virsec™

Ensure Continuous Patient Care: How to Avoid Disruptions Due to Ransomware, Malware, and Data Breaches

Stop tomorrow's Zero-Day attacks today

Healthcare Organizations Face Unprecedented Cyberattacks

Increasing pace of ransomware, zero-day, and remote-code execution attacks

It is no secret that Healthcare Providers are being targeted at an alarming rate by ransomware attacks. Due to the critical nature of health systems, attackers know they are more likely to have their ransom demands met.

> "Ransomware attacks targeting healthcare delivery orgs. doubled from 2016 to 2021."
>
> **-2022 Healthcare Cybersecurity Year In Review, Health Sector Cybersecurity Coordination Center (HC3)**

Zero-day attacks have become a cause for great concern as unpatched systems are increasingly targeted due to their high level of vulnerability.

Remote Code Execution (RCE) is another common attack vector used as traditional cybersecurity tools have not been able to adequately guard against it.

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

Virsec Protects Healthcare Applications and Assures Timely Patient Care

Zero Trust Workload Protection helps to:

- Minimize Disruption to Patient Care
- Improve safety record
- Meet regulatory requirements
- Protect revenue and reputation
- Alleviate patch management
- Keep legacy applications running securely
- Stop ransomware and malware in milliseconds and avoid millions of dollars in data breach costs

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

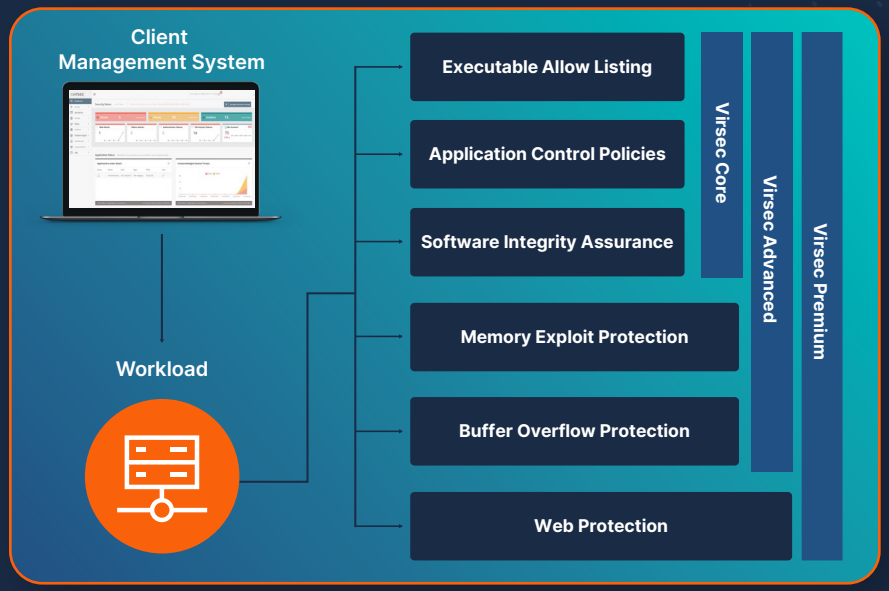
- Enforce dynamic execution control on allow-listed processes to stop living-off-the-land attacks
- Block malicious activities from the otherwise trusted operating system-related process
- Enforce parent-child process controls to stop RCE and lateral movement

