Choose the Solution That's Right for Your Business

Optimize the value of your security infrastructure with protection where you need it most

Building security into your infrastructure is one of the most important decisions you make for your business. Virsec offers you flexibility to optimize application security where you need it most. To make it easier to purchase the right Virsec Security Platform capabilities for your environment, Virsec provides three levels of software offerings: Advanced, Professional, Enterprise.

With Advanced, Professional and Enterprise packages, Virsec tailors solutions that are:

1. **Affordable:** Three packages provide options for a phased approach to deployment
2. **Flexible:** Our comprehensive capabilities support a wide range of app types
3. **Best Value:** Increase your security posture and add value to existing investments

Choose what's right for your business

Go deeper in your defense strategy and ensure advanced application security for business-critical apps in the datacenter or cloud.

Advanced

Advanced application defense for compiled applications, including protection for file system and binaries

Well suited for: ICS/SCADA/OT environments, backend/internal apps, systems not exposed to the web

Professional

All the benefits of Advanced plus full memory-based attack defense

Ideal for: protecting systems supporting vital infrastructure used in oil & gas, chemical, water and energy (no web exposure)

Enterprise

Comprehensive application defense providing full-stack protection for all app components including Web servers, databases, memory and microcode with auto-patching of OWASP 10, intelligence, central monitoring & customizations

Best for: critical infrastructure and business systems, especially those vulnerable to fileless attacks or evasive exploits of system flaws, even Spectre and Meltdown

Virsec

Choose the solution that's right for your business

Features and Capabilities	Advanced	Professional	Enterprise
In-depth ICS/SCADA Security			
Code integrity defense	○	○	●
Interpreted code attack detection			●
Compiled code attack detection	●	●	●
Microcode protection			●
Memory-based attack defense	○	●	●
OWASP top 10 security			●
Database transaction integrity check			●
Brute force attack detection			●
Full request & response examination	●	●	●
Advanced Attack Defense			
Fileless malware, buffer overflows, Meltdown, Triton	○	●	●
Injection attacks SQL, DLL, XSS, CSRF, HTTP Header, OS command, traversal and process injections			●
Java de-serialization attacks CRLF and HTTP Response Splitting			●
Unknown threats	○	○	●
Zero-day attack			●
File system protection	●	●	●
Automated Protection			
SMS and email alerts	●	●	●
Continuous policy-based authentication			●
Attack protections block, log, URL override/redirect			●
Integrated customizable mitigation			●
External ticketing system support	●	●	●
Management and Reporting			
Centralized management			●
Real-time dashboard	●	●	●
Detailed event logging	●	●	●
General threat & attack reporting			●
Customizable reports and charts			●
Forensic threat intelligence data			●
Attack attribution reporting			●
Violation classification and risk scoring			●
Customized alerts			●
REST API			●

● Full protection ○ Partial protection