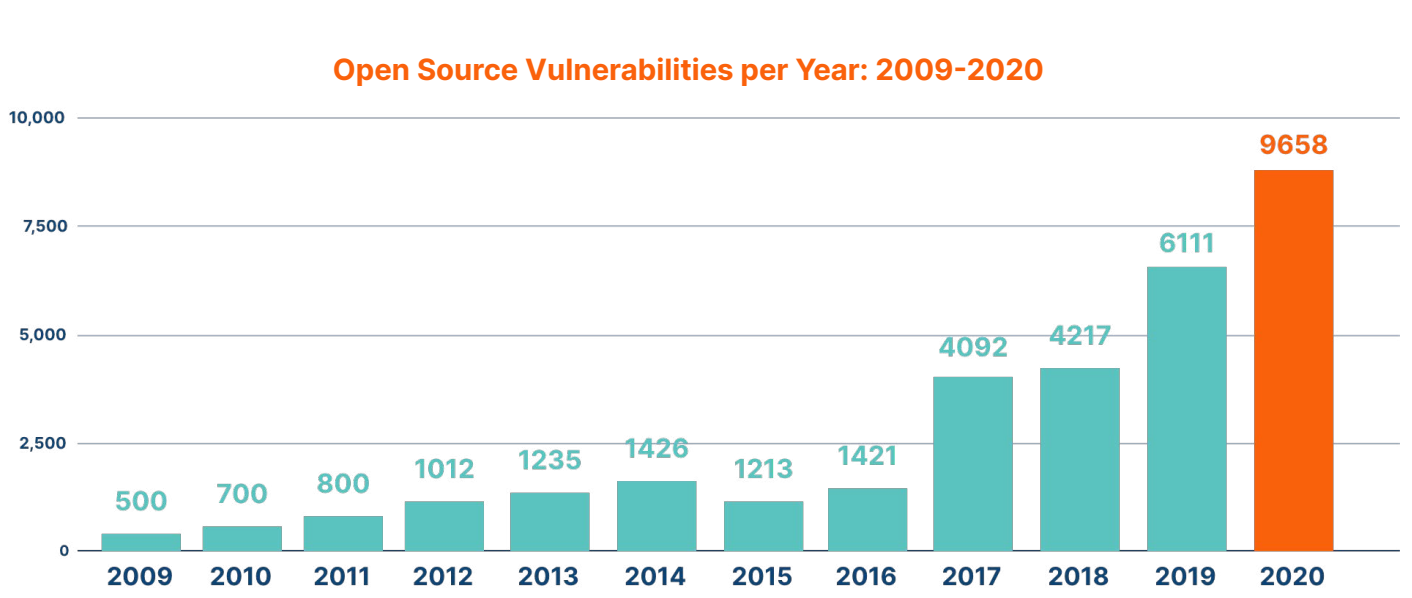
Organizations are looking to stop ransomware threats ideally instantly at runtime and reduce dwell time to near zero while also seeking better operational efficiencies such as fewer false positives.

Use Case 2

Eliminate Panic Patching for Zero-Day Vulnerabilities

According to Forrester Research, *"The number of open vulnerabilities WhiteSource reports more than doubled from 2018 to 2020. 2021 did not disappoint: The Stack estimated that 19,736 vulnerabilities were reported, an average of more than 50 per day!"*

Unpatched vulnerabilities are the most prominent attack vectors exploited by cybercriminal 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 increase, 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.



Source: Mend (WhiteSource), The State of Open Source Security Vulnerabilities, Annual Report 2021

Use Case 2

"How was the external attack carried out?"

Source: Forrester Research, The State of Application Security, 2022

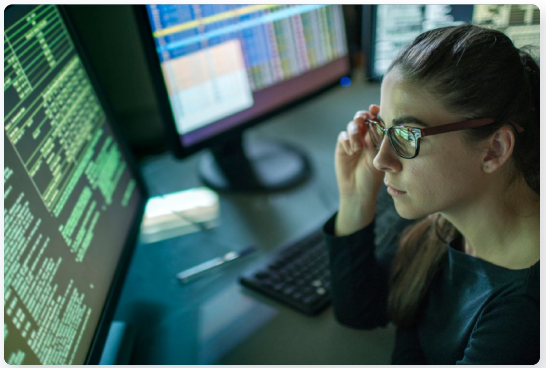
57% of cyberattack victims report that their breaches could have been prevented by installing an available patch

Source: Ponemon Institute and ServiceNow

The reasons organizations struggle with patching in a timely manner are:

