virsec™

How to Extend Zero Trust to Server Workloads

Protect against tomorrow's Zero Day attacks today

Protecting Server Workloads is a Unique Challenge

- Increasing Sophistication
- Relentless Ransomware
- Zero-Day Attacks
- Supply-Chain Attacks

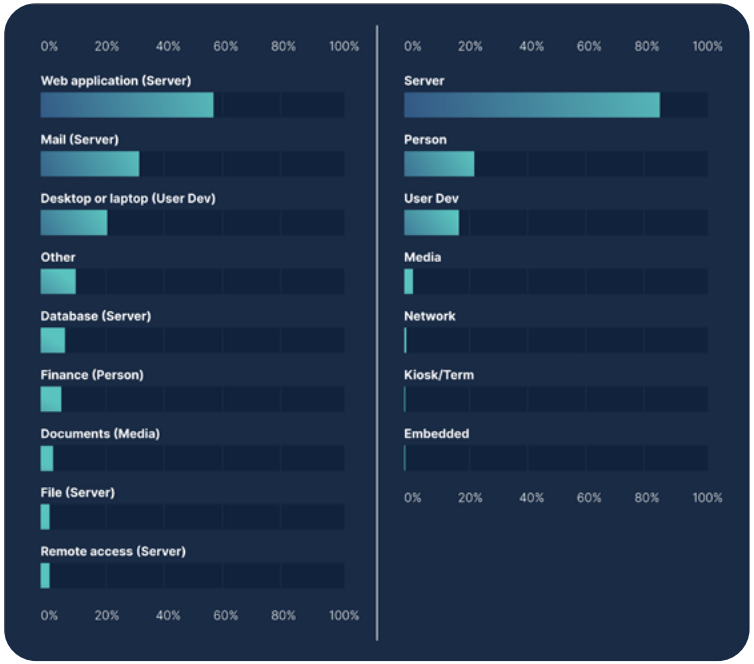
Modern workloads for most organizations typically comprise hundreds of systems executing across multiple cloud and on-premises environments, including virtual machines (VMs) and containers. Protecting dynamic and complex environments is increasingly more critical as advanced attacks target these crown jewels.

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

Zero-day attacks have become a cause for great concern as unpatched systems are increasingly targeted by cybercriminals due to their high level of vulnerability. Remote Code Execution (RCE) is a common attack vector used as existing cybersecurity tools have not been able to adequately guard against it.

