virsec™

Return on Investment

The Value Drivers for Zero Trust Application and Workload Protection

- **Stop Zero-day Malware, Ransomware and Data Breaches**
- **Mitigate Vulnerabilities in Production Environments - Unpatched, Legacy, & Cloud**
- **Automate Application Workload Security Controls**

Executive Summary

The Virsec Security Platform (VSP) adds a layer to your defense in depth strategy that segments and proactively protects applications and virtualized compute infrastructure with automated security controls.

Three use cases are modeled to address:

1. **Ransomware protection**
2. **Legacy Microsoft Windows and Linux applications and host runtime environments**
3. **Unpatched vulnerabilities**

Top 3 Take-aways

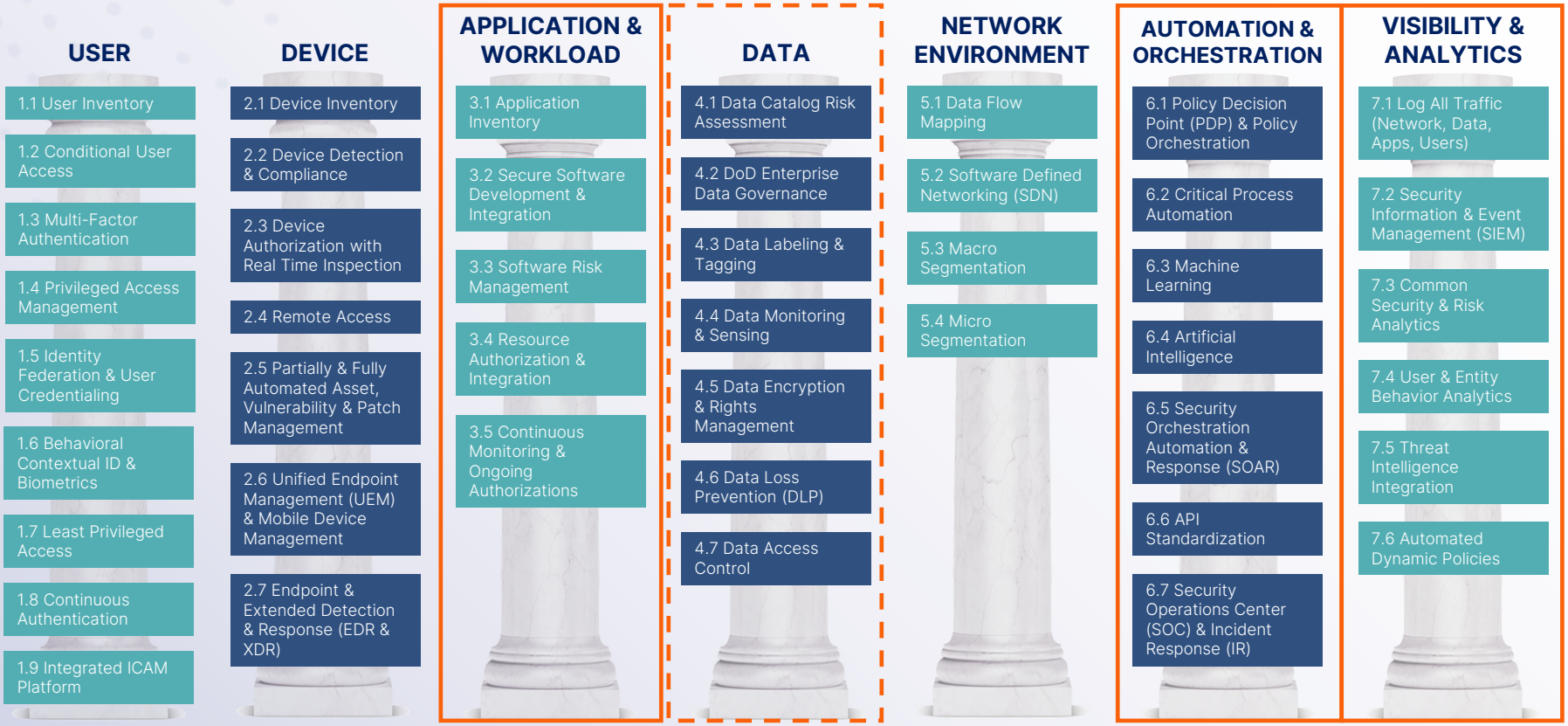
1. **Save $9.4 million over 3 years from operational efficiencies, cost avoidance, and fees for legacy systems.**
2. **Reduce human capital by 90% assigned to analyzing scans, false positives, and incident tasks.**
   - » **Avoid staff burnout**
   - » **Free up resources**
3. **Reduce risk from zero-day threats including: malware, ransomware, and data breaches exploiting vulnerabilities.**