Software 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



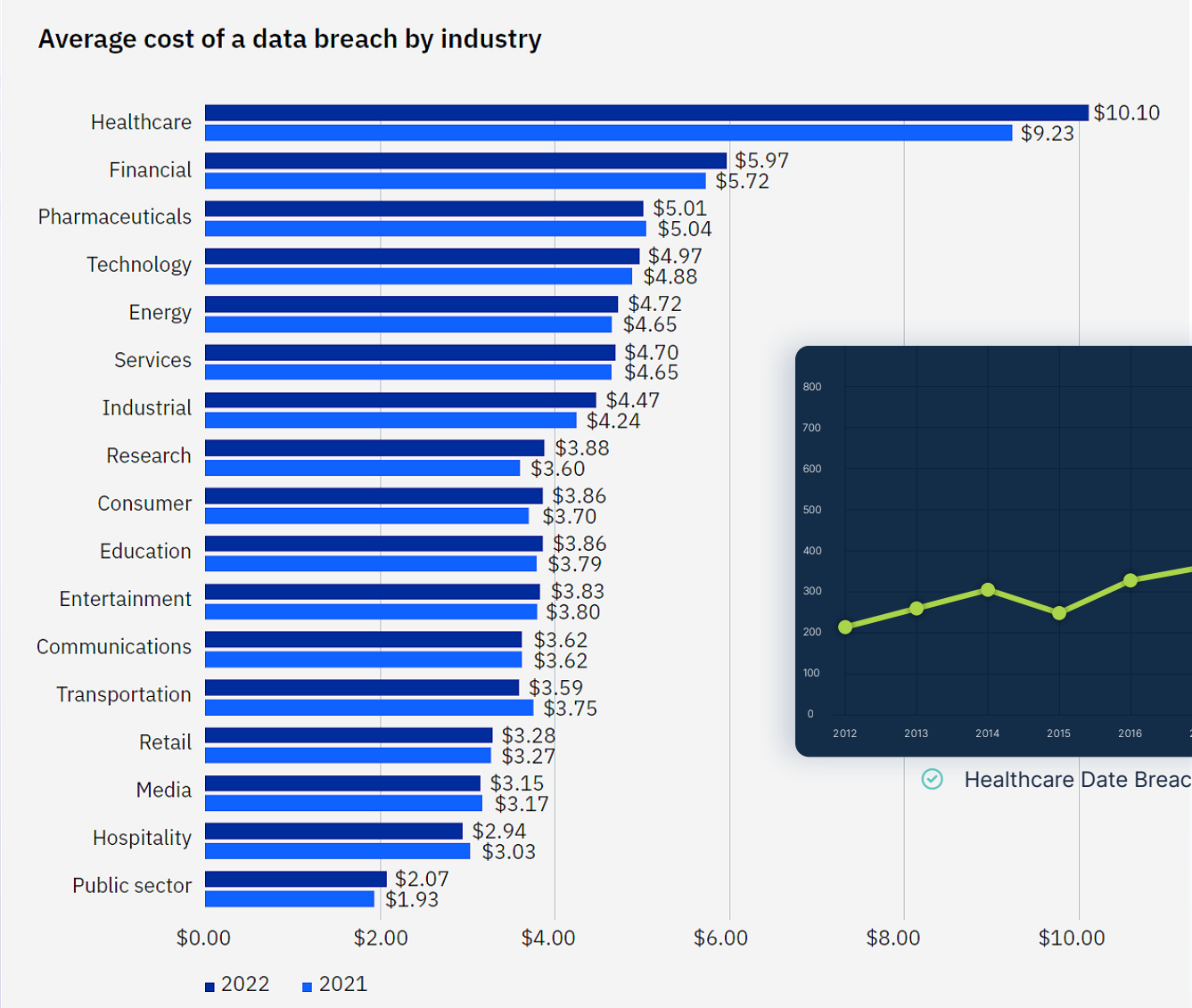
Buffer Overflow Protection

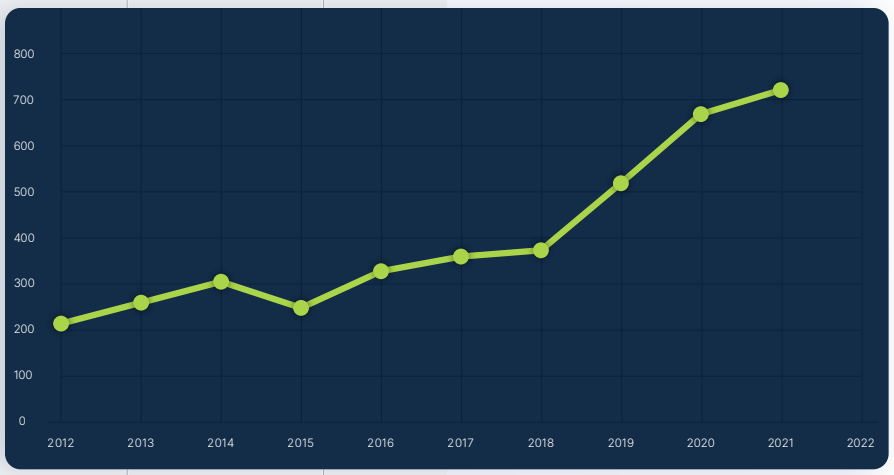
- Detect memory-based attacks such as buffer overflows, return-oriented programming, and other blind attack schemes on program flow, memory stack, and return addresses
- Protects runtime execution of pre-compiled applications by automatically extracting the control flow for every executable, and enforcing 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