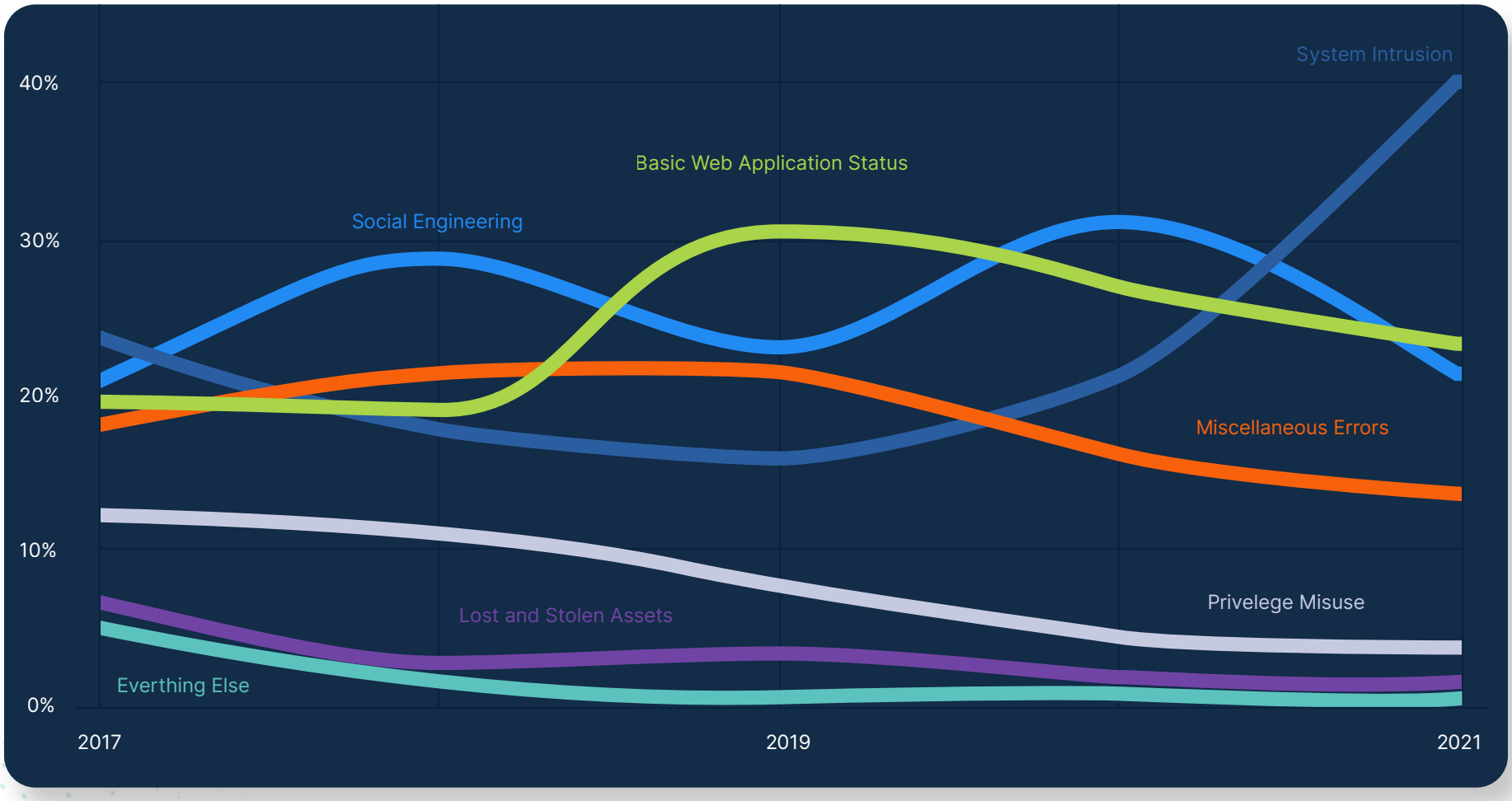
The 2022 Verizon Data Breach Investigations Report shows that attacks on servers dominate compared to those on user accounts and client devices. Furthermore, the report also shows that attacks on web application servers outpace any other asset type.

Servers and their Web Applications are Major Breach Targets



Top Assets and Varieties in Breaches
Source: 2022 Verizon Data Breach Investigations Report

System Intrusions are Trending Upward

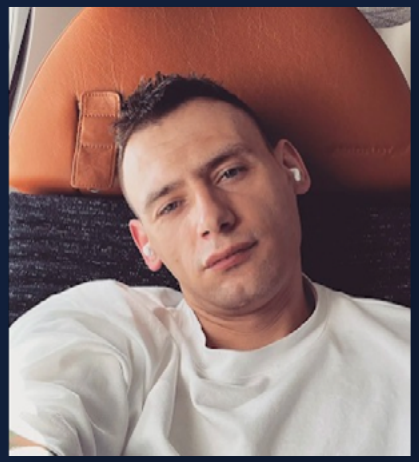


Source: 2022 Verizon Data Breach Investigations Report

12 of the Top 20 Nation State Actors and Cyber Criminals Prefer Remote Code Execution (RCE)

Vendor	CVE	Vulnerability Type
Apache Log4j	CVE-2021-44228	Remote Code Execution
Pulse Connect Secure	CVE-2019-11510	Arbitary File Read
GitLab CE/EE	CVE-2021-22205	Remote Code Execution
Atlassian	CVE-2022-26134	Remote Code Extecution
Microsoft Exchange	CVE-2021-26855	Remote Code Execution
F5 Big-IP	CVE-2020-5902	Remote Code Execution
VMware vCenter Server	CVE-2021-22005	Arbitary File Upload
Citrix ADC	CVE-2019-19781	Path Traversal
Cisco Hyperflex	CVE-2021-1497	Command Line Execution
Buffalo WSR	CVE-2021-20090	Relative Path Traversal
Atlassian Confluence Server and Data Center	CVE-2021-26084	Remote Code Execution
Hikvision Webserver	CVE-2021-36260	Command Injection
Sitecore XP	CVE-2021-42237	Remote Code Execution
F5 Big-IP	CVE-2022-1388	Remote Code Execution
Apache	CVE-2022-24112	Authentication Bypass by Spoofing
ZOHO	CVE-2021-40539	Remote Code Execution
Microsoft	CVE-2021-26857	Remote Code Execution
Microsoft	CVE-2021-26858	Remote Code Execution
Microsoft	CVE-2021-27065	Remote Code Execution
Apache HTTP Server	CVE-2021-41773	Path Traversal