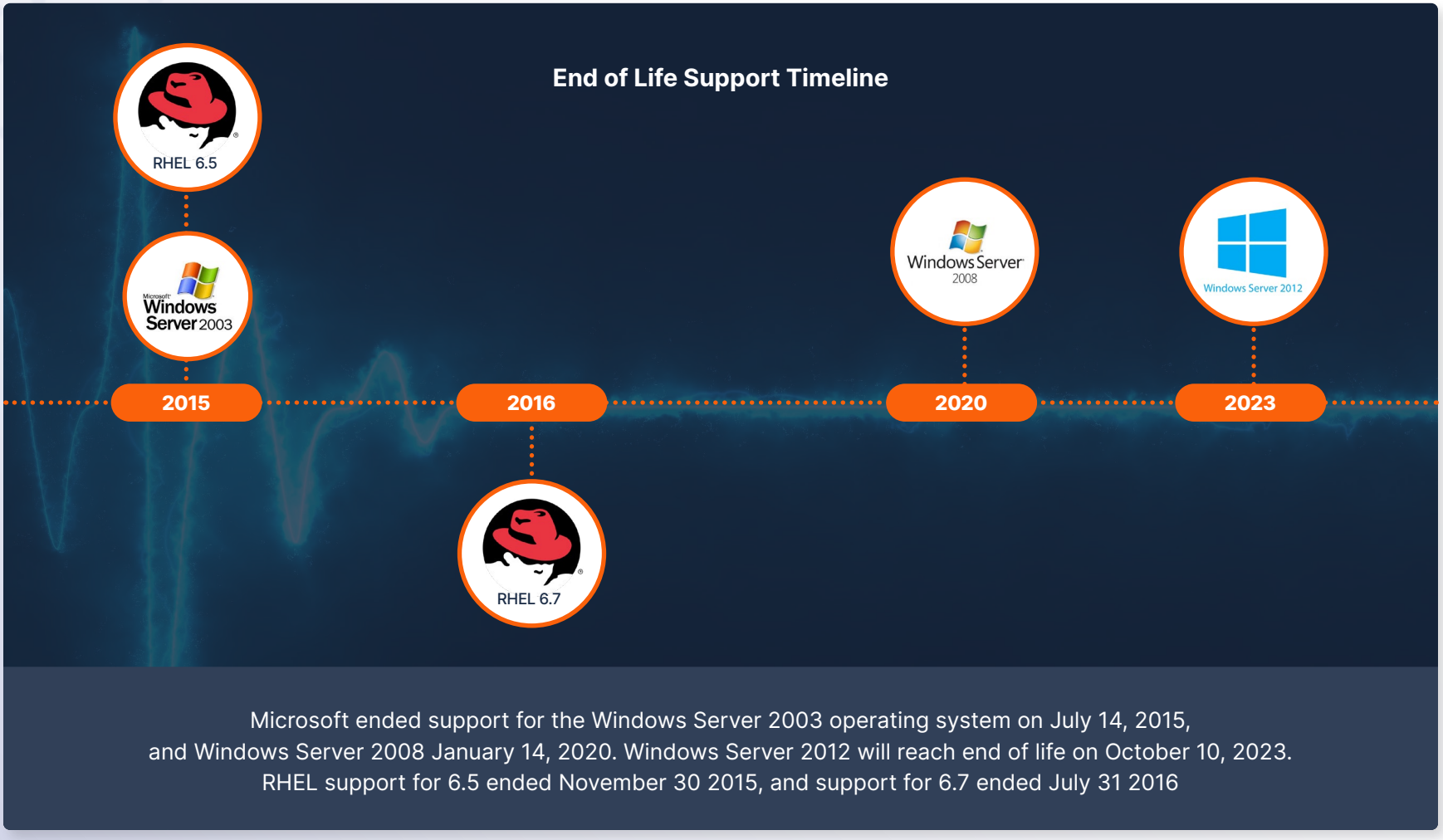
- **Volume** – demands too many to staff, leaving known vulnerabilities unassigned
- **Resources** – updating thousands of VMs takes time, staff, and maintenance windows
- **Critical Processes** – taking systems offline causes business disruption
- **Policies** – many hoops to jump through to get the right staff to deploy the right patch to the right workload
- **Legacy Application** – commercial applications, no vendor support for packages or applications, or the in-house development team is no longer available

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. They need a continuous runtime protection solution that protects workloads even while they have not been patched.