Healthcare Data Breaches Rising and Cost More



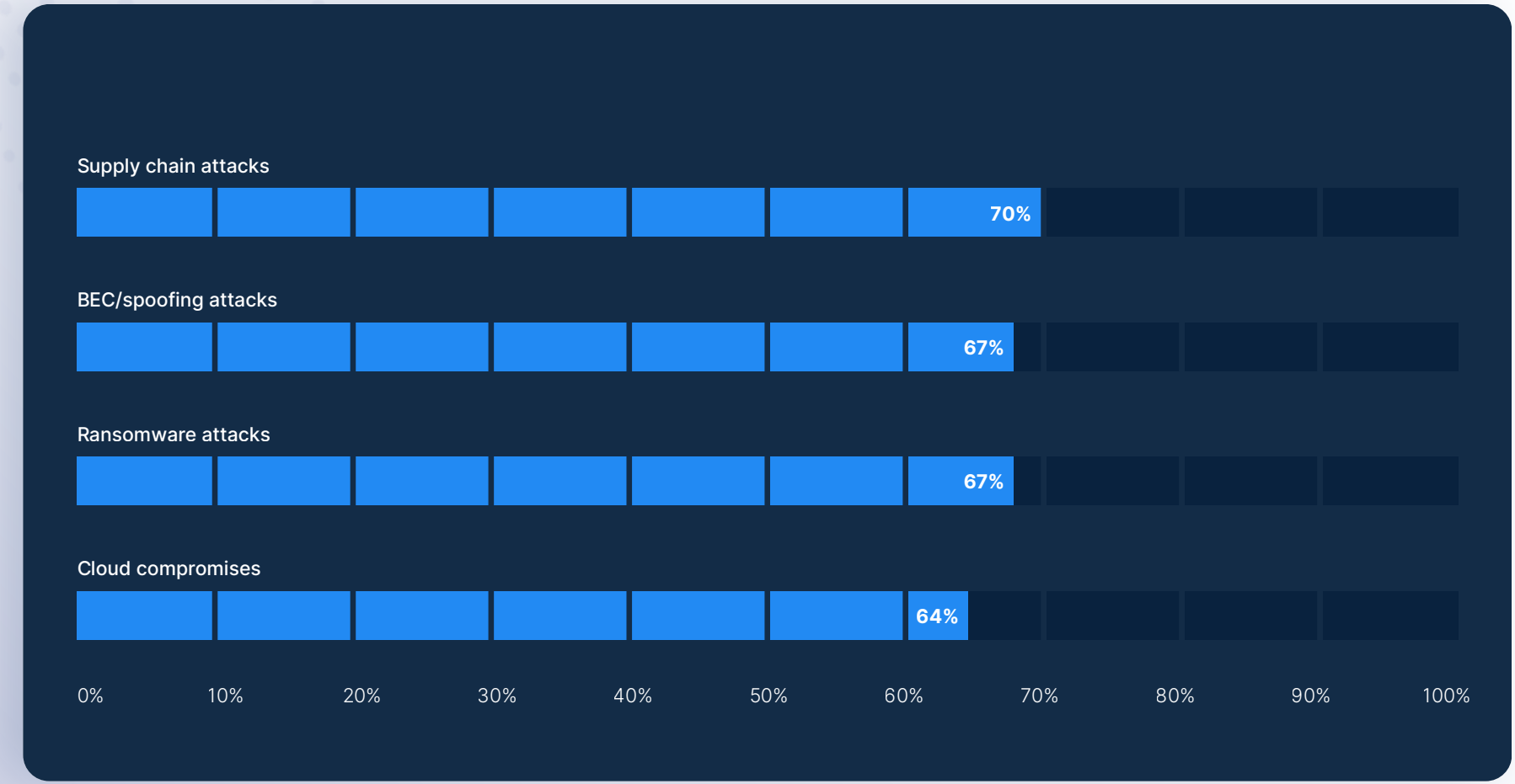


Healthcare Date Breach Costs Trending Upward

Source: IBM, and BankInfoSecurity

Cyberattacks Have Disrupted Care, Increasing The Risk To Patients

Top Cyberattacks That Have Disrupted Patient Care



Source: Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care by Ponemon Institute

Impact Of Cyberattacks On Patient Care

Delays in patient care, loss of revenue, and increase in complications and lives lost

Source: Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care by Ponemon Institute

