Cognizant Managed Microsegmentation Solution

Overview

As enterprises adopt cloud-first strategies and hybrid infrastructures, traditional perimeter-based security models are becoming obsolete. The dynamic nature of modern workloads, distributed applications, and remote access patterns introduces new challenges in maintaining consistent and effective security controls. Threat actors increasingly exploit internal network pathways, making lateral movement a major concern. This exposes organizations to risks such as data exfiltration, ransomware propagation, privilege escalation, and operational disruptions—each with potential regulatory and reputational consequences.

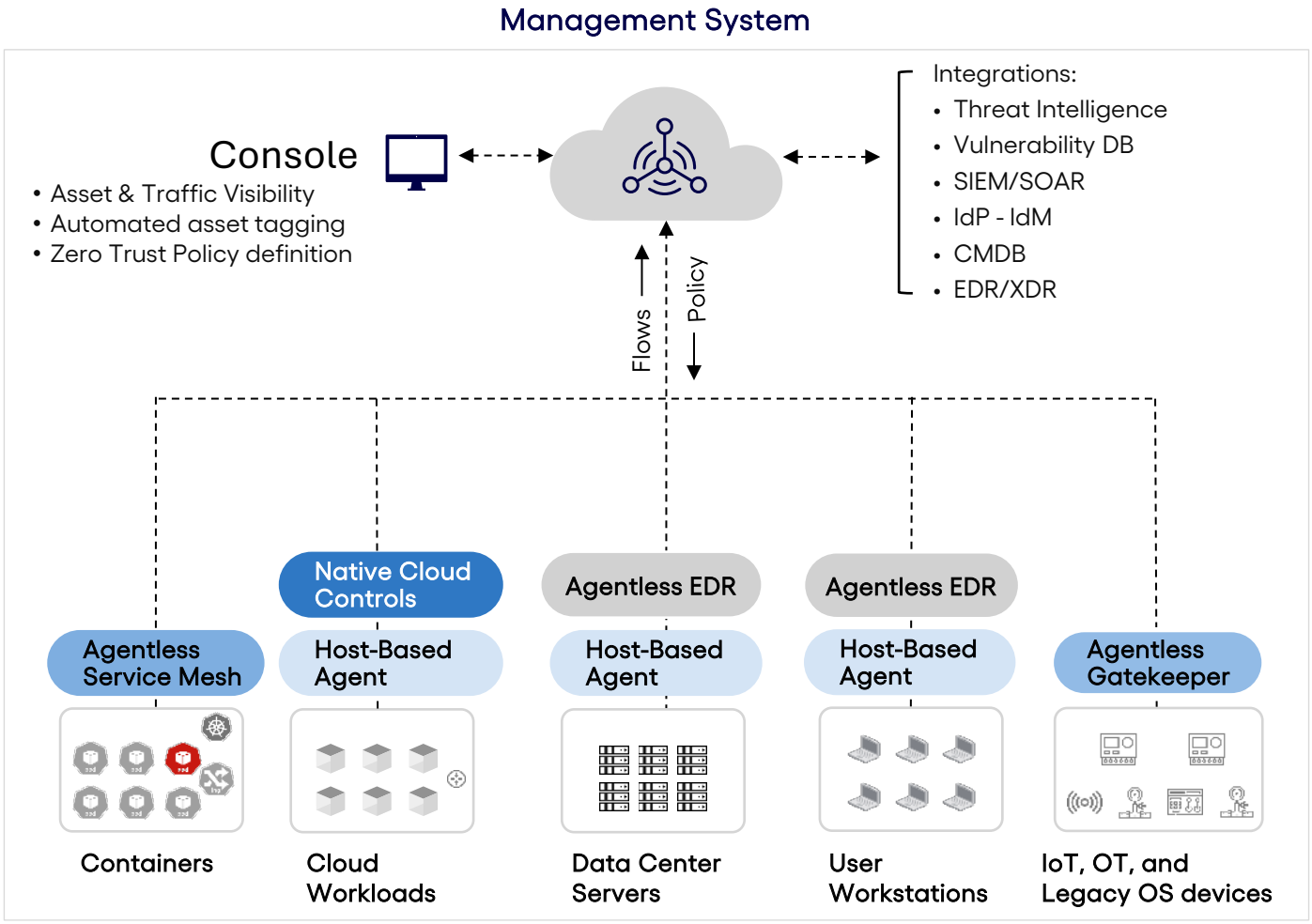
Key Challenges Driving Microsegmentation Adoption