Table of Contents

Zero Trust Application & Workload Protection

The Virsec Security Platform (VSP) integrates with the DoD and CISA Zero Trust pillars to deliver Zero Trust protection to:

- Application & Workloads
- Automation & Orchestration
- Visibility & Analytics



Source: DOD

Calculating Risk 5 Key Factors...

3 Factors

Likelihood of a Breach

1. the real-time threat of the vulnerability being exploited
2. the exposure of the asset to the threat
3. whether mitigating security controls are in place to protect the asset

2 Factors

Impact of a Breach

4. the severity of the vulnerability
5. the business criticality of the underlying asset

Risk = likelihood (%) x impact ($)

Source: https://www.balbix.com

Likelihood of a Breach

Highest Value Target: Servers

- **80%** of data breaches happen on **servers**
- Top attack patterns are **system intrusions** with basic **web application** attacks

Figure 19. Assets in breaches (n=4,433)

source: Verizon Data Breach Investigation Report, 2023

Impact of a Breach - System Intrusions

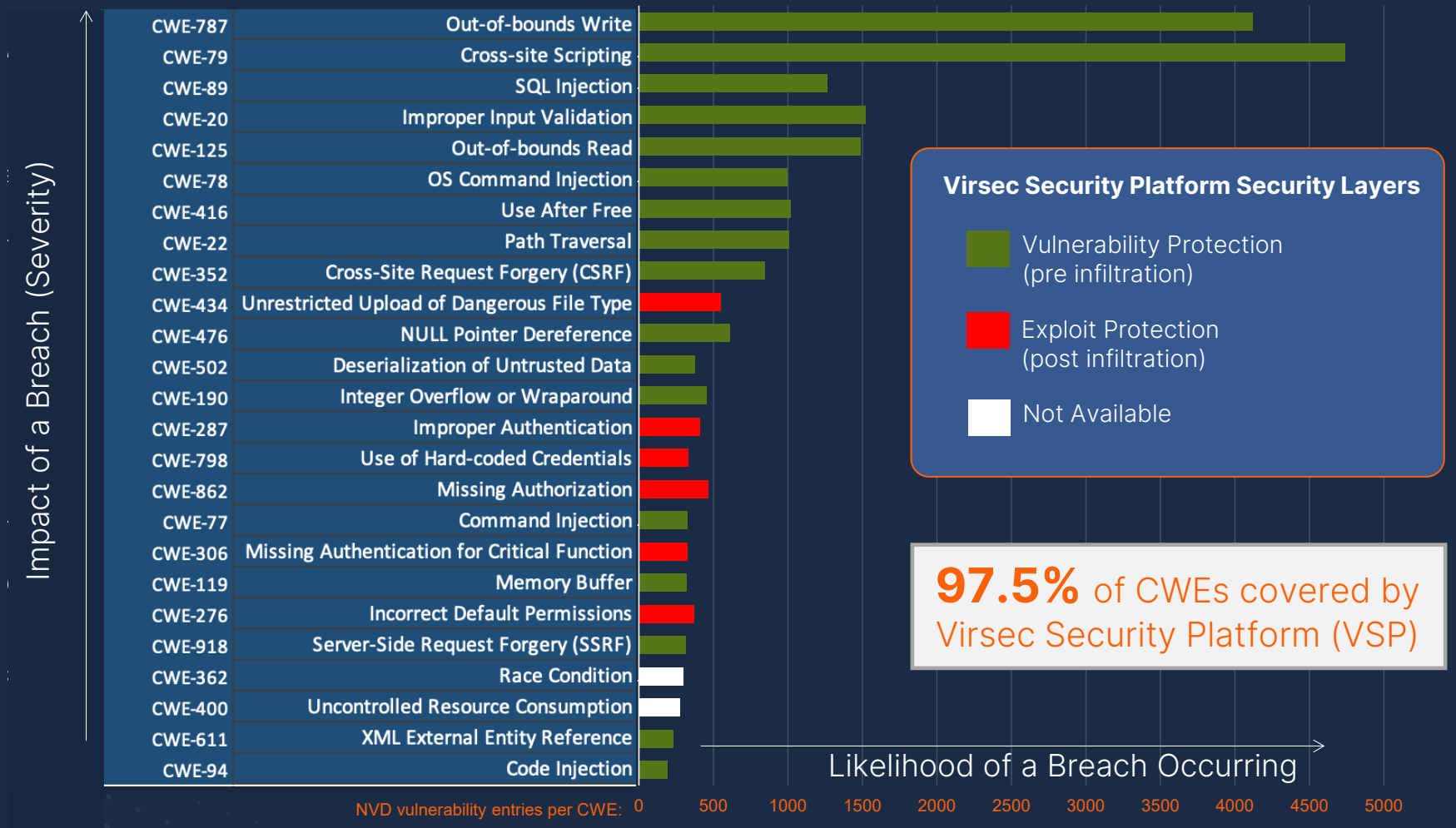
Top Routinely Exploited Vulnerabilities - CISA