Source: https://www.cisa.gov/uscert/ncas/alerts/aa22-279a



Wazawaka

Leader of Russian Ransomeware Gang "Babuk"

DS: How do you access networks?

MM: I took everything from GitHub. As they say, made from shit and sticks. The first interesting exploit was Fortinet, and then a **very old vulnerability in a SharePoint** application. Then there was Sonic Wall. In general, I have always tried to get initial access from RCE (remote code execution). I have tried buying logs from RedLine stealers. **But the best entry point is given by RCE.**

Source: https://therecord.media/an-interview-with-initial-access-broker-waza-waka-there-is-no-such-money-anywere-as-there-is-in-ranswomware

What Exactly is Zero Trust?

Let's look at the definition of Zero Trust.

"Zero Trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated."

— NIST, Zero Trust Architecture, Special Publication 800–207

"Zero Trust advocates these three core principles: all entities are untrusted by default, least privilege access is enforced, and comprehensive security monitoring is implemented."

— Forrester Research, The Definition of Modern Zero Trust, January 2022

The bottom line is that **most server workloads today allow too much implicit trust.** And Zero Trust is more than networks and infrastructure. It can, and should, be applied to server *workloads* as well.

Key Zero Trust Execution Requirements

Authorized Processes, Libraries, and Dependencies

Zero Trust for Memory Protection

Ensure that the process memory of legitimate applications is not tampered with to inject malicious code or fileless malware onto the system.

Stop process injection techniques including but not limited to process hollowing, process Doppelgänging, and ptrace injection. Additionally, stop methods that involve stealing critical workload data like credentials from memory dumping of OS processes.

Zero Trust for Software Supply Chain

Establish the provenance, integrity, and authority of software and its executables and libraries.

This provides visibility into every component of an application workload — similar to Software Bill of Materials (SBOM) — creating an authorized list to allow the execution of known good components and blocking anything else that is not authorized.

Zero Trust for Runtime Code

To protect runtime code with zero-trust principles requires monitoring the control flow of process execution in runtime and identifying any deviations.

This method first captures an application's sequence of instructions and their traversal in memory from the compiled code, providing a finite map of what the executable is supposed to do. It then monitors actual execution at runtime and prevents any execution that deviates from this map.

Key Zero Trust Application Workload Protection Requirements

Zero-Day Protection with Zero Dwell Time

Zero Trust for Executables

Only allow validated and approved executables (processes, libraries and scripts) to run on a server.

Methods to verify legitimacy could be file metadata and reputation to ensure the creation and enforcement of a baseline — much like (Software Bill of Materials) SBOM enforcement. Also, connecting with Threat Intelligence services to verify legitimacy of files on the workloads and automatically allow-list files that are known good.

Zero Trust for Living-off-the-land Binaries

Prohibit known living-off-the-land binaries (lolbins) such as PowerShell and Bash, which are not required on specific production workloads.

Additionally, and crucially, provide fine-grained control for allowed lolbins, like execution prevention of other files, restricting commonly abused command line parameters or enforcing rules to allow/deny process parents, user access control, and more.

Zero Trust for File System Access

Prevent unauthorized activity and tampering by continuously monitoring files for:

- Creation
- Modification
- Permission change
- Deletion

VIRSEC OFFERS THE INDUSTRY'S FIRST

Zero-Trust Platform for Server Workload Protection

Virsec's groundbreaking approach delivers the highest levels of protection, with **zero dwell time** and **low false positives.**

Virsec leverages security controls that embrace a modern automated "allow listing" 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.