- Data Exfiltration – Attackers can move laterally to locate and steal sensitive data, leading to regulatory violations and reputational damage.
- Persistence and Stealth – Threat actors establish backdoors and maintain long-term access, often remaining undetected for extended periods.
- Privilege Escalation – Attackers gain administrative rights, allowing full control over systems and disabling security tools.
- Operational Disruption – Critical systems like HR, finance, or manufacturing can be compromised, causing downtime and productivity loss.
- Ransomware Spread ransomware can propagate quickly across the network, amplifying the impact of a breach.
- Compliance Failures – In regulated industries, uncontrolled lateral movement can result in non-compliance with standards like HIPAA, PCI-DSS, or GDPR.

Cognizant Approach

To counter evolving cyber threats, organizations should reassess internal security architectures. A key strategy recommended is granular, workload-level segmentation that goes beyond traditional VLANs and firewalls. Microsegmentation enables dynamic policy enforcement, enhanced visibility, and tighter control over east-west traffic within datacentres and cloud environments. By isolating workloads and applying context-aware policies, it reduces the attack surface, contains breaches, and supports compliance across multi-cloud ecosystems—strengthening internal defences and aligning with secure digital transformation goals.

This Microsegmentation approach provides a unified framework to secure diverse IT environments through deep visibility and granular policy enforcement. It starts with a centralized console for asset discovery, automated tagging, and Zero Trust policy definition. Subsequently, connects to a management system that orchestrates traffic flows and security policies across workloads. The solution integrates with enterprise tools like threat intelligence platforms, SIEM/SOAR, CMDBs, identity providers, and EDR/XDR. It supports multiple deployment models—agentless service mesh, native cloud controls, host-based agents, and gatekeepers for IoT/OT/legacy systems—empowering organizations to secure both modern and legacy infrastructures while maintaining operational agility.



Key Capabilities

- Granular Access Control: Enables fine-grained segmentation of critical assets to enforce least-privilege access.
- Legacy System Containment: Restricts communication paths for outdated or proprietary systems lacking modern security controls.
- Threat Containment: Limits lateral movements and blast radius of threats like ransomware through strict access enforcement.
- Standards-Based Segmentation: Supports industry frameworks such as ISA/IEC 62443 and NIST SP 800-82 for ICS/OT environments.
- Regulatory Compliance Enablement: Facilitates adherence to mandates like SEC 8-K / Item 106 and PCI DSS via policy enforcement and auditability.
- Cloud-Native Policy Enforcement: Applies identity-based security policies across dynamic cloud workloads, including containers and microservices.
- Unified Visibility and Control: Integrates with enterprise tools for centralized management and monitoring across hybrid environments.

Use Cases

Crown Jewel Protection: Securing sensitive assets like PII, IP, EHR, and Active Directory

Vulnerability Management: Containing legacy and proprietary systems lacking modern controls

Ransomware Resiliency: Limiting spread and impact of ransomware attacks

ICS/OT Segmentation: Isolating and protecting industrial and operational technology environments

