Infopercept

Invinsense Cloud - Code, Manage, Repeat- The Three Pillars of Cloud Security Excellence

In an age defined by digital transformation, organizations increasingly rely on cloud technologies to drive innovation, scalability, and agility. However, this shift to the cloud introduces new security challenges and vulnerabilities. Infopercept, a leading platform based managed security services company, recognizes the critical need for robust cloud security solutions tailored to the evolving needs of modern businesses.

This whitepaper presents Infopercept's holistic approach to cloud security, through its cloud security platform 'Invinsense Cloud' emphasizing its unique methodology of "Code, Manage, Repeat." By integrating security into every phase of the cloud lifecycle, Invinsense cloud empowers organizations to navigate the complexities of the digital landscape with confidence, ensuring the confidentiality, integrity, and availability of their data and applications.

Invinsense Cloud's Security as Code Offerings:

1. **Infrastructure as Code (IaC) Security**
2. **Invinsense DevSecops**
   - Invinsense OXDR
   - Invinsense Vulnerability Management
   - Image Inspection

Invinsense Cloud Management of Security Offerings:

- Invinsense Cloud Security Posture Management
- Invinsense Cloud Work Load Protection
- Invinsense XDR and MDR
- Invinsense XDR+ and MDR+
- Invinsense OXDR and OMDR
- Invinsense GSOS

Invinsense Cloud - Code, Manage, Repeat- The Three Pillars of Cloud Security Excellence

Cloud security is a huge responsibility. Cloud has provided agility and scalability to the organizations. However, it has also increased the attack surface and has made entire landscape complex and difficult to secure.

Invinsense Cloud is our consolidated offering of cloud security solutions and services which takes care of your end-to-end security in the cloud in the three steps process: Code Manage Repeat.

Code: Invinsense Cloud provides 'security as a code' ensuring your applications and cloud infrastructure are fortified against potential threats right from their inception.

Manage: Under manage, Invinsense Cloud Security takes care of cloud detection and response, cloud discovery and exposure management, and cloud security compliances.

Invinsense cloud security supports any private cloud, public cloud - AWS, GCP, Azure, Oracle and all hybrid or multi cloud environments.

Invinsense Cloud- Code

Why code level security is the best practice?

Security as a Code is the best way to ensure a series of security measures to protect your assets in the cloud. There are many advantages of utilizing code for security in the cloud.

Reduces Complexity	Utilizing code allows for consistent application of security measures across different parts of the cloud system. This consistency reduces the complexity of applying security measures through GUI.
Reduces Human Error	As code allows automation, there are reduced chances of human error in the implementation of security protocols.
Enhances Scalability	With code, security measures can be made scalable according to the needs of the system. The security measures can be easily adapted to the increase of data stored or users accessing the cloud as it does not need extensive manual adjustments.
Aligns with DevOps Practices	Using code for security aligns well with DevOps practices, where security is integrated throughout the development process. This ensures the priority of the security left approach and it continues to be a priority as the system evolves.

Invinsense Cloud provides the following under Security as a Code:

1) Infrastructure as Code (IaC) Security

Securing Infrastructure as a Code (IaC) in the cloud is critical to maintain a secured environment for your resources and data. It is also crucial for building various best practices for your cloud environment. Under this we help you take care of the below:

Provision of Cloud Resources	Our engineering team utilizes various IaC tools like Terraform, Ansible, Google Cloud Deployment Manager, Azure Resource Manager, AWS CDK, AWS Cloud formation etc. to describe and deploy cloud resources facilitating automated, uniform, and consistent infrastructure and management.
Regular scanning of infrastructure and IaC Code	Invinsense engineering team sets up a security scanning process that regularly scans: • Infrastructure utilizing infrastructure security scanners like Terraform Sentinel, AWS Config Rules, Azure Policy, etc. to check for security compliance • IaC Code for security vulnerabilities and coding errors using tools like Terrascan, Checkov, etc.
Well Architected Framework	Utilizing IaC, we provide continuous implementation of best practices and guidance for designing and operating reliable, secure, efficient, and cost-effective well architected framework in your cloud environment.

