CASE STUDY

Middle Eastern Government Achieves Application-Aware Workload Protection for Critical Systems

The Customer

As a stable country in one of the world's most volatile regions, this Middle Eastern government has made an exceptional effort to maintain strong political ties with its neighbors, often acting as an arbiter in many disputes. The country is also known as being highly technologically savvy, seeking out industry leaders to maintain robust and secure systems. But this unique standing has also made it a target, especially for nation-state sponsored cyberattacks.

The Challenge

Security experts within the government had noticed a prevalent spike in persistent, targeted cyberattacks that were seeking to exploit gaps in their security to steal sensitive data and cause disruption. Officials were most concerned about the significant increase in advanced in-memory techniques that inject code directly into applications during runtime without using detectable files – also known as "fileless malware." Memory-based attacks can easily bypass conventional security tools like firewalls, antivirus, or intrusion prevention systems, and the government needed to harden their defenses.

Memory-Based Attacks

The government detected evidence of ongoing and increasing memory-based attacks but lacked confidence in their existing security tools to systematically protect hundreds of their servers running critical applications with highly sensitive data.

Limited Control and Visibility

The government had multiple, disparate point solutions, each with limited scope and visibility. Evasive attacks that were occurring at the memory level proliferated, going undetected for untold amounts of time. Their infrastructure was not prepared to defend against sophisticated and evasive attacks that were occurring at runtime, a gaping blind spot for their security team.

Overburdened Resources

Though they had a robust cybersecurity posture, the government's existing security tools required extensive tuning and signature updates, as well as generating excessive noise and false positives. This was a drain on their resources and made it more difficult to stay up to date with the numerous vulnerability patch requirements and policy updates.

VIRSEC

"We were looking for a state-of-the-art way to protect our critical server infrastructure. By implementing Virsec, we were able to close a security gap quickly and effectively, hardening our defenses against memory-based attacks and gaining control and visibility at runtime across our operations."

Senior Government Security Official

The Solution

Government officials turned to their long-term partner Raytheon, who introduced Virsec's innovative technology to them. The Virsec Security Platform is uniquely suited for protecting critical applications from memory attacks during runtime. Raytheon and Virsec jointly engaged in a proof-of-concept and competitive testing on-site to demonstrate effectiveness within the government's own infrastructure. The Virsec Security Platform detected and stopped both evasive memory-based attacks as well as other advanced exploits that attempted to execute in runtime.

Full-Stack Protection

With the Virsec Security Platform deployed, the country's critical infrastructure and data were protected across the full application stack at the web, host, and memory layers. Attacks are detected and stopped instantly at the first step in the kill chain. And the system can detect zero-day attacks with no prior knowledge, no signatures, no noise, and no tuning.

Memory Protection

The government can now identify and stop advanced in-memory attacks that were not identified by their previous system. Because the solution operates in process memory it can pinpoint fileless attacks with unprecedented speed and accuracy and take immediate action. Any memory-based attacks, fileless exploits, and filesystem changes levied against the country's infrastructure are now stopped at the first step of the kill chain.

Zero Noise, Zero Tuning, Zero Dwell Time

The government selected Virsec because of its automation, depth of protection, and lack of false positives or extraneous security alerts. They found Virsec easy to manage because of the automated, out-of-the-box detection that does not require signatures, learning, tuning, or policy updates. Virsec's compensating controls against vulnerabilities that have not been patched provides an effective form of virtual patching.

Superior Protection Against Sophisticated Attacks

The government was able to scale the Virsec solution to protect a broad range of their critical application workloads at the web, host, and memory layers in a multitude of their environments. Virsec's unique application-awareness technology ensures that code executes only as it should at runtime, providing critical visibility and control over this new security battleground. As a result, the government has achieved true cyber resiliency, with full visibility and control over how their critical applications execute during runtime.