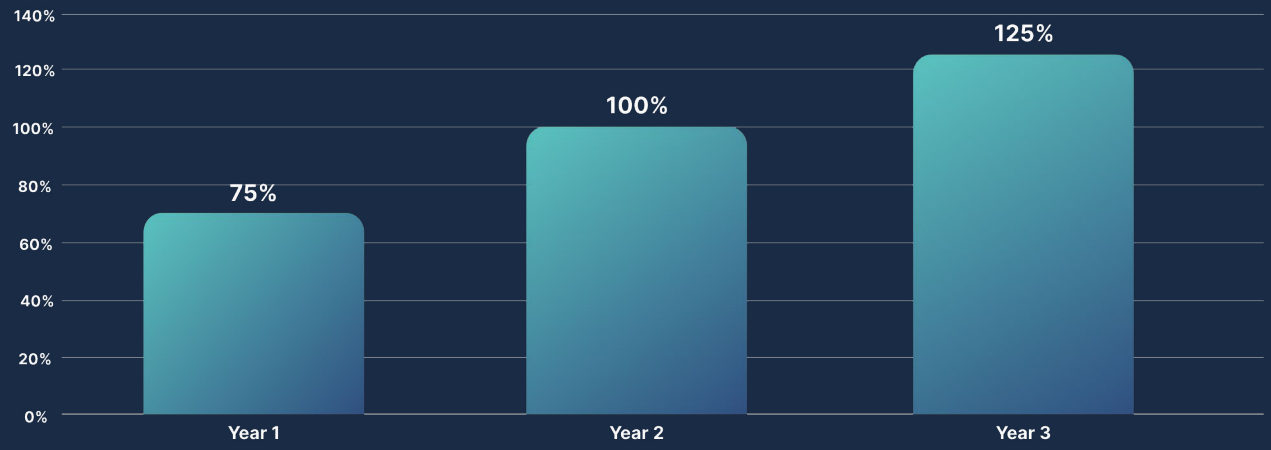
Use Case 3

Protect Legacy Out-of-Support Applications and Workloads



Microsoft ended support for the Windows Server 2003 operating system on July 14, 2015, and Windows Server 2008 January 14, 2020. Windows Server 2012 will reach end of life on October 10, 2023. RHEL support for 6.5 ended November 30 2015, and support for 6.7 ended July 31 2016

Use Case 3



Source: The Register

Legacy systems no longer supported by the vendor present a security risk. Even if your organization is making progress in patching legacy systems still supported by vendors, thousands of applications and varying workloads often pose an imminent security risk that remains unresolved, especially within expansive infrastructures with thousands of known vulnerabilities.

Where patching is not viable or too difficult to accomplish, organizations accept the risk without immediate remediation as they look to upgrade the business system sometime in the future.

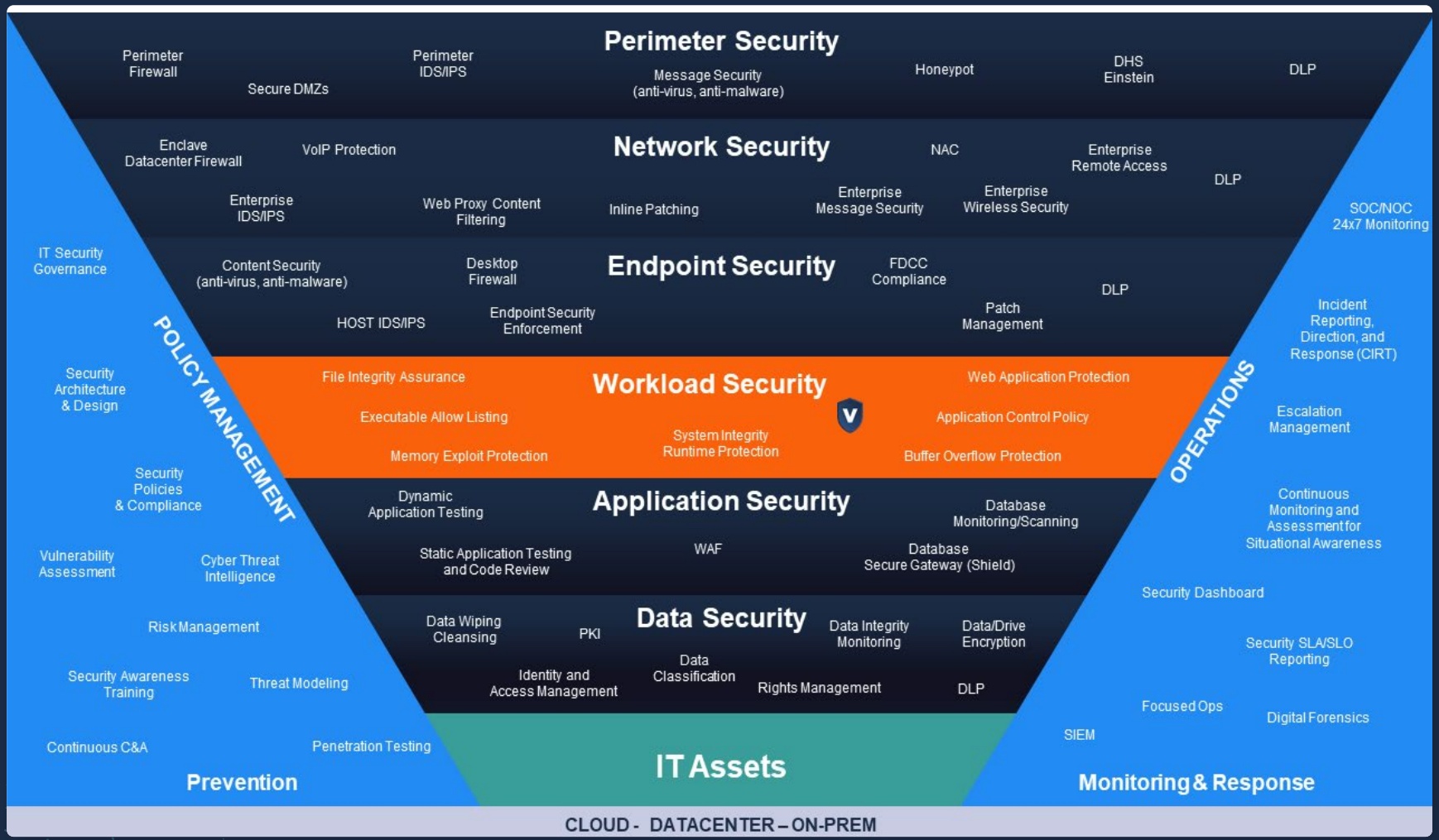
Typical Workload Security Challenges include:

- Legacy applications were written when application security was simple or non-existent
- New vulnerabilities and the sophistication of attack method continuously evolves, reaching voluminous levels
- Vendors have gone out of business, support has slowed or ceased with obsolescence
- Expertise to develop software patches or address software errors has become specialized and costly to maintain
- Digital transformation is an arduous process taking months or years to complete as risk remains

Organizations seek a solution that can provide the assurance that protection is in place for legacy application workloads that expose the business to risk, even when it is not practical or possible to patch those systems anymore.

Typical Approaches and their Advantages and Disadvantages

Vulnerable Attack Surface Workloads — Defense in Depth



Historically organizations have focused on shoring up their defenses for the network perimeter, endpoints, applications, data, and IT infrastructure. However, workload security has been largely underserved in the hybrid cloud age. As the diagram above illustrates, a modern Defense in Depth architecture must successfully implement specific controls for protecting server workloads.

As computing and the threat landscape have evolved, there have been a few different approaches employed by organizations to attempt to protect server workloads. Many of these were primarily designed for protecting other asset classes and are not ideally suited for modern workloads.

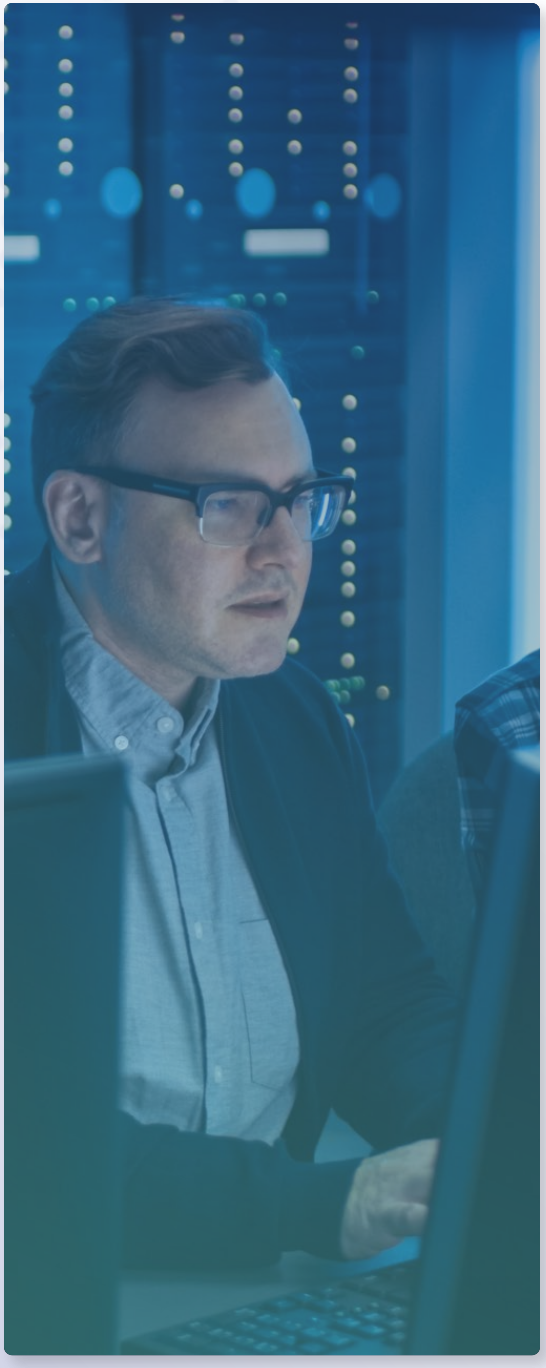
Here are some typical approaches and their advantages and disadvantages:

Endpoint Protection Platforms (EPP)

Born in the era of client-server computing, these EPP solutions primarily target end-user assets such as desktops, laptops, and mobile devices. Their primary protection mode is to use signatures to detect and block known malware. Their advantage is they can reliably block most cataloged malware, albeit sophisticated cybercriminals are able to morph their toolkits at an alarming pace to avoid signature-based detection. However, these tools were not created with server workloads in mind and are not ideal for protecting your crown jewels.