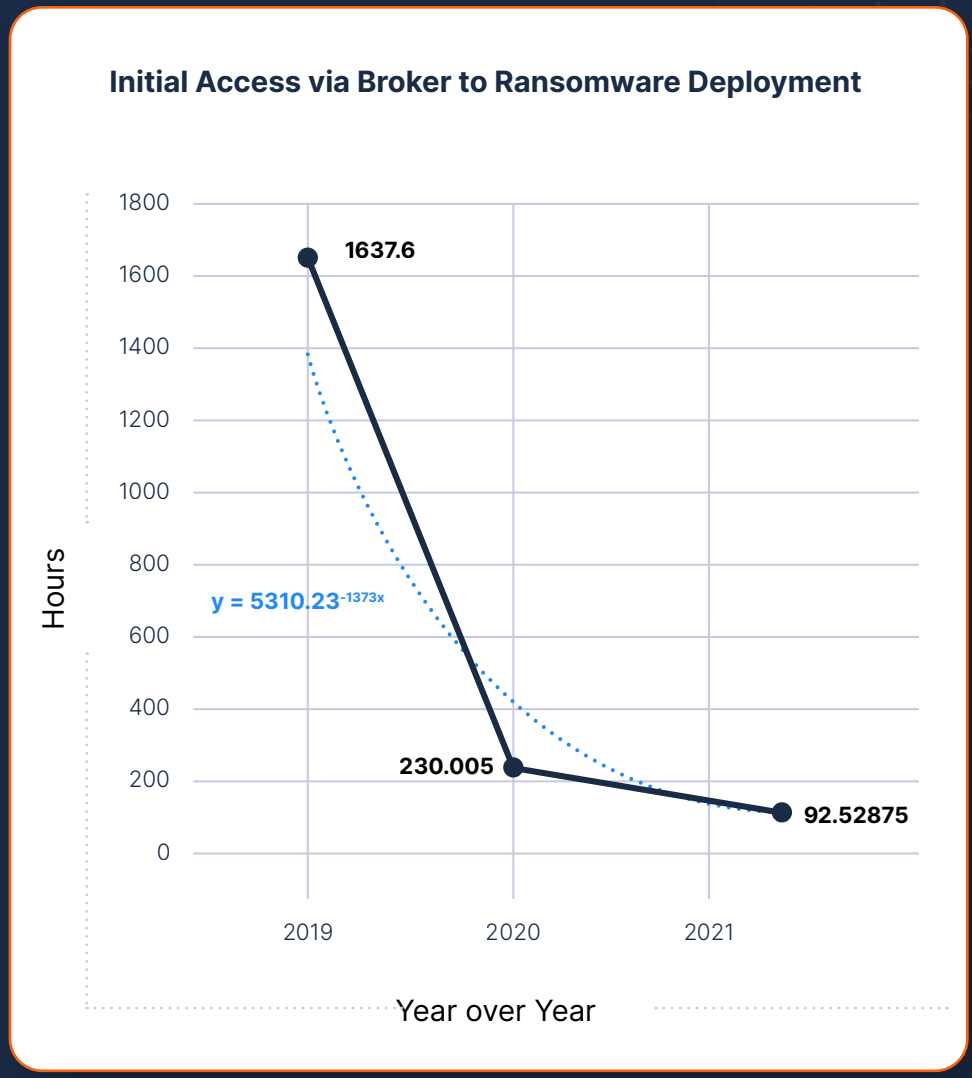
Ransomware Time-to-Encrypt Getting Worse

Patient care and EHR systems targeted with sophisticated attacks leading to faster encryption

The speed with which attackers can discover and encrypt systems is putting organizations at even greater risk.

According to IBM, ransomware attacks need less than four days to encrypt systems on average.

Furthermore, we have already seen attacks that can compromise data within 30 minutes, e.g. the QBot malware discussed in more detail later in this eBook.



Source: IBM SecurityIntelligence
https://securityintelligence.com/posts/analysis-of-ransomware/

Expanding Healthcare Regulations for Cyberattacks

New laws to require rapid response and reporting

The White House signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

This new law is applicable to public and private health organizations; once the proper standards are developed, the following will be in effect:

- Critical infrastructure entities must report cyberattacks to CISA **within 72 hours of discovery.**
- Critical infrastructure entities must report ransomware payments made **within 24 hours.**

The seven requested items include:

- **Description of the incident**
- **Description of the vulnerability**
- **Security defenses maintained**
- **Tactics, techniques, and procedures**
- **Compromised information**
- **Contact information for a covered entity**

CISA's CIRCIA website: https://www.cisa.gov/circia

Source: 2022 Healthcare Cybersecurity Year In Review, Health Sector Cybersecurity Coordination Center (HC3)

Solve Healthcare's Toughest Cybersecurity Challenges

PROTECT AGAINST RANSOMWARE BREACHES

Proactively prevent advanced attacks from exploiting breaches and corrupting server workloads.

PROTECT LEGACY AND OUT-OF-SUPPORT APPLICATIONS AND WORKLOADS

Reduce vulnerable attack surface by securing workloads even if they are no longer receiving security updates, and without needing access to the source code.