2) Invinsense DevSecOps:

Cloud-native application development stands at the forefront of digital transformation's agility. While it accelerates development, it introduces complexities that challenge security teams. Invinsense DevSecOps harnesses a blend of culture, tools, and best practices to fortify applications and infrastructure, securing them from code to cloud.

Invinsense DevSecOps: Cultivating Culture and Best Practices:

Today, implementing DevSecOps isn't tough, but instilling it with optimal practices and embedding it within organizational culture remains a challenge. For instance, DevSecOps aids in identifying vulnerabilities during Dynamic Application Security Testing (DAST), Static Application Security Testing (SAST), and Interactive Application Security Testing (IAST). However, without a culture aligned with DevSecOps, reported vulnerabilities from DAST might go unaddressed due to business priorities overshadowing security concerns. Similarly, vulnerabilities identified through SAST and IAST may linger unpatched, accumulating in the queue of vulnerabilities.

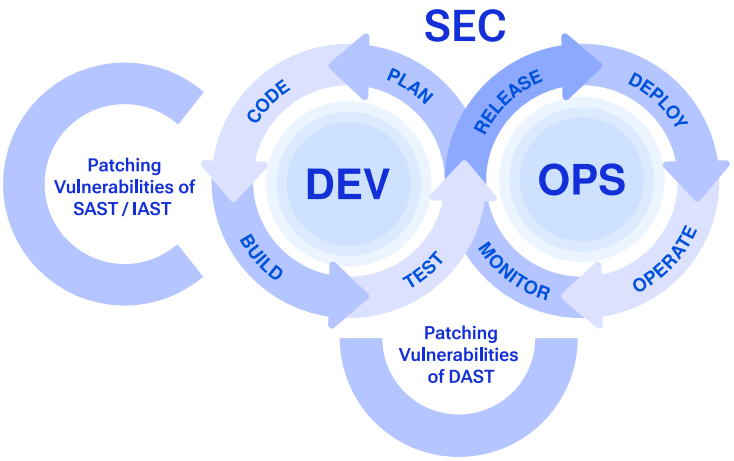

Figure 1 Invinsense DevSecOps in Action

Invinsense DevSecOps empowers the development of a culture that encompasses developers and processes, prioritizing the patching of application and infrastructure vulnerabilities. This approach seamlessly integrates with the development of business logic, ensuring timely vulnerability patches and averting potential delays.

Invinsense DevSecOps: An Ecosystem of Tools Ensuring Security for Cloud-Native Infrastructure and Applications

Invinsense Offensive Extended Detection and Response (OXDR):

This platform offers a comprehensive suite of offensive security tools integrated into a single platform. It combines RedOps, Continuous and Automated Red Teaming (CART), Vulnerability Management, and Breach and Attack Simulations (BAS). RedOps, CART, and BAS collectively identify vulnerabilities across various phases, while Vulnerability Management (VM) consolidates and centralizes all reported vulnerabilities.

Invinsense Vulnerability Management:

At the core of Invinsense DevSecOps, this aspect centralizes reported vulnerabilities from static and dynamic code analysis, software composition analysis, CIS review, manual application vulnerability testing, and image inspection. Invinsense VM collates these vulnerabilities, offering a centralized view. This consolidation helps in eliminating duplicates, establishing workflows, and tracking tasks.

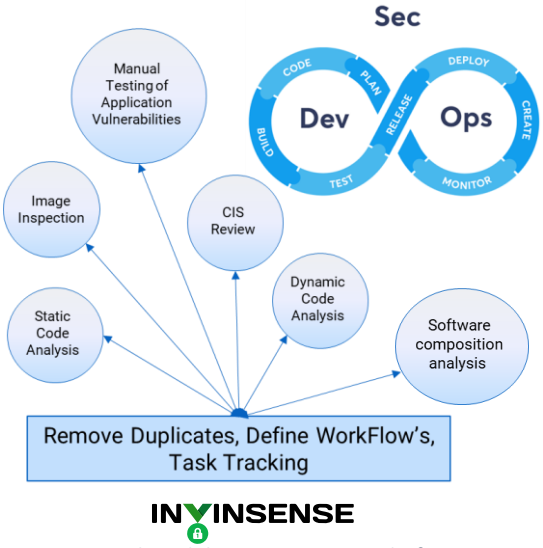

Figure 2Vulnerability Management Platform

Image Inspection

Invinsense VM leverages NeuVector's Image Inspection to identify and report vulnerabilities within images.