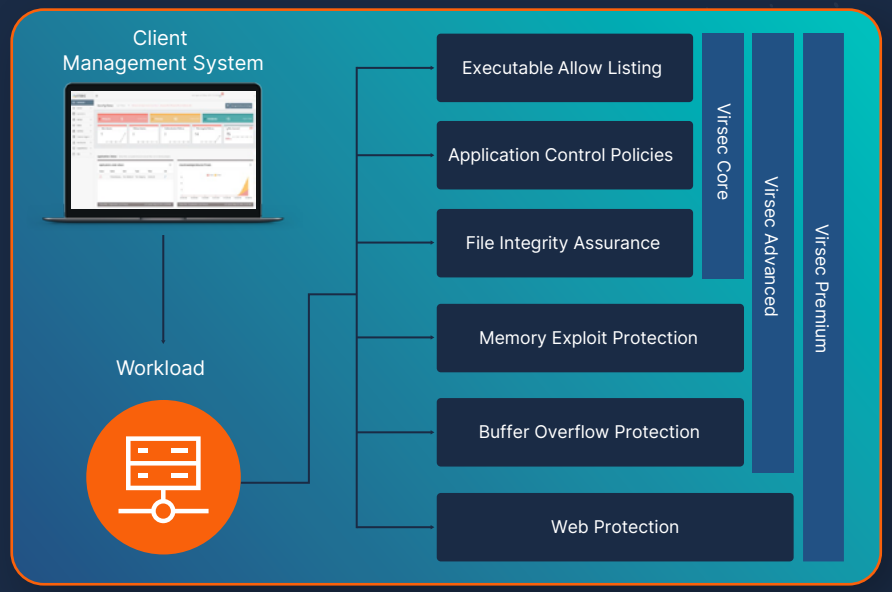
- Stop known and unknown attacks
- Protect servers, even unpatched and legacy systems
- Reduce dwell time to zero
- Lower false positives
- Better performance than other security solutions

Behavior-based solutions rely on stopping the known bad but struggle with the large set of unknown executables. This **"default allow"** approach assumes implicit trust (the opposite of Zero Trust).

Virsec's approach adopts a **"default deny"** policy that only allows known good code to execute and stops everything else. That's true Zero Trust.

The Virsec Security Platform (VSP) Protection Stack

The Virsec Security Platform (VSP) Enables Critical Capabilities



Executable Allow Listing

- Establish and enforce system-wide allow-listing for processes, libraries, and scripts based on trustworthiness
- Establish trustworthiness by verifying the pristineness based on trusted publishers and reputation based on our reputation database
- Monitor deviations in run-time and mitigate any instances of modified or added executables

Application Control Policy

- Enforce dynamic execution control on allow-listed processes to stop living-off-the-land attacks
- Block malicious activities from the otherwise trusted operating system-related process
- Enforce parent-child process controls to stop RCE and lateral movement

File Integrity Assurance

- Monitors critical application folders and directories for file I/O activity
- Reports any changes in access privileges and file ownership in the monitored folders

Memory Exploit Protection

- Stops process injection techniques including, but not limited to, Code Injection, Process Hollowing, and Process Doppelgänging
- Stop dumping OS credentials from the memory of key processes like LSASS
- Stop privilege escalation attacks like dirtypipe, dirtycow and in-memory attacks on Linux servers
- Exploit techniques are detected and stopped in real time without the need for any signature, learning, or customization

Buffer Overflow Protection

- Detect 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 enforcing any deviation during runtime

Web Protection

- Web Application & API Protection for attacks coming via http/https channel
- Detects OWASP Top 10 Attacks on protected web applications using deep instrumentation of application frameworks and/or web servers
- Blocks Web-based attacks by examining the HTTP payloads and resulting transactions in the application

Battle-Tested by the Department of Defense

Validation

2021 Spring Red-Team Test

218 Ethical Hackers, broken into seven teams

VS

virsec™

- **14.5K** Hacking Attempts
- **0.0** Successful RCE, after 79 attempts
- **100%** Perfect score by Virsec

Endorsed by Industry Leaders

Andy Nallappan
Chief Technology Officer

BROADCOM

"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."

John Desimone
Vice President, Cyber

Raytheon

"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."

Norm Messenger
Chief Security Officer

inspirage

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

Extend Zero Trust to your Server Workloads

- Stop known and unknown attacks
- Protect servers, even unpatched and legacy systems
- Reduce dwell time to zero
- Lower false positives
- Better performance than other security solutions

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.

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.

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.