	Vendor	CVE	Type
1	Citrix	CVE-2019-19781	arbitrary code execution
2	Pulse	CVE 2019-11510	arbitrary file reading
3	Fortinet	CVE 2018-13379	path traversal
4	F5- Big IP	CVE 2020-5902	Remote Code Execution (RCE)
5	MobileIron	CVE 2020-15505	RCE
6	Microsoft	CVE-2017-11882	RCE
7	Atlassian	CVE-2019-11580	RCE
8	Drupal	CVE-2018-7600	RCE
9	Telerik	CVE 2019-18935	RCE
10	Microsoft	CVE-2019-0604	RCE

source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-209a

70% of the top ten routinely exploited vulnerabilities are Remote Code Executions (RCE)

Mitigating Risk - 2022 MITRE Top 25



Why Invest in Application and Workload Protection

1. **Prevent interruptions** to customer services and business processes.
2. **Save up to $9.4 million** within three years.
3. **Reduce risk** and comply with NIST, CISA, PCI, CIS compensating controls.
4. **Reduce alert fatigue** to the Ops, SOC and App teams.
5. **Extend Zero Trust with enforcement** of authorized application dependencies and their host environments at runtime.

Add Protection to Detect and Respond

Enhancing Your Security Posture

- **Positive security posture** to protect application workloads – no implicit trust.
- Prevent sophisticated malware, ransomware and data breach **zero-day exploits** of known, unknown, unpatched, and legacy vulnerabilities.
- Increase **operational efficiencies** by 90% with less false positives hitting the SIEM and SOC teams.
- Prevent **data loss** to cyber criminals and other bad actors.
- Extend defense in depth with an added security layer that is **independent of identity** or perimeter security

Value Drivers – Protecting Open Attack Surfaces

Virsec leverages security controls that embrace a modern automated “allowlisting” approach — permitting only known good code (executables, libraries, and scripts) to run. All other code is explicitly denied execution — eliminating dwell time and stopping zero-day attacks before exploitation can occur.

Protect Mission-Critical Workloads

Backstop protection against zero-day, RCE, ransomware and software supply chain vulnerability exploits to ensure business continuity and avoid the cost of a breach.

Legacy System and Workload Protection

Protect vulnerable **out-of-support** applications and host OS workloads **open attack surfaces** against modern cyber attacks. Virsec’s platform protects legacy systems like RHEL 6, Microsoft 2003, 2008, or 2012. Reduce the need for “best effort” patching and maintenance contracts.

