virsec™

Stop Ransomware and Zero-day Attacks with True Runtime Protection

In the second half of 2021, ransomware complaints to the FBI were up 62% from the same period in 2020.[1] Many ransomware attacks go unreported to Federal law enforcement.

- **Cybersecurity budgets continue to grow year over year, but are we safer?**
- **Why is Ransomware still on the rise?**
- **Can we fully protect ourselves from Zero-day attacks?**

Here, we'll examine some of the key factors that contribute to the rise of ransomware attacks, as well as recent initiatives and innovations that enable defenders to better mitigate risk and stop attacks before they start.

Ransomware is Big Business

If Ransomware were a Silicon Valley start-up, it would be considered a “Unicorn”: high growth, high reward, low risk, minimal competition. Ransomware techniques are often successful, and the perpetrators are rarely prosecuted. When combined with the emergence of Bitcoin and other cryptocurrencies as means of payment, cybercriminals are difficult to trace. As a result, ransomware attacks are escalating and becoming more sophisticated and elusive.

Cyber extortion is now an official **multi-billion-dollar industry.**

In 2021, for the first time, attackers were successful in shutting down critical infrastructure in the U.S., including Colonial Pipeline, the East Coast’s largest gasoline, diesel, and natural gas distributor, and JBS, the world’s largest meat processor.

Initial demands for payment are reaching new heights—exceeding 10 million dollars and sometimes as high as 40 to 60 million—**for targets with deep pockets.**[2]

The Democratization of Ransomware

Trends are emerging around ransomware-as-a-service (RaaS), unlocking additional sources of revenue for a host of participants in this underground economy. Highly skilled cybercriminals develop and sell their capabilities to malicious actors who don’t have the resources to develop these tools independently.

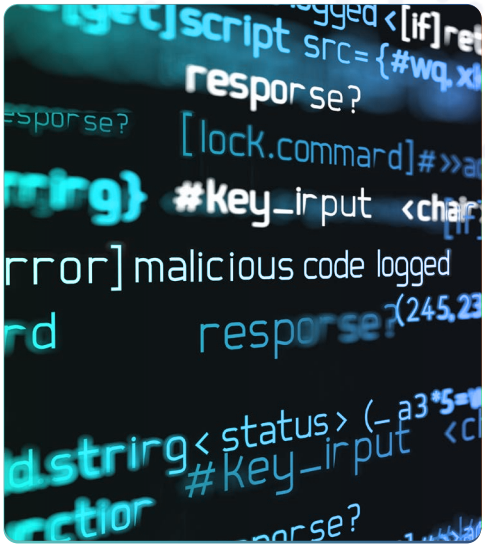
One way to think of it would be as a **pyramid scheme of cyber extortion**—those that provide encryption tools, communications, technical support, training, and ransom collection—now share in the profits and the success of those who leverage their expertise and infrastructure. Mature models already exist in the underground: pure profit sharing, monthly subscription fees, one-time licensing fees, etc.

In short: Ransomware is a burgeoning business with hierarchies, sophisticated reporting and collection methods, encrypted sharing of data, etc.

Costs, Beyond the Ransom

The total financial impact of successful attacks on an organization is staggering. Collective global ransomware costs to businesses for 2021 **are estimated to exceed $20 billion.**[3]

In a year when the average total cost of a data breach increased by nearly 10% ransomware breaches jumped even higher, now exceeding $4.62 million, **costlier than any other type of breach.**[4]



Milliseconds Matter

The average ransomware attack takes 3 seconds from the time an adversary initiates a ransomware attack. Leveraging a wide range of techniques to break into systems, hackers can gain access to sensitive data, escalate privileges, hijack operations, deploy encryption tools and encrypt data before demanding a ransom. All of this can happen with pre-written scripts—in seconds.

Even with today's latest cyber tools, more than 75% of organizations infected with ransomware are using endpoint protection products (EPP) or endpoint detection and response (EDR) tools that they believe could help mitigate risk.[5] However, EPP/EDR tools are not fully equipped to protect against ransomware that can bypass conventional, probabilistic tools like these.