Endpoint Detection and Response (EDR)

In the last decade, we have seen the rise of EDR solutions. Their primary premise was recognizing that EPP solutions fail to detect all known and unknown malware. They also recognized that attackers would dwell for months without being detected once the malware could infiltrate an environment. EDR systems use Machine Learning to correlate logs from multiple systems and detect anomalous behavior indicating a compromise of IT assets. Their advantage is that they can detect attacks after they have happened, reducing dwell time to days or weeks from months. However, EDRs can generate a high volume of false positives due to the nature of ML algorithms. They also leave a wide enough window for attackers to inflict damage as malware is typically not blocked in real-time, only detected after a breach has already occurred.



First Generation Allow Listing Solutions

Another approach has been to catalog all good executables that should be allowed to execute and block everything else. While in theory, this approach is ideal for server workloads, the first-generation solutions required IT teams to update and tune the catalog manually and continuously. This was not only highly burdensome but also very difficult to manage as application development teams increased the pace at which they released new software and updates.

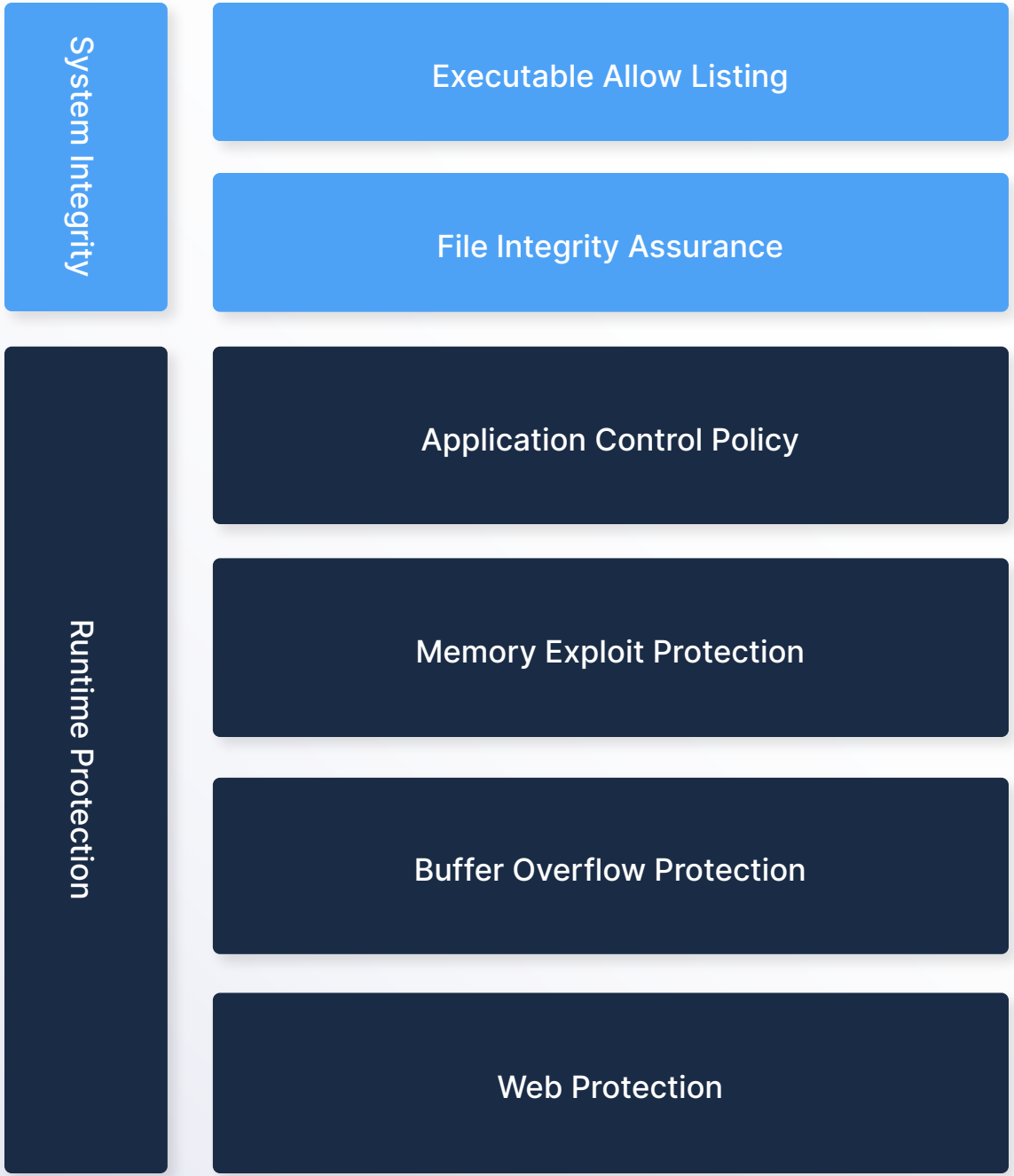
Zero Trust Protection

The most modern of solutions, zero trust protection of application workloads, takes a fundamentally different approach. Virsec Map automatically maps authorized processes, scripts, and libraries for the application workload and Virsec Enforce continuously enforces the mapping to maintain zero trust provenance and integrity of the dependencies. This mapping spans multiple layers, including the host filesystem, executables, and their libraries, memory, and web requests. By knowing exactly what is allowed at each layer, any malicious behavior is stopped instantly at runtime, thus reducing dwell time to milliseconds. This has proven to be highly effective at stopping modern threats that use advanced techniques such as fileless attacks, process hollowing, buffer overflow attacks, and SQL injection. In fact, deterministic protection blocks more attacks on the MITRE Software Weaknesses and OWASP Top Ten lists than any other type of solution. Most remarkably, this approach can even protect unpatched systems.
Another significant benefit is the drastic reduction in false positives.

Key Capabilities for Zero Day Server Workload Protection

Modern server workload protection platforms must meet critical criteria such as ensuring system integrity and offering runtime protection. They must also do so with minimum disruption, not require application source code, and ensure workloads are highly performant to meet business requirements.

Here are the key elements leading these solutions must provide:



For Protecting Hosts and Systems

Capability	Description	Evaluation Criteria
Executable Reputation Analysis	• Check every executable's reputation based on trusted publishers and a reputation database	✓ Built-in reputation service or integration with additional 3rd party services