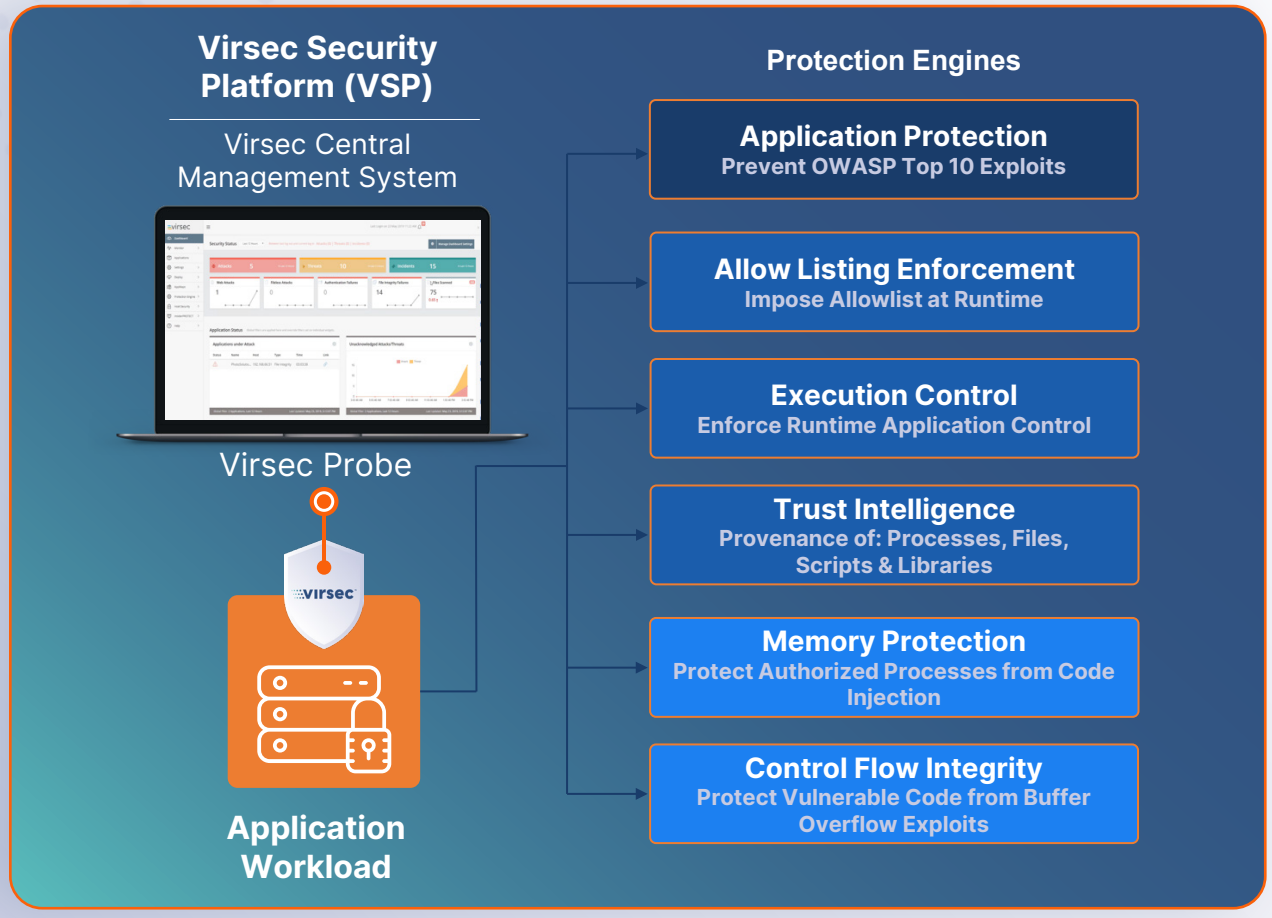
Continuous Shielding for Unpatched Vulnerabilities

Take proactive steps to thwart cyber criminals from **exploiting unpatched vulnerabilities**. Prevent Remote Code Execution (RCE), Living-off-the-Land and Cross-Site Scripting threats.

