FOCUS ON PROTECTION, NOT CURE

Runtime protection, where all runtime actions are monitored, is the optimal solution for protecting your business from cybercrime, writes Danny Kim

Another day, another high-profile ransomware attack. That's how the rolling news of the last year has played out as bad actors exploit new vulnerabilities in remote working infrastructures. There were 2,084 ransomware attacks in the US in the first half of 2021, a staggering 62 per cent increase from the same period in 2020. And that's just the complaints that are reported to the FBI.

What's more, given its relatively low risk and high reward nature, ransomware techniques are often highly successful. With the emergence of cryptocurrencies, cyber criminals can be difficult to trace. Since the Covid-19 pandemic, ransomware has burgeoned into a multibillion-dollar industry. Collective global ransomware costs to businesses for 2021 are estimated to exceed $20bn, with the average breach yielding a ransom of $4.6m.

The truth is cybersecurity incidents involving corporate data being withheld through criminal infiltration or ransomware have been carried out for years. So much so, that any single organisation is often violated more than once.

DANNY KIM

PRINCIPAL ARCHITECT

VIRSEC

2,084

RANSOMWARE ATTACKS IN THE US IN THE FIRST HALF OF 2021

RISKS AT SOFTWARE RUNTIME

Ransomware attacks can be executed in a matter of seconds. Malware varieties often gain system access though SQL injection, stealing credentials, phishing and other social engineering methods. Once inside, threat actors access data, hijack operations, deploy encryption tools, encrypt data, and, once they have the data, demand a ransom.

Such attacks do the most damage when they move from desktops to servers. Inside servers, the malicious code runs at the same time as applications, infiltrating application architecture, data sets and complete workloads.

Enterprise applications in runtime are among the most vulnerable to the threats posed by ransomware malware. Multi-step kill chains, fileless malware and remote code execution are now able to bypass conventional, signature-based, probabilistic security tools.

FOCUS ON PROTECTION, NOT CURE

The good news is that continuous innovation has now yielded a breakthrough solution to prevent ransomware malware from running in-memory alongside runtime applications.

Protection of runtime applications requires that every action be fully mapped and understood. Such protective solutions should monitor every step of application execution and only permit predetermined actions. This is known as 'deterministic protection'.

These types of innovative solutions do not permit any runtime applications that are not predetermined including malware that is loaded in-memory. The malware routine in-memory will appear as a deviation from the concurrent runtime and will be prevented from execution.

By comparison, conventional cybersecurity tools cannot distinguish between expected and deviant behaviour. Such tools also fail to prevent ransomware because they do not have application runtime visibility.

Conventional tools often only control, protect and provide visibility before and after application runtime – and not when the application deviates from its intended performance.

This breakthrough approach protects the software workload while it is in runtime and prevents ransomware attacks on applications and workloads. It also creates a snapshot of all critical applications, including files, scripts, binaries, container images, libraries, and only allows predetermined processes to execute.

No matter which platform is being used by applications, such as cloud, on-premises, containers, hybrid, or air-gapped, runtime application protection ensures pervasive high security levels. This type of deterministic protection promises to temper the present-day threats of ransomware, no matter what level of advanced malware sophistication is being used.