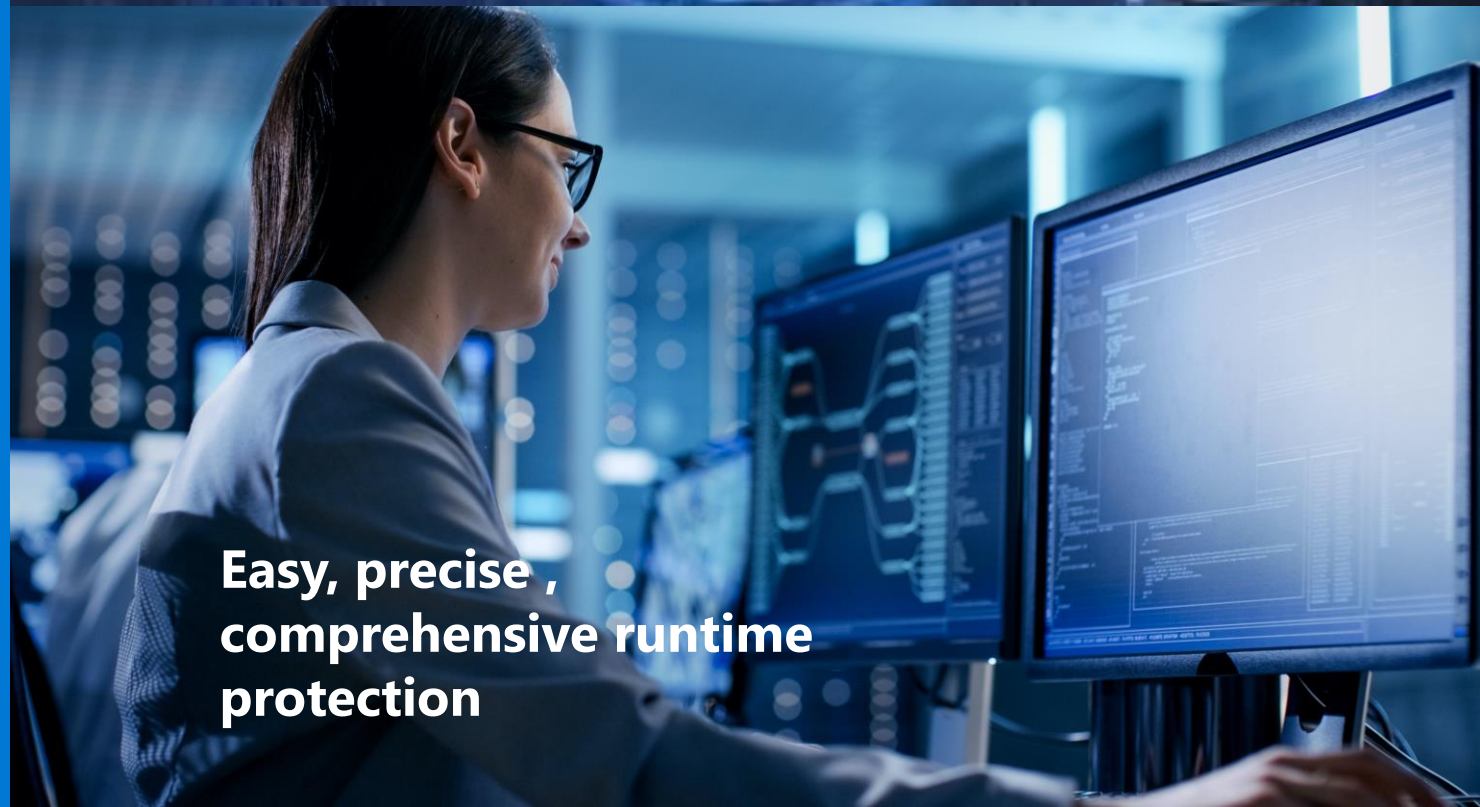
Vinca Cyber

Azure Workload Security

[yourhyperlinkedwebsiteURL.com]



vinca Cyber

[Your Microsoft Partner Badge]

Enterprises: Effective cloud security requires more salient protection at runtime