NIST Based Security Controls

Zero Trust Application & Workload Protection

Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53r5)



- Security & Privacy Controls
- Trustworthiness & Assurance
- Control Implementation

source: https://nvlpubs.nist.gov/nistpubs/Special-Publications/NIST.SP.800-53r5.pdf

Summary Customer Value

Protect Mission-Critical Workloads

3-Year Impact
$3.5 M

Legacy System and Workload Protection

3-Year Impact
$3.2 M

Continuous Shielding for Unpatched Vulnerabilities

3-Year Impact
$2.7 M

$9.4 M
Saved within 3 Years

Keep reading to explore how the savings are realized...

Protect Mission-Critical Workloads

Saved $3.58 million through cost avoidance

Metric	Cost Element	Source	Year 1	Year 2	Year 3	Total
D1	Average global cost of a data breach	Ponemon, IBM	$4.4M	$4.4M	$4.4M	
D2	Probability of a large data breach	Ponemon, IBM	27%	27%	27%	
D3	**Savings from preventing data breaches**		**$1.188M**	**$1.188M**	**$1.188M**	**$3.56M**

- **Take the average $4.4 million-dollar cost of a global breach and 27% as the probability that it will occur.**
- **Treat malware, ransomware and data breaches as being equal exploits with similar potential impacts.**
- **Additional impact avoided: paying the ransom, compliance penalties, lost customer business, lost employee productivity.**

Legacy System & Workload Protection

Microsoft Windows 2003, 2008, 2012

- **Legacy applications and host operating system (OS) workloads present a sizable attack surface for cyber criminals and nation-state organizations to find and exploit known vulnerabilities.**
  - » **75% of attacks in 2020 used vulnerabilities that were at least two years old.***

- **The alternatives to organizations are limited :**
  1. **Do nothing, play the odds that you're lucky.**
  2. **Pay significant amounts of money for Extended Security Updates (ESUs) and out-of-support patches.**
  3. **Partner with Virsec for vulnerability shielding and hardening techniques.**

* Source: Checkpoint Cyber Security Report

Protect Legacy Applications and Host Workloads

Save $3.2 Million and Reduce Risk

Metric	Cost Element	Source	Year 1	Year 2	Year 3	Total
A1	Microsoft fees for a special release	Customer	$246,749	$370,124	$431,811	
A2	Number of out-of-support servers	Customer	100	150	175	
A3	Average global cost of a data breach	Ponemon, IBM	$4.4M	$4.4M	$4.4M	
A4	Probability of a large data breach	Ponemon, IBM	27%	27%	27%	
A5	**Savings from preventing data breaches**		**$1.069M**	**$1.069M**	**$1.069M**	**$3.207M**

* Server pricing model - $3,289

Continuous Shielding for Unpatched Vulnerabilities

- Virsec Security Platform (VSP) proactively monitors applications and host OS workloads allowing human capital to be allocated to high potential incidents.
- Reduction in false positives generated – estimate 90%.
  - The positive security model (deny all) allows authorized application dependencies to execute at runtime without generating significant false positives.
  - The negative security model (allow all) generates large volumes of false positives as it attempts to match known behavior patterns.
- Reduction analysis of vulnerability scans – estimate 90%.
  - VSP incidents are precise and accurate, eliminating the need for deep analysis of low probability incidents.

Continuous Shielding for Unpatched Vulnerabilities

Save $2.7 Million and Reduce Alert Fatigue

Metric	Cost Element	Source	Year 1	Year 2	Year 3	Total
B1	Number of Security Incidents – false positives	Customer	20,000/mth	35,000/mth	50,000/mth	
B2	% Reduction after Virsec Security Platform	Observed	90%	90%	90%	
D1	Average hours to analyze – false positives	Customer	0.32	0.32	0.32	
D2	Number of hours saved per year	Observed	5,760	10,080	14,400	
D3	**Productivity gains**	**$85 / Hour**	**$525,600**	**$919,800**	**$1.314M**	**$3.207M**

How Virsec Strengthens

Defense in Depth for Applications and Workloads

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.

Automated Allowlisting and Application Control

Virsec's approach strikes the right balance between granular control and ease of use, eliminating hours of manual effort in managing allowlists.

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

[1]Gartner, Market Guide for Cloud Workload Protection Platforms, 12 July 2021, Neil MacDonald, Tom Croll.

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**.