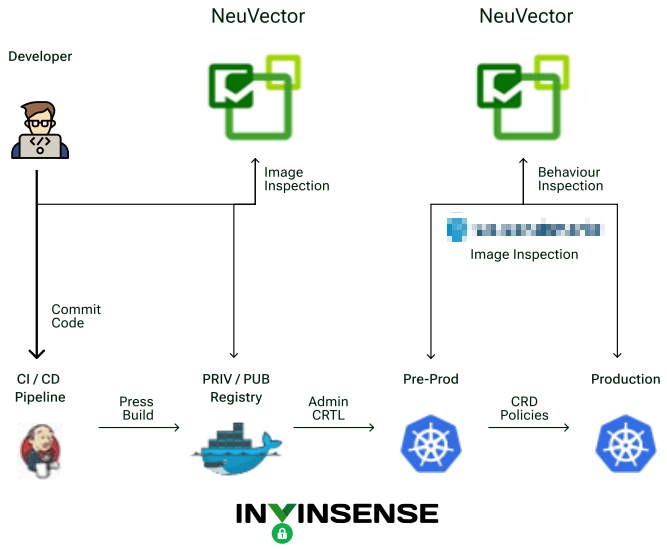

Figure 3Vulnerability & Compliance Management

Invinsense Cloud- Manage (Management of tools and processes by experts)

Invinsense Cloud provides the following under Management of Security:

1) Invinsense Cloud Security Posture Management

Invinsense cloud security posture management gives you the complete visibility of your cloud environment. It supports multi-cloud security audits and helps you in maintaining security and compliance of your cloud environment.

Using the APIs exposed by various cloud providers, Invinsense CSPM gathers data across your multi-cloud and hybrid environment and highlights risk areas. It presents a single view of the cloud attack surface.

It provides the following:

Improved Visibility — Provides a consolidated monitoring view of security across multi-cloud and hybrid environments. This helps the security team to have better visibility and control over cloud assets.

Enhanced Security — Continuous monitoring and automated checks help identify and mitigate security vulnerabilities and misconfigurations. Alerts and remediation helps improve cloud security posture.

Compliance Assistance — It helps with adherence to various cloud security compliances by ensuring consistent security configuration and policies across your cloud environments.

Risk Reduction — It minimizes the risk of data breaches due to misconfigurations and unauthorized access.

Enhances Incident and Response — It enhances incident and response by providing required insight of security incidents.

The following cloud providers are currently supported:

- Private Clouds
- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform
- Alibaba Cloud (alpha)
- Oracle Cloud Infrastructure (alpha)
- Kubernetes clusters on a cloud provider (alpha)

2) Invinsense Cloud Workload Protection:

Every organization has various computer infrastructure like VMs, monolithic servers, hosts, containers, Kubernetes, and serverless architecture for its cloud-native applications.

Security of each of these computer infrastructures needs different approaches and tools.

Invinsense cloud workload protection covers all of them to provide secure deployments covering the entire application lifecycle.

For Applications on Monolithic server and Windows, Mac and Linux Operating Systems

Invinsense Defense in Depth is a five layered single agent security tool for protecting your cloud applications. It provides layered security to your applications.

Layer 1 (Windows firewall and Defender) prevents from known attacks, layer 2 (OS Query) provides user based behavior analysis, layer 3 (Invinsense EDR) provides end point detection and response, layer 4 (Microsoft Sysmon) increases visibility in depth and breadth, and layer 5 uses deceptive files to trap adversaries.

For Container and Kubernetes Security

Enterprises deploying containers need to ensure they meet the highest level of security for containers and Kubernetes.

Invinsense uses NeuVector for container and Kubernetes security. NeuVector is a zero-trust, full-lifecycle container security platform designed to safeguard cloud-native applications from build to deployment. It offers comprehensive features such as vulnerability scans, image assurance, runtime security, and network segmentation.

