virsec®

CASE STUDY

Technology Giant Secures Customer Portal

Virsec Ensures Security, Data Privacy and Continuity for Global Customers

With the sharp increase in advanced cyberattacks, this global technology leader was concerned about potential security gaps in their customer portal. This web-based portal provides critical product information and support services for thousands of customers globally.

The customer had a full range of conventional security technology including endpoint protection, WAF and EDR products, as well as dozens of security products available from their own security division.

Despite this, they believed there were critical gaps in their portal protection which could potentially expose sensitive data and customer information. They also felt their existing security tools required too much tuning, policy adjusting, false positives, and tedious man hours to keep up with new vulnerabilities.

Customer Profile

- **Top designer & manufacturer of semiconductor technology**
- **Leader in infrastructure, networking, software, and security solutions**
- **Global customer base supported through web portal**

Virsec Security Platform Outperforms Conventional Tools

Virsec was engaged for a detailed POC with the Virsec Security Platform (VSP) protecting the full application stack for the customer portal, including Java, Node.js, and Nginx web servers. The solution was tested for efficacy, performance, and usability while protecting web, memory, and host layers against advanced attacks.

VSP was found to detect and stop the widest range of attacks that bypassed their existing WAF, endpoint and EDR solutions. 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 detects attacks we've never seen before, without any tuning, tweaking or false positives. This gives us the confidence we need to protect critical customer data."*
>
> - ***Enterprise Security Architect***

After careful evaluation, VSP was selected because of its depth of protection, automation, and lack of false positives or extraneous security alerts. The solution is being deployed to protect over 100 application instances across the full application stack of the customer portal including web applications, web servers, third-party tools, and host systems.

Key Challenges

The technology giant had multiple security challenges before working with Virsec, including:

- Concerns over application integrity and data privacy for their global customer portal
- 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 WAF and EDR solutions
- Limited IT resources and security specialists to assist with monitoring and maintaining cybersecurity
- Difficulty staying up to date with vulnerability patching

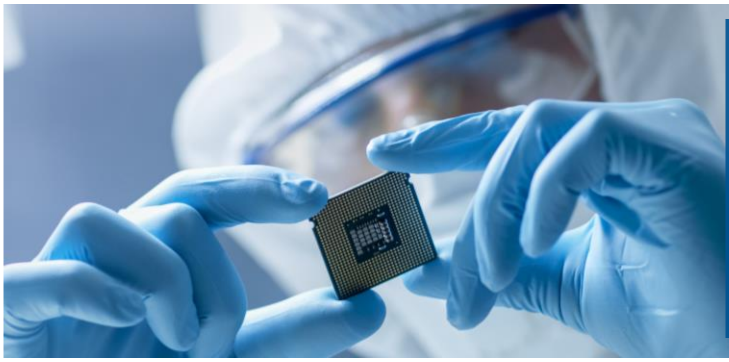
Definitive Results with Virsec

- **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 selected and deployed by this major customer because it:

- Protects the full stack of portal application including Java apps, Node.js, and Nginx web servers
- Was fully integrated with the **Nutanix** platform
- 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***

ProtectedIT
Elevating & Unifying Security Technologies