One thing becomes clear: tactics based on endless threat chasing, attempting to guess the adversary's next move based on their last one, and trying to seal off ever-shifting perimeters **continue to prove inefficient.**

The Defender's Dilemma: To Pay or Not to Pay?

For some government agencies, the decision to pay or not to pay may soon be out of their hands. New York, North Carolina, and Pennsylvania are considering legislation that would ban state and local government agencies from paying the ransom. They argue that prohibiting payments would deter attacks. But some experts point out that attacks will still happen as cybercriminals aren't going to research state laws and back off accordingly.

Restoring and rebuilding systems could prove more costly and time-consuming, particularly for smaller local governments. Instead of inadvertently further penalizing victims, providing aid to enable better protection is a more effective approach.[6] Many cities are underfunded, but often struggle to retain skilled cybersecurity talent — even if the budget is there.

The Role of Cyber Insurance

Cyber insurance is becoming an increasingly popular risk mitigation strategy. Most policies cover costs to investigate a ransomware attack, negotiate with hackers, and make a ransom payment. So, it comes as no surprise that the number of companies opting for cybersecurity coverage grew from 26% in 2016 to 47% in 2020.[7]

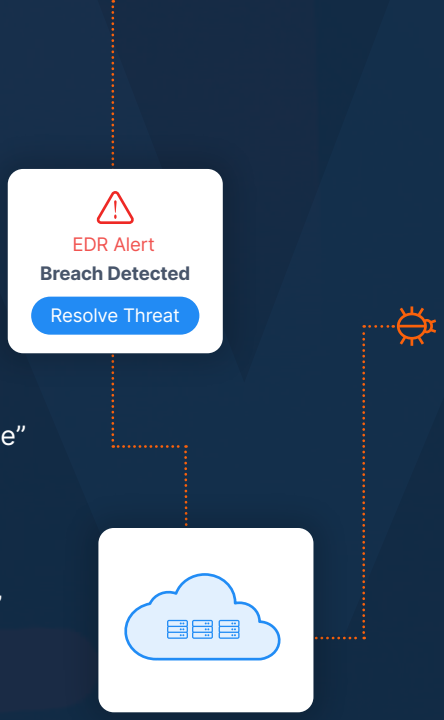
While most agencies have seen a rise in premiums by up to 30%,[8] the financial stakes are still too high for some insurers, jeopardizing the availability of coverage.

If we take at face value the possibility that sophisticated cyber groups are in the business to make money, we must also believe that they are just as sophisticated in their research—of potential targets as well as macro-level trends and policies which could impact their business.

As a result, research suggests that this practice of cyber insurance is encouraging cybercriminals. Insurers are not using incentives to reward better security practices or imposing higher fees or penalties for those who fail to improve security practices. Cybercriminals know that insured companies are often quick to pay the ransom. They have even been able to infiltrate insurance companies to seek customers' identities and scope of coverage so they can target them.

It's becoming increasingly clear that cyber insurance is not a silver bullet solution to protect organizations but instead should be viewed as one part of a risk mitigation strategy that must include best practices, compensating controls, and advanced ransomware protection.

A New Era: Continuous Runtime Protection for Server Workloads



Until now, the best the cyber industry has had to offer is “detection and response” tools that generally discover breaches after they occur. The reason for this is that these tools are ultimately abstracted from where the action is occurring, particularly in zero-day attacks which make up the bulk of today’s threat landscape. The adversary is operating much deeper than today’s “kernel hooks” so prevalent in detection and response products. They are now at the deepest levels of an application, such as the memory - where data becomes code.

This is why protection in milliseconds is so crucial. If the adversary needs a mere 3 seconds to affect an attack on a server workload, cyber solutions must fully protect the application as it is running—and do so faster than the adversary can gain purchase.

Deterministic Protection

Deterministic protection is a ground-breaking new approach ideally suited for workload security. It relies on mapping an application at the deepest levels, validating the map according to the developer’s intent for that application, and locking it down. It’s a simple concept but to date has been difficult to do without heavy-handed methods which cause latency or compromise user data.

All server application compromises have one thing in common, regardless of the motivation behind the attack: the application is being forced to do something it was not intended to do. Command and control, shift left or right to see what is around, escalate privileges, reach out to the cloud, download malicious payloads, etc. All of these are examples of ways an adversary forces the application to do something they want it to do.