Organizations continue to invest in new network security tools and instrumentations to shield known vulnerabilities and block everyday malicious user activities affecting cloud workloads and applications. However, unique exposures and more evasive attack schemes surface rapidly, which remain difficult to protect against using AV, EPP, EDR and analytics

CHALLENGES

- Lack of app-aware visibility across the stack leaves data and services greatly exposed
- Addressing vulnerabilities can take time (weeks), be expensive, strain resources and affect SLA's
- Trusted processes, files, functions, OS tools and memory are frequently used to bypass security

EFFECTIVE SOLUTION

Today's cloud security demands …

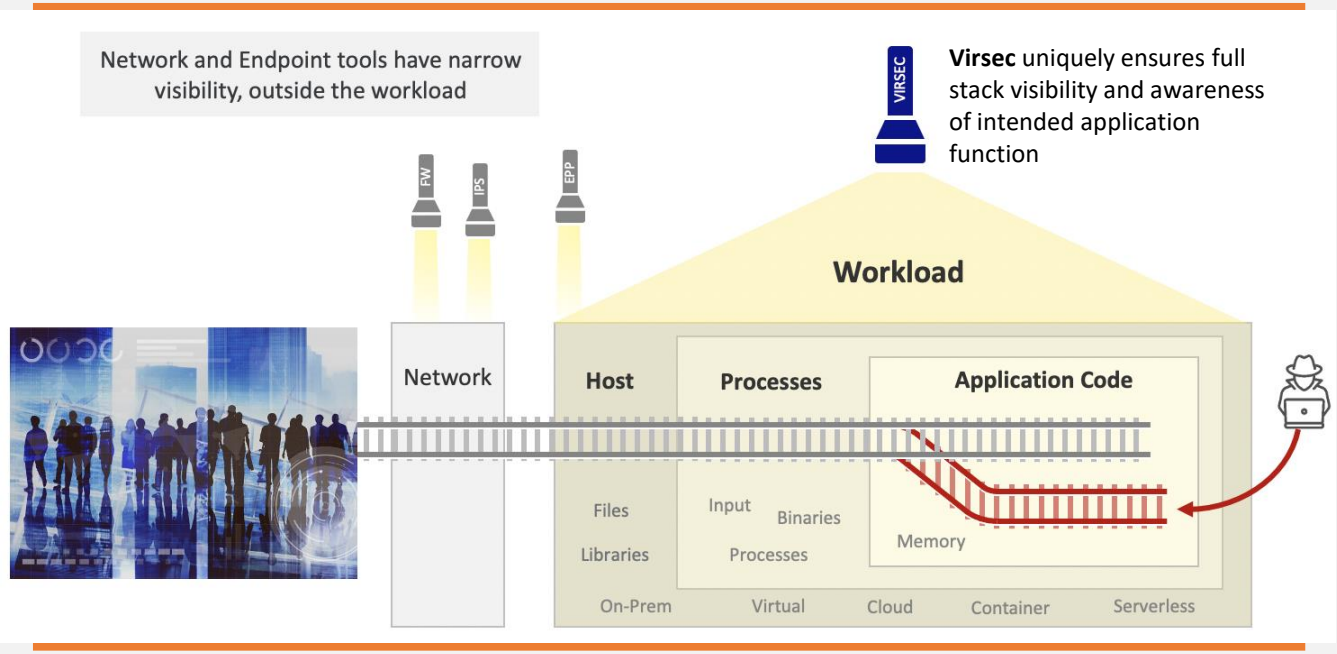
App-aware workload protection that stems from pervasive application monitoring on the inside *(not the network or outside containers)*

Assurance of trusted execution throughout runtime for all workload and app deployments

Reduced dependency on expert human efforts, post attack data analysis, and false positives

Better Security in the Cloud

Vinca Cyber helps enterprises implement the most effective CWPP* capabilities with ease, expanding Azure Defender to ensure only trusted code executes as intended for continuous control flow integrity with automated protection against evolving attacks, and evasive fileless exploits targeting unpatched and unknown vulnerabilities in apps, OS & memory.