ELIMINATE PANIC PATCHING

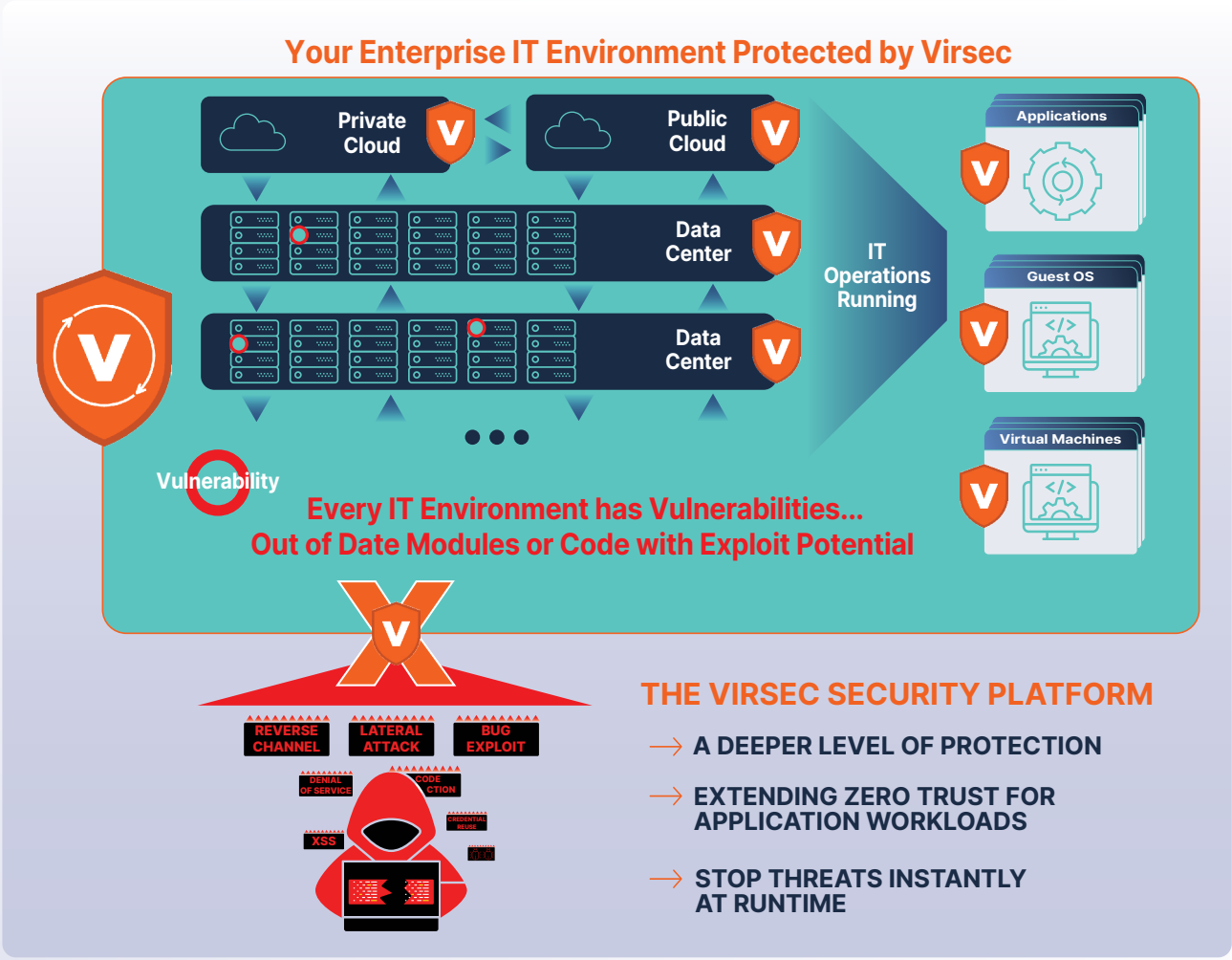
Shift from a reactive to a proactive approach to patch management, applying patches on your schedule thus allowing for a thorough test and deployment process.

Protect Against Ransomware Breaches

Virsec Security Platform (VSP) stops attacks in milliseconds, preventing attackers from leveraging vulnerabilities to take control and run malicious code. It enables organizations to protect critical workloads **at runtime with very high efficacy, thus also drastically reducing false positives.**

VSP proactively protects against ransomware and malware exploits with VirsecMap, which defines the executable allow list of what is authorized (system integrity), and VirsecEnforce which dynamically enforces that the software executes as expected (runtime protection). With a protection-first approach to zero trust, Virsec's approach of allowing only 'known good' dependencies such as files, scripts, and libraries to run, stops all other malicious behaviors regardless of 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.**

VSP continuously monitors file systems, registries, scripts, and processes to ensure the system integrity of applications and workloads. It verifies that 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. VSP also prevents lateral progress in the event chain by **blocking unauthorized code execution on host operating systems (OS).**