Executable Allow-Listing	• Establish and enforce system-wide allow-listing for executables, libraries, and scripts based on their reputation • Enforce process-library dependencies at runtime	✓ Automated Allow-Listing ✓ Allows for manual entries and exceptions ✓ Accounts for all processes, libraries, and scripts
File Integrity Assurance	• Protects executables and library files from malicious tampering • Monitors critical folders for malicious file changes	✓ Stops all unlisted files and executables ✓ Takes a Default-Deny approach ✓ Monitors specific folders

For Protecting Binary Applications

Capability	Description	Evaluation Criteria
Application Control Policies	• Protects against advanced defense evasion techniques such as script-based attacks, Remote-Code Execution (RCE), and lateral movement	✓ Enforces parent-child process controls to stop RCE and lateral movement ✓ Runtime controls to allow/disallow binary applications to spawn child processes ✓ Access controls on binaries via allow list or deny list for processes such that either only a certain set of users are allowed to run a defined set of applications, or a specific set of users are always denied running a defined set of applications ✓ Block binary applications from running under all circumstances, even if they are generally trusted

Capability	Description	Evaluation Criteria
Living Off the Land Attack Protection	• Protects workload from file-less attacks • Stops misuse of trusted executables and interpreters	✓ Fine-grained access control for PowerShell, bash, and other native scripting tools ✓ Enforces specific command-line arguments and flags are allowed, or some risky command-line arguments and flags are denied during the execution of a defined set of binaries ✓ Low rate of false positives and false negatives
Memory Exploit Protection	• Protects legitimate and trusted workload processes from runtime memory injection attacks	✓ Precise protection via a zero trust approach ✓ Stops process injection techniques including, but not limited to, Code Injection, Process Hollowing, and Process Doppelgänging ✓ Stops OS credential dumping from the memory of key processes like LSASS ✓ Stops privilege escalation attacks like in-memory attacks ✓ Exploit techniques are detected and stopped in real time without the need for any signature, learning, or customization ✓ Protection for out-of-support Windows and Linux servers ✓ Low rate of false positives and false negatives ✓ High detection rate of true positives ✓ Dwell time down to milliseconds
Buffer Overflow Protection	• Protects vulnerable binary processes from buffer attacks	✓ Detects memory-based attacks such as buffer overflows, return-oriented programming, and other blind attack schemes on program flow, memory stack, and return addresses ✓ Protects runtime execution of pre-compiled applications by automatically extracting the control flow for every executable, and enforce any deviation during runtime ✓ Low rate of false positives and false negatives ✓ High detection rate of true positives ✓ Dwell time down to milliseconds