VINCA CYBER

VIRSEC SECURITY PLATFORM

APPLICATION-AWARE WORKLOAD PROTECTION extends security beyond network and endpoint tools to secure applications from the inside using unified app controls, web security, workload integrity monitoring and memory protection, *so you can counter known and unknown attacks with unprecedented speed and accuracy, and without tuning, signature, noise or attacker dwell-time*

COMPLETE RUNTIME VISIBILITY

Instrumented in the server workload for complete visibility across the application stack preventing misuse of commands, processes, scripts, libraries

DETERMINISTIC PROTECTION

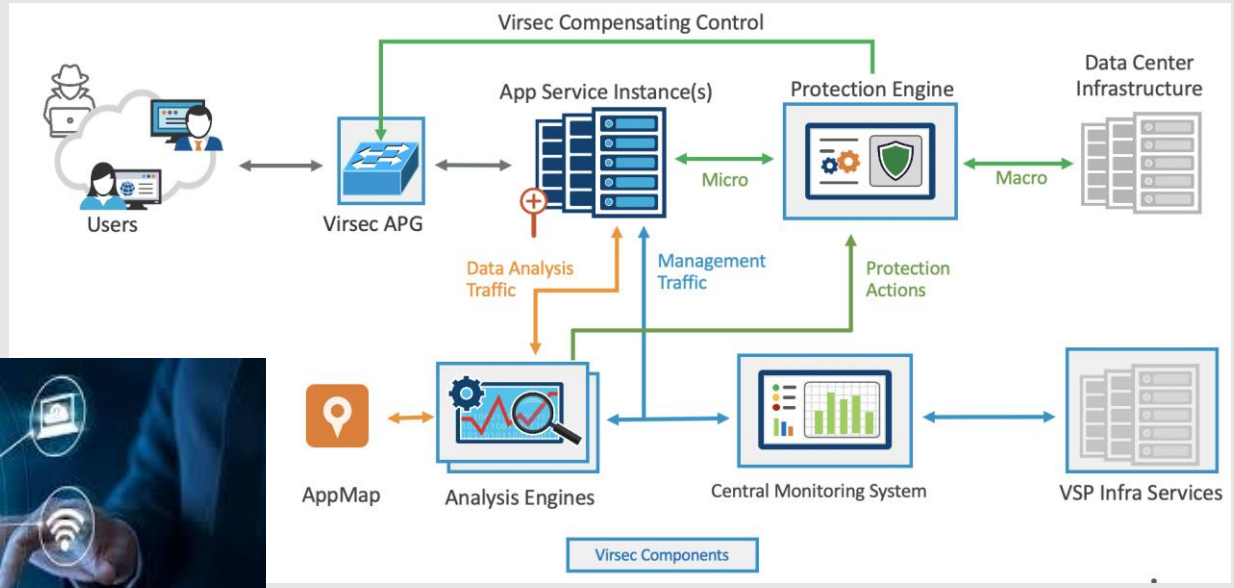
Maps application memory use to detect movement towards unintended code, ensuring malicious code and instructions never execute

COMPREHENSIVE COVERAGE

Uncover unauthorized workload modifications & attempts to deliver or detonate known/unknown malware in real-time at **web, memory or host level**

Vinca Cyber Virsec Security Platform (VSP) + Microsoft Azure

Better Protection Together – Azure and VSP allows you to easily deploy, run and protect vulnerable software with precision wherever patching is outstanding, identifying and stopping malicious events without false positives, and no policies, no learning, no analysis, or the need for expertise and hunting. Deploy cloud workloads with confidence of the most effective and efficient protection, and unmatched threat visibility no matter attacks originate.