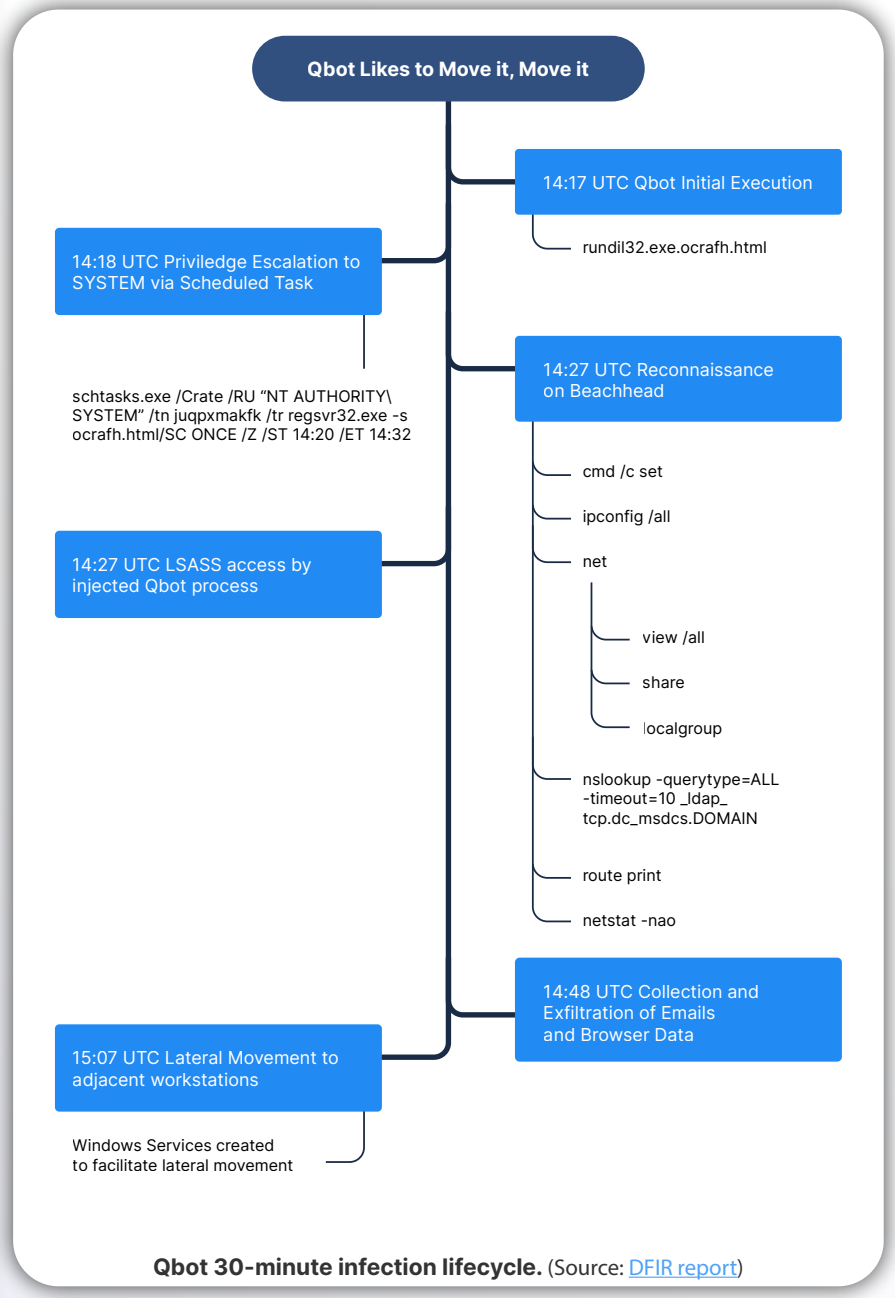
Qbot Malware Infects Healthcare Organizations in 30 minutes

Virsec prevents Qbot infection in milliseconds

- DFIR released an analysis noting that Qbot can compromise data within 30 minutes of initial infection.
- Qbot has been used aggressively to target the U.S. healthcare sector.
- Qbot is often used in multi-stage attacks, and to drop ransomware.