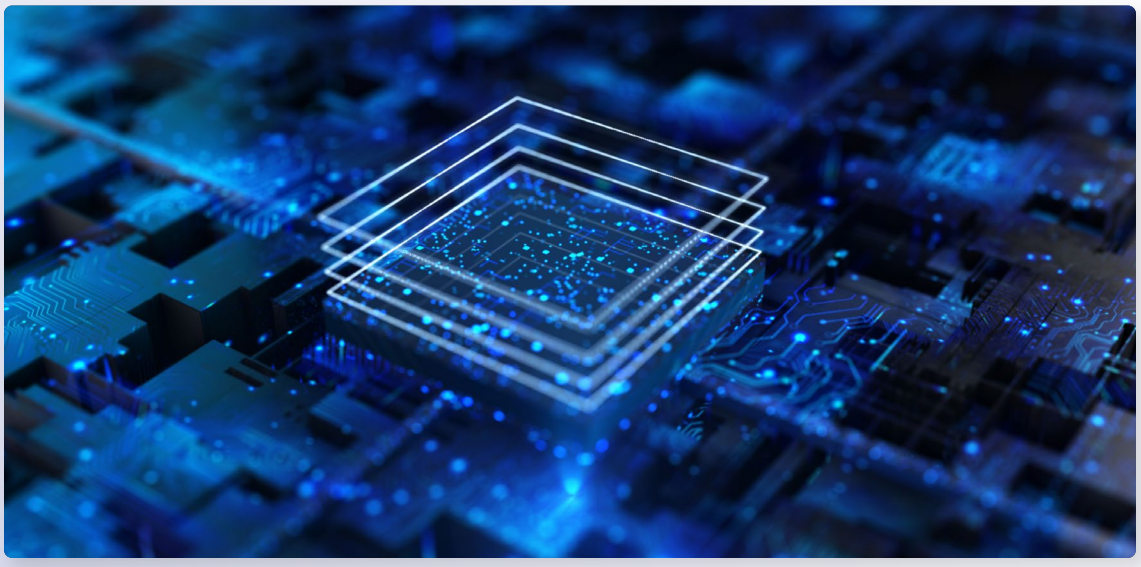
For Protecting Interpreted Web Applications

Capability	Description	Evaluation Criteria
Runtime Protection	• Continuously evaluates runtime instructions and stops attacks instantly	✓ Software Exception Logging ✓ Does not require app code modifications ✓ Minimal performance impact on applications
Injection Protection	• Prevents malformed input data from turning into malicious code	✓ Prevents Command Injection ✓ Prevents SQL Injection ✓ Prevents Carriage Return Line Feed Injection attack
Cross-Site Scripting (XSS) Prevention	• Prevents attacks that use malicious scripts to infiltrate web pages	✓ Prevents Cross-site Scripting Injection ✓ Prevents XML Injection
File Integrity Assurance	• Protects executables and library files from malicious tampering • Monitors critical folders for malicious file changes	✓ Local File Inclusion ✓ Remote File Inclusion ✓ Prevents Path Traversal Injection ✓ Implements a “Default Deny” approach

For Protection by Threat / Attack Vectors

Threat Vector	Required Capabilities	Evaluation Criteria
Ransomware	• Runtime protection for workloads • Deterministic and precise protection • Multi-layered defense	✓ Instant protection at runtime ✓ Efficacy against known and unknown malware ✓ Coverage against MITRE and OWASP attack types ✓ Low false positives and false negatives ✓ Dwell time down to milliseconds ✓ Does not require daily signature updates ✓ Protection across operating systems
Remote Code Execution (RCE)	• Protect against malicious commands being executed remotely	✓ Protects against unpatched vulnerabilities ✓ Protects against unknown zero-day vulnerabilities ✓ Implements a “default deny” approach ✓ Executable allow-listing to prevent unauthorized code to execute ✓ Prevents memory-based attacks ✓ Prevents fileless and living-off-the-land attacks
Zero-Day Attacks	• Runtime protection for workloads • Deterministic and precise protection • Multi-layered defense	✓ Instant protection at runtime ✓ Efficacy against known and unknown malware ✓ Coverage against MITRE and OWASP attack types ✓ Low false positives and false negatives ✓ Dwell time down to milliseconds