COMPLETE RUNTIME VISIBILTIY

- Agent sensors provide deterministic runtime analysis across all app layers & composite workload structure
- Delivers realtime threat details & workload status insights
- Executes a broad range of protective actions without guessing, threat hunting or alert validation.
- Integrates with common SOC services supported by AZURE to best enable workflows

EXTENDS APP DEFENDER CAPAPBILITIES

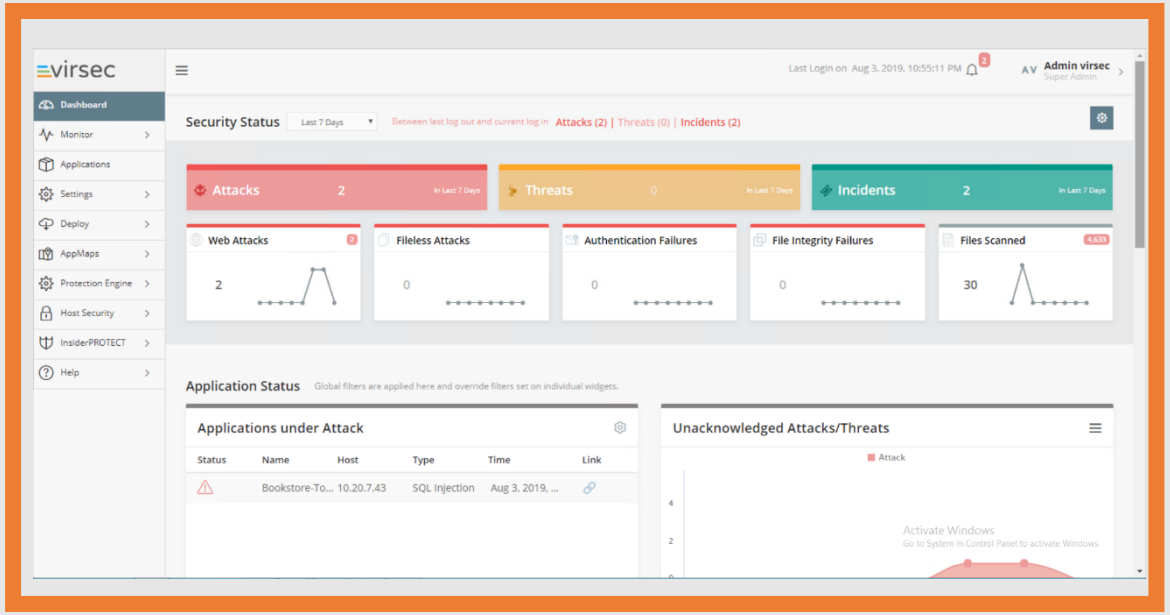
- Provides app-aware protection by mapping acceptable runtime execution for precise detection
- instantly stops code deviations for real-time protection against evolving attacks
- Prevents threats from advancing, and ensures services continue to function as intended without disruption

EVOLVING THREAT PREVENTION

Overcomes challenges with patching software flaws in 3rd party of proprietary apps, operating systems, databases, servers, and other code, preventing malicious code execution in memory to stop attacks in real-time

Regulatory Agency minimizes cyber risk for all Azure deployments with VSP runtime visibility, attack prevention and automation

"Activating VSP within Azure workloads increased SOC efficiency and protection assurance for critical cloud deployments -- reducing dependency on complex network tools that gather meta data and run analytics that only identify known suspicious events without true distinction of new attacks as they happen, creating more work without risk reduction"



Protection Efficiency for 100+ VMs

"Delivered automation and provided an intimate level of security controls we hadn't had before, addressing compliance and improving coverage throughout 100+ VM's without management or MSSP efforts" **Dir Security and Operation, Cloud**

Easily Addresses vulnerabilities

- Malformed requests
- Kernel vulnerabilities
- Script Code Execution
- All OWASP Threats
- Memory & Code injection
- Side-Channel attacks
- Privilege Escalation
- MITRE top 25

Continuously addresses high-risk and critical CVEs and CWE's without manual efforts or deep expertise

Improved threat visibility

"Alerted us to attacks and threats that we were not made aware of until significant time and investigation happened – like certain SQL injections, XSS and XML web attacks and fileless attempts to compromise libraries without malware". **Sr. Cyber Threat specialist**

Reach out to us today to discuss Better Cloud Protection *with*

VINCA CYBER - *Virsec Security Platform*

Get a free trial: [yourhyperlinkedtrialURL.com]

Call for more information: [555-555-5555]

Ask a question via email: [email@site.com]

Learn more: [yourhyperlinkedproductsiteURL.com]

Link to your Microsoft Commercial Marketplace offer

[Your Company Logo]

[Your Microsoft Partner Badge]