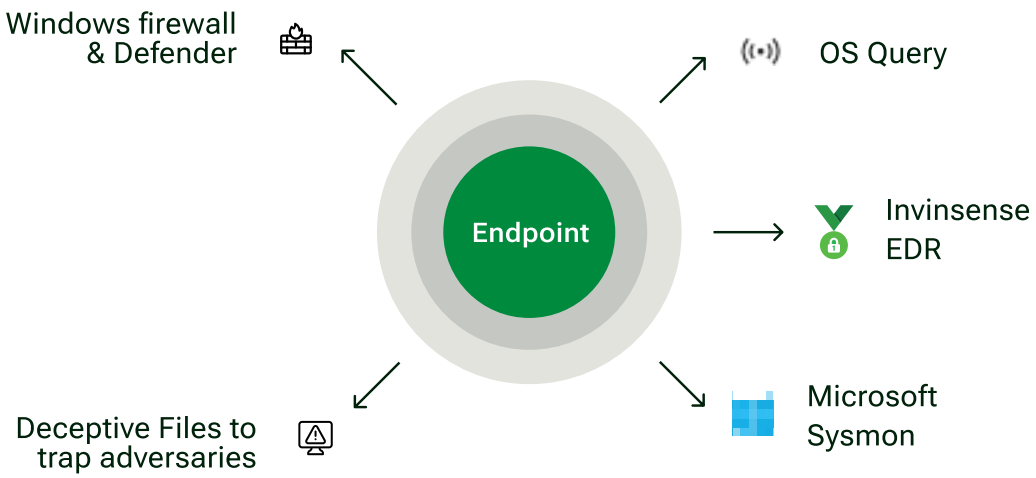

Figure 4 Tiered endpoint security ecosystem

3) Invinsense Extended Detection and Response (XDR) and Managed Detection and Response (MDR)

Our XDR solution focuses on defensive security, empowering organizations to establish their own detection and response systems. Invinsense XDR seamlessly integrates various detection and response tools, such as SIEM, SOAR, EDR, Threat Intelligence, Threat Exchange, and Case Management. These tools communicate with each other, exchanging intelligence to form the "defender's brain," which aids organizations in enhancing their detection and response efforts.

Under Invinsense MDR, our blue team takes care of your entire XDR solution and runs a 24x7 security operations center on your behalf.

4) Invinsense Extended Detection and Response Plus (XDR+) and Managed Detection and Response plus (MDR+)

XDR+ goes beyond defensive security by including deception and patch management. Organizations often face vulnerabilities that require quick patches and others that demand more time. Our patch management feature addresses vulnerabilities with shorter patch times, while our deception technology allows organizations to create decoys for longer-patch vulnerabilities. This approach buys organizations time to patch these vulnerabilities, ultimately aiding in threat detection. XDR+ contributes the "attacker's mind" to the detection and response efforts of any organization.

Under MDR+, our purple team takes care of the patch management and deception by managing your XDR+ on your behalf.

5) Invinsense Offensive Detection and Response (OXDR) and Offensive Managed Detection and Response (OMDR)

OXDR specializes in offensive security, employing tools like Vulnerability Management, Breach and Attack Simulation, Red Ops, and Continuous Automated Red Team. This solution assists organizations in identifying vulnerabilities within their people, processes, and technologies and effectively managing them. OXDR equips organizations to simulate attacker's actions, preparing them for sophisticated attacks.

Under OMDR, our red team manages your OXDR and carry out various attacks to test your defence regurarly.

6) Invinsense GSOS (Govern Secure Optimize and Strengthen)- our GRC platform and compliance team

GSOS serves as a compliance platform, guiding organizations through various security compliances, cybersecurity strategies, and cybersecurity awareness. It functions as a roadmap for organizations to progress on their cybersecurity maturity journey.

In our managed services, our compliance team with the help of Invinsense GSOS helps you with all kinds of security compliances.

Invinsense Cloud- Repeat

Security in the cloud is a continuous process. We believe in the philosophy and we run all of the above security services on a 24x7 format.

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/white-paper