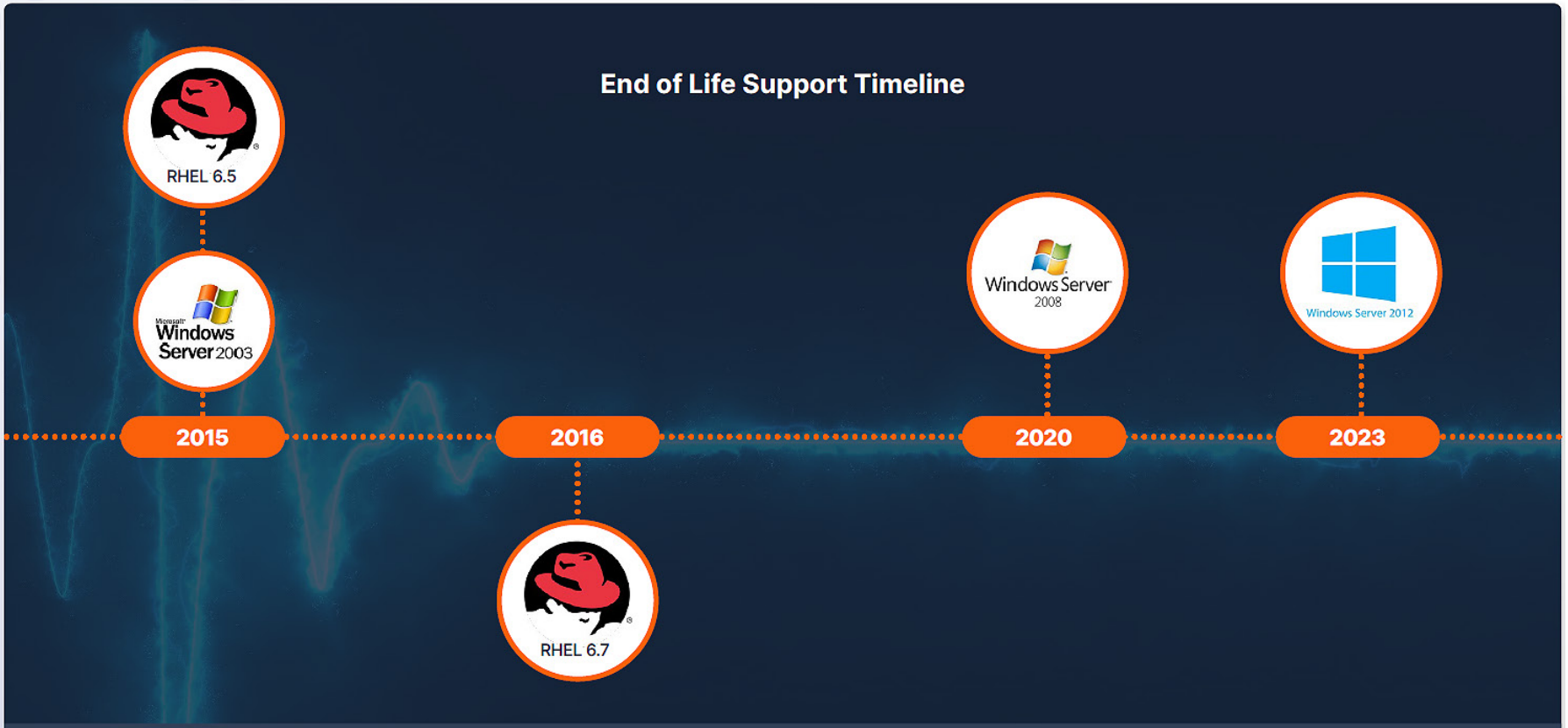
Virsec stops Qbot at the very first stage of the attack by:

1. Detecting the DLL Qbot is trying to inject onto the system and recognizing that is not a known file does not have good provenance.
2. A Positive Model ACP Policy in Virsec would deny Powershell execution



Qbot 30-minute infection lifecycle. (Source: DFIR report)

Protect Legacy and 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

Typical Legacy Workload Security Challenges include:

- Support has slowed or ceased with obsolescence or vendor is charging very high fees to support end-of-life products
- 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
- Digital transformation is an arduous process taking months or years to complete as risk remains

How Virsec Protects Legacy Workloads

Virsec Security Platform allows you to protect applications running in Windows Server 2003, 2008 R2 SP1, 2012, Red Hat Enterprise Linux or CentOS 6.5, 6.7, 6.10, and SUSE 12 with strict application controls and runtime analysis. It covers vulnerabilities exposed due to the time between patching and will act as a patch-bridge for Windows Server between upgrades. The implementation will continuously protect the entire software stack across all runtime components, including files, executables, processes, and libraries that allow attacks to build in memory as systems execute.

Eliminate Panic Patching

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.

