XDR+

With Patch Management and Deception Across Landscape, Invinsense ODS Makes it harder and confusing for adversaries to achieve their objective.

Offensive Defensive Strategy against All Odds

With so many sophisticated cyberattacks happening everyday worldwide, one thing is proven, adversaries can enter any kind of organizations. The main reason of their success is that they work as a community which is more organized than even legitimate organizations. Defense in depth should also be around the preparedness of neutralizing the threats that have entered an organization.

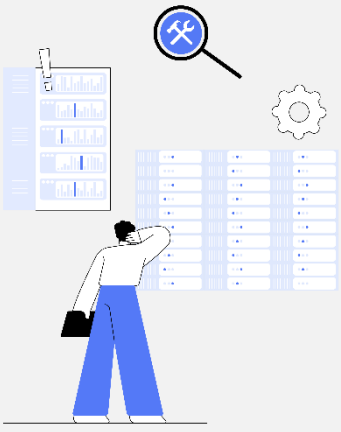
Invinsense Deception- An Integrated Network and Endpoint Deception

Invinsense Deception is a combination of two cybersecurity approaches: 'Network Deception' and 'End Point Deception' that help to deceive and divert adversaries from achieving their objective. Deception allows deploying various decoys in your network to deceive the attacker and the end point deception approach allows altering real assets with assets to set a trap for attackers. Invinsense Network Deception and End point Deception work in coordination to change environments in real-time. End point deception creates dynamic & deceptive information, responds to the evolving nature of advanced threat landscape and interferes with attackers attempts to recon the environment that deters them from executing their malicious intents, through all the stages of compromise in the Attack Kill Chain and Network Deception creates more decoys to further trap adversaries in a broader environment. These two technologies share threat intelligence and trap adversaries in real-time and protect you from falling victim to advanced attacks across your network, endpoints, servers, and application.

Power of Deception with Deceptive Files

Invinsense deeply understands the attacker's tactics and techniques and offers a powerful deception platform to trap the attacker. Invinsense deception offers deployment of deceptive files as honey pots, honey credentials, honey hashes, honey files, and servers, etc. to deceive and lure the attacker. It deceives attackers by deploying decoys similar to real components e.g. fake network systems, fake FTP servers, fake files, etc. Whenever there is any security incident it remediates threats by an automated incident response like isolating and blocking the source of activity or quarantine that network component to stop lateral movement of threats.

Network Deception



Key Features:

- Personalized threat intelligence
- Accurate alerts
- Environment specific decoys
- Interactive and non-interactive decoys
- Client-side decoys to detect MITM attacks
- Customized alerts
- Data exfiltration detection
- Decoys with exploit detection capabilities
- Video recording- Attack activities, Evidence
- Forensics Keystroke recording
- Supported platforms – Windows, Mac, Linux
- Honey hashes and breadcrumbs to deceive and lure the attacker
- Ensures early detection threats
- Automated incident response like isolation, blocking, and quarantine

Proactive Defense by End Point Deception

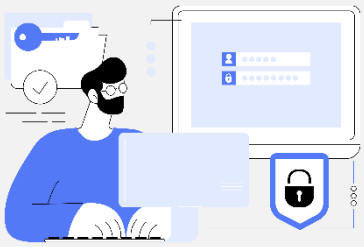
An innovative solution against threats in enterprises' most critical and exposed assets, their endpoints! The solution is a fully endpoint-centric deception platform that creates dynamic & deceptive information, responds to the evolving nature of advanced threat landscape and interferes with attackers attempts to recon the environment that deters them from executing their malicious intents, through all the stages of compromise in the Attack Kill Chain – covering advanced & sophisticated malware techniques, constantly making sure all the endpoints & data in the enterprise are secured in several ways.

Pre-emptive Defense

Making malware believe it's in an unattractive/hostile environment to attack, reducing its motivation and the chance of infection, e.g. by creating a sandbox/VM environment which deter malware.

Proactive Defense

Actively responding to threats as they evolve, changing the outcome of the attack through all the stages of the Endpoint Kill Chain, e.g. by deceiving and stopping Ransomware, thinking it succeeded encrypting the files as the solution safeguard them.



Key Features:

- Prevents unknown & sophisticated threats
- Real time detection & response
- Full protection at all times, even when offline
- Very high prevention & detection rates
- Extremely low resource consumption (CPU, RAM)
- System-wide protection with pinpoint handling
- Deploys in seconds
- Automatically approves legitimate processes
- Low to non-existing false positive rate
- No constant updates
- Can operate outside the corporate network
- Stop millions of threats using 1 defense evasion

Patching often is the right thing to do. One of the favorite tactics of adversaries is to exploit unpatched machines or software and enter an organization. Stopping adversaries completely may not be possible but making it harder for them is very much possible. Patches are new or updated lines of code that determine how an operating system, platform, or application behaves.

Patches are usually released as needed to fix mistakes in code, improve the performance of existing features, or add new features to software. Patches are always released as updates to existing software, and are not newly compiled OSs, platforms, or applications.

Because modifications like these are usually quicker to distribute than minor or major software releases, patches are regularly used as network security tools against cyber-attacks, security breaches, and malware —vulnerabilities that are caused by emerging threats, outdated patches, or system misconfigurations.

One of the hardest tasks for any organization is getting 100% patched. Every time you get a Common Vulnerabilities and Exposure (CVE) notification or Information Assurance Vulnerability Alert (IAVA) mandated by security, you have to kick into and get the patches installed which is never simple and easy, still we can automate to the best possible extent.

Invinsense Patch Management Makes It Harder For Adversaries to Enter an Organization

Invinsense Patch Management is an administrator's control over operating system (OS), platform, or application updates. It entails identifying system features that can be improved or fixed, creating that improvement or fix, releasing the update package, and validating the installation of those updates. Patching— along with software updates and system reconfiguration—is an important part of IT system lifecycle management. Enterprise IT environments can contain hundreds of systems operated by large teams—requiring thousands of security patches, bug fixes, and configuration changes. Even with a scanning tool, manually sifting through data files to identify systems, updates, and patches can be onerous. Invinsense Patch management allows automation to roll-out patches, generate clear reports on which systems are patched, which need patching, and which are noncompliant.

The Key Features Are:

- Discover Asset and Inventory
- Prioritize Assets and Users
- Security Policies and Updates
- Staying Ahead of New Patches and Updates
- Testing Security Patches
- Change Management
- Deploy Patched
- Patch Validation
- Reporting
- Review and Improve

Purchasing

Unit	SKU	Description
Invinsense ODS	ICPL-INV-ODS-0110	With Patch Management and Deception Across Landscape, Invinsense ODS Makes it harder and confusing for adversaries to achieve their objective

About Infopercept - Infopercept is one of the fastest-growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Publisher

3rd floor, Optionz Complex, CG Rd, Opp. Regenta Hotel, Navrangpura, Ahmedabad, Gujarat 380009, INDIA

Contact

sos@infopercept.com
www.infopercept.com/knowledge/datasheets