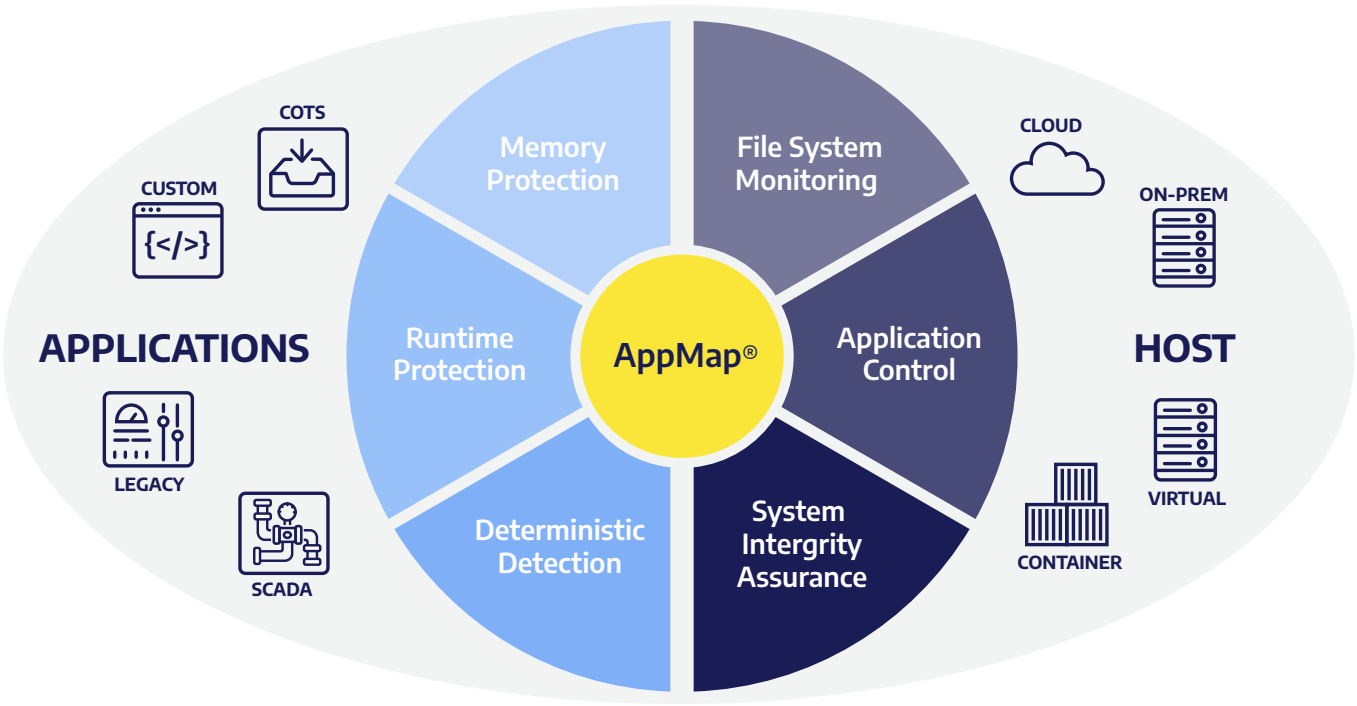
Application-Aware Server Workload Protection

Virsec provides application-aware server workload protection against the widest range of cyberattacks – known and unknown – and secures applications from the inside.

ANYWHERE	ANYTHING	ANYTIME
On-prem, public/private cloud, hybrid, container	*Custom, legacy, COTS and air gapped applications*	*Deploys in minutes, protects continuously in real-time*

Unique AppMapp® Technology

Virsec's patented AppMap® technology maps the sequence of processes and commands for all applications authorized to run across the full server workload. The solution does not have to know every legitimate system call in every app and every context, nor is it learning as it goes. Instead, the Virsec security platform immediately detects any variations or deviations in execution and initiates an immediate defense.



VIRSEC

Securing the World's Most Critical Applications

Virsec is deployed globally protecting mission-critical applications and infrastructure in industries including financial services, healthcare, government, defense, power, oil & gas, transportation, telco, technology, and more.

Recognition

Cyber Catalyst · CRN · Cyber Defense Magazine Global Awards 2019 Winner · Gartner

Cyber Security Excellence Awards Winner 2020 · MITRE · Info Security Products Guide 2020 Global Excellence Gold · Ovum

Partners & Customers

Tech Mahindra · NCUA · Raytheon Technologies · Godrej

Schneider Electric · YOTTA · du · AVEVA

BROADCOM · inspirage · etisalat · GDIT

No Signatures, No Tuning, No Noise from false alerts

Zero Dwell Time: stops attacks instantly at the first step

Full-Stack Runtime Protection" protect web, processes, memory, libraries, iles, hosts

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

VIRSEC