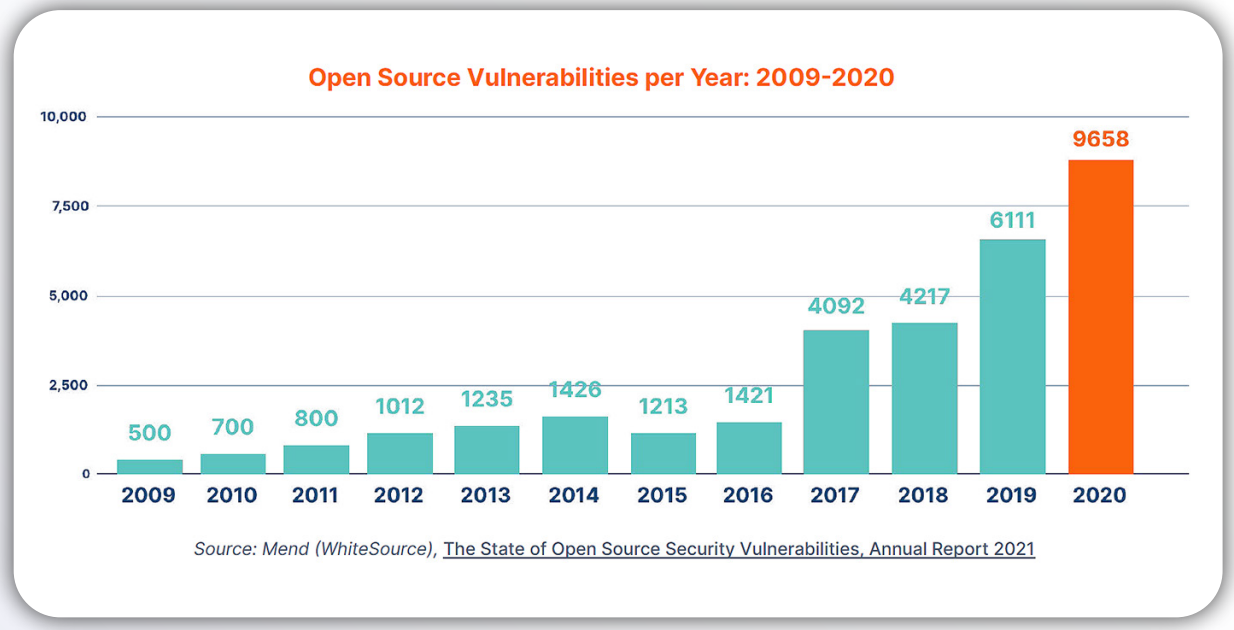
How Virsec Alleviates Panic Patching

Server Hardening

With automated allow listing and granular application control policies, server workloads are protected from external attempts to inject malicious code or hijack processes or files until the patch can be deployed.

Automatically Contain the Vulnerability

Stop lateral move through cross-site scripting (stored XSS) to prevent infiltration and weaponization.



Patch on Your Terms

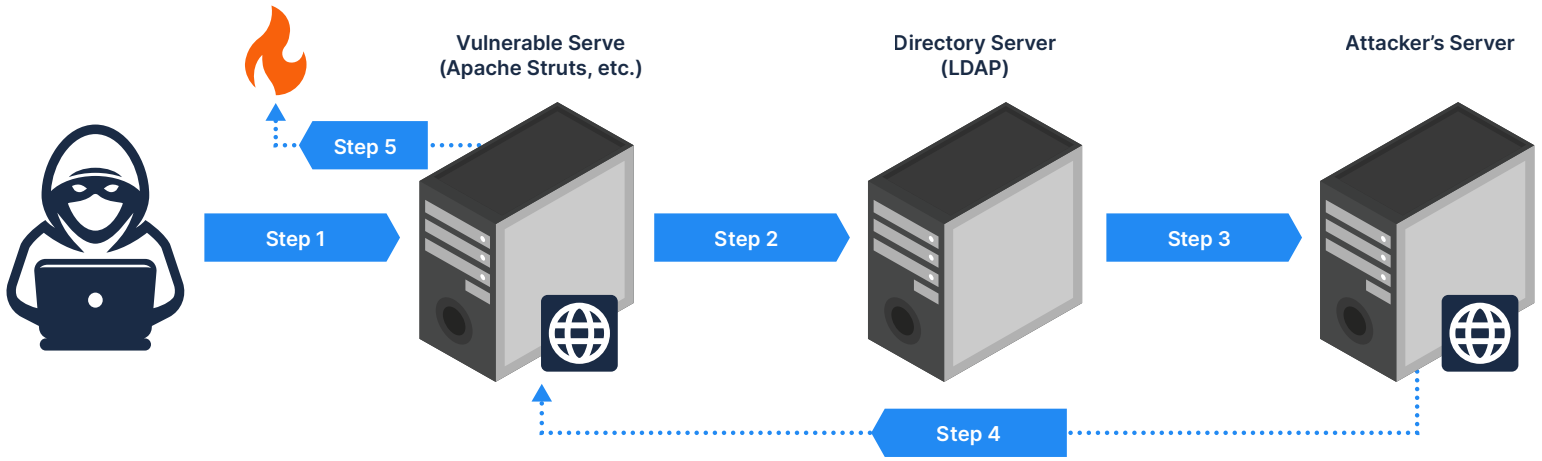
Avoid panic patching due to a critical security incident knowing only authorized applications, dependencies, and bills of materials of processes and files will be enforced at runtime. Patch once analysis, testing and deployment plans are fully vetted.

Application Visibility

With auto-discovery of applications IT and Security organizations now have insights into which applications are running on server workloads for risk assessment and prioritization.

Log4J Vulnerability for Healthcare Applications

Virsec Stops Log4J Attacks on Unpatched Systems



How Virsec Stopped Log4J Attacks

- The first malicious action occurs at **Step 3** as the LDAP Server reaches out to the attacker's server. Virsec identifies that as an RFI vulnerability.
- At **Step 4**, the response from the bad actor server triggers a malicious java class to get loaded. Virsec detects this malicious class load directly into memory.
- Once the malicious class gets loaded in memory, it could unleash more file-based or fileless malware. Virsec Security Platform for Host, otherwise known as, VSP-Host (Process Monitoring and ACP Engine), stops those attacks without even one instruction from such malware executing.

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

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.