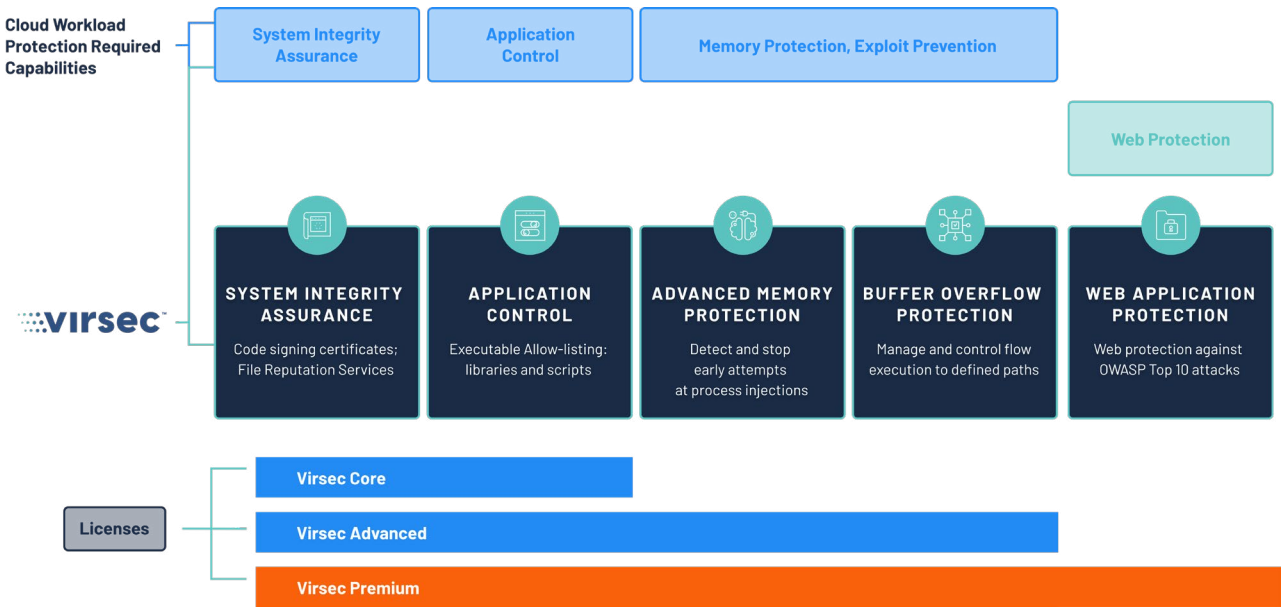
Threat Vector	Required Capabilities	Evaluation Criteria
Legacy workloads which are un-patchable	• Deterministic and precise protection • Virtual patching • Multi-layered defense	✓ Instant protection at runtime ✓ Protects legacy Windows and Linux server operating systems ✓ Efficacy against known and unknown malware ✓ Coverage against MITRE and OWASP attack types ✓ Low false positives and false negatives ✓ Dwell time down to milliseconds
Fileless attacks	• Living-off-the-land attack protection • Memory Exploit Protection • Buffer Overflow Protection	✓ Fine-grained access control for PowerShell, bash, and other native scripting tools ✓ Precise protection via deterministic approach ✓ Low false positives and false negatives ✓ Efficacy rate of true positives ✓ Dwell time down to milliseconds



Key Questions to Ask

- Does your solution ensure zero dwell time stopping attacks before any damage is done?
- What is the average dwell time with your solutions?
- Does your solution take a "Default Deny" or "Default Allow" approach?
- What mechanisms do you provide to protect legacy out-of-support systems?
- Does your solution provide Host protection for the application workload after a critical vulnerability is published and before a patch is released?
- How many false positives does your solution generate per month?
- How much tuning and rule-writing is required to maximize protection?
- How does the solution impact workload performance?
- Was your product specifically designed for server workloads, or was it created for client endpoints?
- Can your solution span across both cloud and on-prem systems?
- What is your coverage for MITRE Top 25 Most Dangerous Software Weaknesses?
- What is your coverage for OWASP Top 10?

Virsec Security Platform



The Virsec Security Platform (VSP) leverages the patented Virsec Map technology to protect high-value enterprise workloads from increasingly sophisticated cyber criminal attacks, including; memory corruption, code injection, supply chain poisoning, web attacks, and others. Unlike behavioral-based approaches that "estimate" malicious patterns, VSP takes a positive security posture to deliver a deterministic approach to authorize dependencies with certainty for runtime execution. Virsec Enforce automatically delineates between authorized dependencies such as files, scripts, and libraries and instantly stops any deviations.

Virsec proactively protects 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).

With a protection-first approach to zero trust, Virsec's positive security posture of allowing only 'known good' dependencies such as files, scripts, and libraries to run, stops all other malicious behaviors regardless if they are known or unknown attacks. VSP eliminates the logistical nightmare of reacting to vulnerabilities and security patches and does not require the ongoing update of threat feeds. Virsec Security Platform (VSP) protects against zero-day attacks with zero dwell time (milliseconds).

Conclusion

Securing server workloads in the cloud or on-premises is different from security for client endpoints such as desktops, laptops, and mobile devices. As such, you need security solutions specifically designed to protect server workloads, offering a broad set of specialized protection modes spanning system integrity and runtime protection.

At the highest level, your Zero Trust Application Workload Protection solution should offer all the following benefits:

Zero Dwell Time – Attackers should not have the luxury of infiltrating your systems and moving within your environment for hours and days.

Protect Legacy Servers – Reduce support costs and raise software security assurance by ensuring protection for operating systems and applications that are no longer supported by the vendor.

Eliminate Panic Patching – Get back hours in the day and reduce IT stress levels by implementing a pro-active patching process versus having to rush critical patches at unscheduled times.

Ransomware Protection – Stop advanced ransomware infiltration techniques such as fileless attacks and Remote Code Execution.

Low False Positives – Avoid noisy solutions that generate too many alerts. Your security team will be unable to keep up and likely to miss key indicators of compromise.

virsec™

[1]Gartner, Market Guide for Cloud Workload Protection Platforms, 12 July 2021, Neil MacDonald, Tom Croll. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.