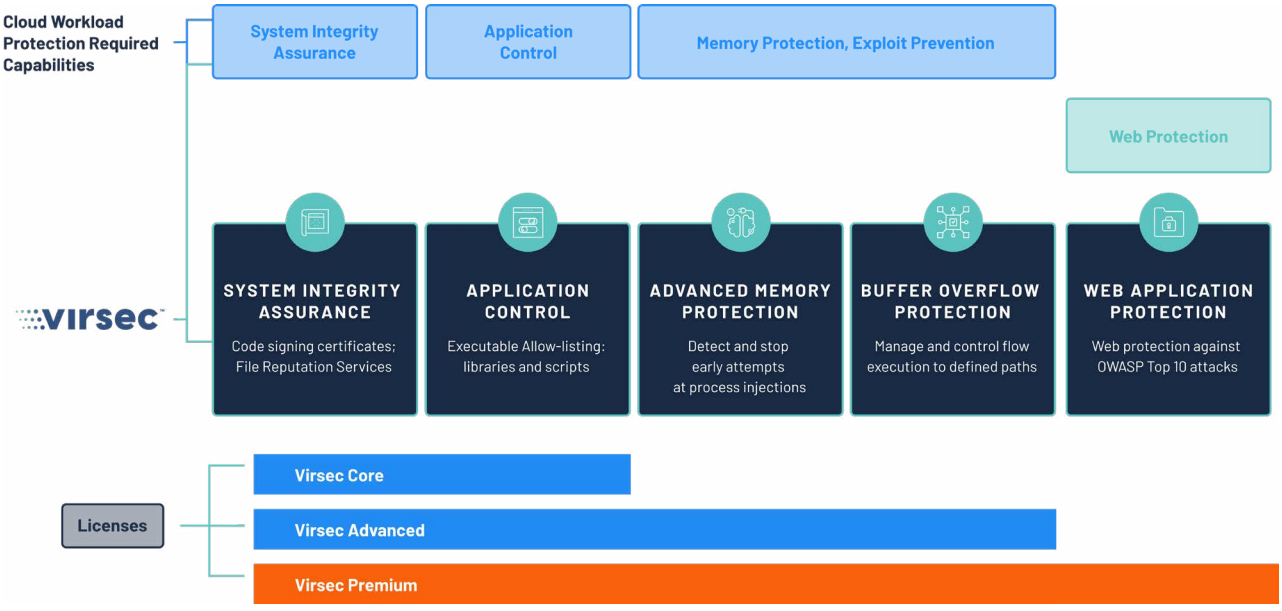
If we can lock down an application into an immutable status until we, the user, decide to update or make a change (patching, for example), then we are fully protected from a myriad of attacks, including Zero Days, Remote Code Execution (RCE), Advanced Persistent Threats (APT).

Put simply, it’s easier to fully protect the known, validated good code while it is running than it is to peer into the abyss of past threats and make an educated guess at the vast possibility of unknown threats that the adversary might execute next.

Virsec Security Platform

Virsec Security Platform (VSP) applies deterministic protection to enable a protection-first strategy. It stops attacks 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 with very high efficacy, **thus also drastically reducing false positives.**

