virsec

CASE STUDY

Middle Eastern Government Secures Critical Systems

Virsec Delivers Advanced Protection for Hundreds of Applications

The executive branch of a Middle Eastern government was concerned about the increase in targeted cyberattacks that use advanced in-memory techniques to bypass conventional security tools. These memory-based attacks inject code directly into applications during runtime without using detectable files.

This administrative arm of the government handles large amounts of highly sensitive information and was concerned that advanced attacks could bypass their existing server endpoint solutions. They turned to Raytheon and Virsec to recommend advanced solutions to protect hundreds of server-based applications.

The customer had a full range of conventional security technology including endpoint protection, WAF and EDR products. Despite this, they believed there were critical gaps in their protection which could expose sensitive data. They also felt their existing security tools required too much tuning, signature updates, false positives, and tedious man hours to keep up with new vulnerabilities.

Customer Profile

- Regional Leader Providing Stability in a Volatile Region
- Critical systems and data frequently targeted by attacks
- Long-term partnership with Raytheon who introduced Virsec to upgrade protection

Virsec Security Platform Outperforms Conventional Tools

The Virsec Security Platform (VSP) was tested in a detailed, competitive POC with leading conventional endpoint security tools. Virsec was found to provide far greater efficacy and accuracy then their existing tools, while detecting and stopping advanced in-memory attacks that were not previously detected. The solution has been deployed to protect over 200 applications at the host and memory layers.

VSP was selected because of its depth of protection, automation, and lack of false positives or extraneous security alerts. Virsec was also found to be easier to manage with automated, out-of-the-box detection that requires no signatures, learning, tuning, or policy updates.

Because the solution can detect zero-day attacks with no prior knowledge, the customer found that Virsec can provide compensating controls against vulnerabilities that have not been patched – and effective form of virtual patching.

> *"Virsec has allowed us to detect and stop dangerous, advanced attacks that were previously invisible. Once deployed it automatically adapts to new threats without any changes or tuning on our part."*
>
> - ***Lead Security Architect***

©2020, VIRSEC, all rights reserved

Key Challenges

This regional government had multiple security challenges before working with Virsec, including:

- Concerns over advanced, in-memory attacks
- Gaps in security coverage and blind spots with existing conventional security tools
- Too many disparate point solutions, each with only limited scope and visibility
- Numerous policy updates, tuning, and false positives with endpoint security tools
- Limited IT resources and security specialists to assist with monitoring and maintaining cybersecurity
- Difficulty staying up to date with vulnerability patching

Definitive Results with Virsec

- **Protects the full application stack** including web, memory and host layers
- **Scalable to protect hundreds of apps** with automated deployment and out-of-the-box protection
- **Stops threats that bypass existing tools** including memory-based attacks, fileless exploits that bypass EDR and WAF solutions
- **Reduces management time** without tuning, policy updates or false positive analysis
- **Delivers Compensating Controls** to prevent vulnerability exploits even if patches have not been applied

Virsec Protects the Full Application Stack from the Inside

VSP was deployed by this government customer because it:

- Protects the full application stack including host, memory, and web layers
- Could be deployed automatically to over 100 application instances with automated instrumentation
- Delivers out-of-the-box protection against advanced threats without signatures, tuning, learning, policy updates or manual intervention
- Enables unprecedented runtime visibility of process memory to prevent memory-based threats, fileless malware, and unknown or zero-day attacks
- Provides effective compensating controls against vulnerability exploits regardless of patch status.

> *"Virsec was easy to deploy and required no customization. It's a win-win for us – providing better security coverage with less effort to manage than our previous tools."*
>
> - ***Director of IT Security***