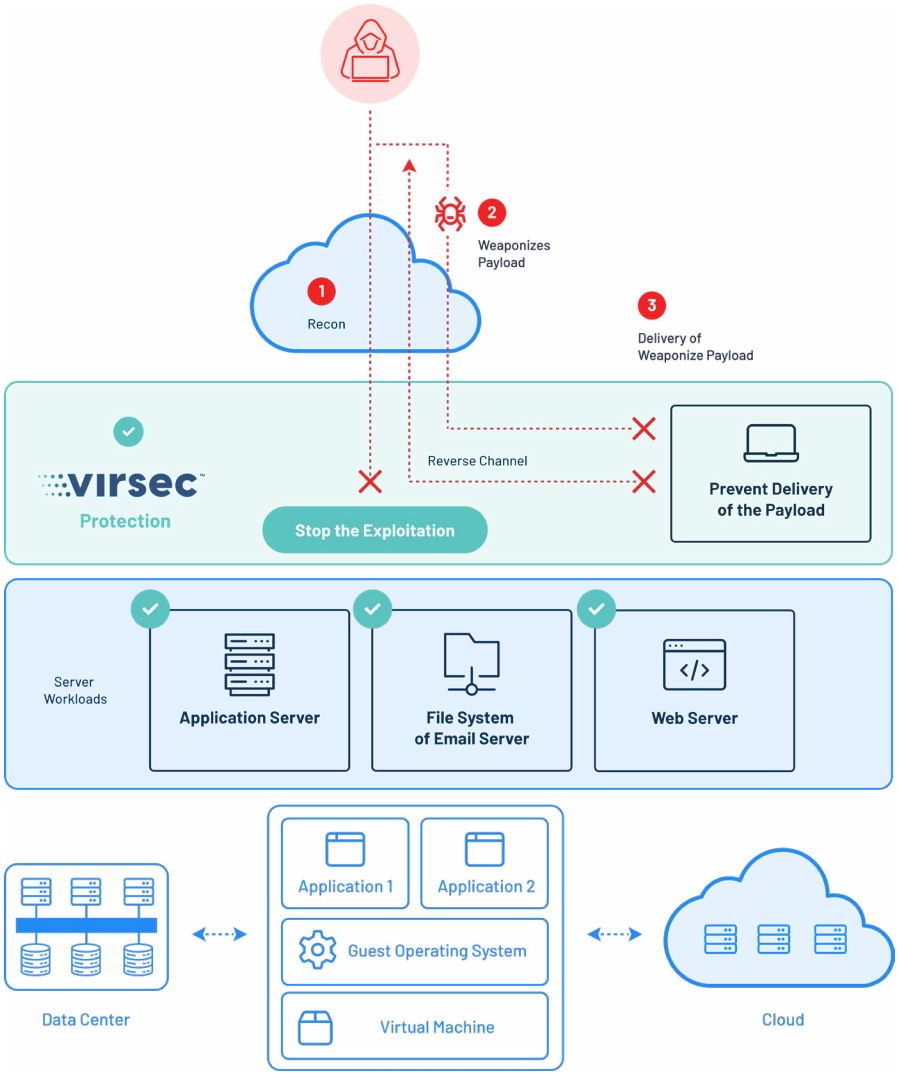
Virsec proactively protects against ransomware and malware exploits with VirsecMap, which defines the executable allow list of what is authorized (system integrity), and VirsecEnforce which dynamically enforces that the software executes as expected (runtime protection). With a protection-first approach 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.**



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

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. Virsec also continuously addresses high-risk and critical Common Vulnerabilities and Exposures (CVEs), 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.

VSP also prevents lateral progress in the event chain by **blocking unauthorized code execution on host operating systems (OS).**



Conclusion

Ransomware attacks continue to be pervasive and damaging, but there is a solution and end in sight. Public and private organizations are continuing to innovate their thinking and collective need for a new approach to the problem. With government and industry coming together, a portfolio of risk mitigation strategies and offerings, and first-of-a-kind solutions like the Virsec Security Platform that immediately blocks ransomware before damage can be done.

Endnotes

1 U.S.-CERT CISA Alert (AA21-243A)

2 NPR

3 Cybersecurity Ventures

4 Cost of a Data Breach Report 2021

5 Sophos

6 The PEW Charitable Trusts

7 U.S. Government Accountability Office

8 U.S. Government Accountability Office

Additional Sources

https://www.washingtonpost.com/politics/2021/09/07/cybersecurity-202-ransomware-is-wreaking-havoc-us-cities/

https://www.policyholderpulse.com/ransomware-insurance-coverage/

https://www.insurancejournal.com/news/national/2021/07/07/621416.htm

https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-security-challenge

https://www.zdnet.com/article/ransomware-has-become-an-existential-threat-that-means-cyber-insurance-is-about-to-change/

https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/ https://www.cisa.gov/stopransomware

virsec™

Virsec protects the world's most important applications and systems from the inside, stopping advanced cyberattacks on any application workload in any environment.