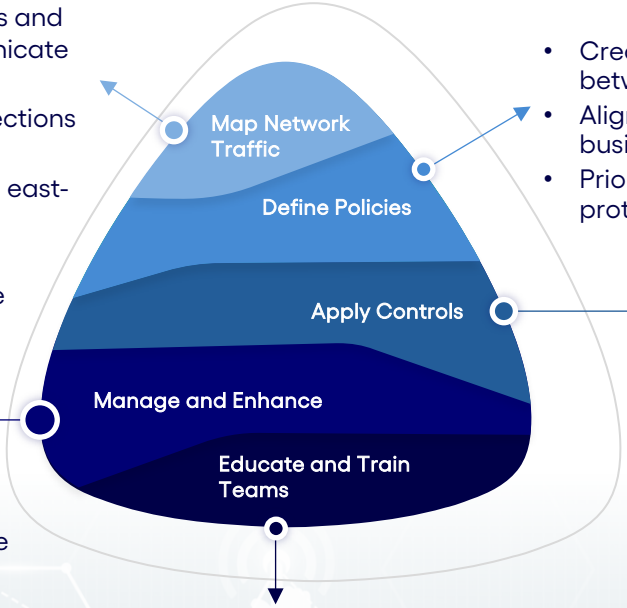
Compliance and Assurance: Meeting mandates such as SEC 8-K / Item 106 and PCI DSS

Cloud Native Security: Securing microservices and Kubernetes clusters in dynamic cloud setups

Our Offerings:

Cognizant's Managed Microsegmentation offering provides a structured approach to help organizations reduce lateral movement, enforce least-privilege access, and strengthen internal security across hybrid environments. The offering guides clients through a phased implementation journey, from traffic mapping and policy definition to control deployment, monitoring, and team enablement. Ensuring alignment with Zero Trust principles and operational resilience.

- Discover how systems and applications communicate across environments
- Identify critical connections and dependencies
- Establish visibility into east-west traffic patterns



- Create least-privilege access rules between workloads
- Align segmentation policies with business and compliance needs
- Prioritize high-risk assets for protection

- Continuously observe traffic and policy effectiveness
- Refine segmentation rules based on evolving threats and changes
- Maintain security posture with adaptive controls

- Enforce policies using scalable, non-disruptive tools
- Support agent-based and agentless deployment models
- Ensure compatibility across cloud, data center, and legacy systems

- Enable IT and security teams with tool-specific training
- Promote best practices for policy management and incident response
- Foster a culture of proactive security operations

Benefits:

Architecture

Business-Aligned Architecture: Domain-centric reference architectures ensure solutions are tailored to specific business needs, driving better outcomes.

Enhanced Security Through Automation: AI-driven automation enables proactive threat detection and mitigation, improving overall security posture.

Deployment

Rapid Deployment: Accelerators ensure fast-track deployment with minimal risk through golden templates, validated checklists, and standardized policies.

Seamless Integration and Adoption: Frictionless onboarding with smooth integration into existing services minimizing disruption and accelerating value realization.

Access to Expert Talent: A large pool of over 1500 certified professionals ensure high-quality execution and support.

Commercial

Cost Efficiency and Scalability: Flexible operating and commercial models help organizations optimize costs while scaling securely.

Why Choose Cognizant

With over 1500 certified professionals and a proven set of accelerators, Cognizant's microsegmentation solutions deliver scalable, domain-aligned security tailored for enterprise environments. Leveraging golden templates and standardized policies, these solutions enable rapid, failsafe implementation while ensuring consistency and compliance. Cognizant's automation-first approach, flexible operating models, and seamless integration capabilities simplify adoption and enhance threat protection—empowering organizations to embrace Zero Trust with confidence and efficiency. Contact us today to discover how we can help you achieve unparalleled security and efficiency. To know more contact – cybersecuritypulse@cognizant.com

Cognizant helps engineer modern businesses by helping to modernize technology, reimagine processes and transform experiences so they can stay ahead in our fast-changing world. To see how Cognizant is improving everyday life, visit them at **www.cognizant.com** or across their socials **@cognizant**.

World Headquarters

300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

280 Bishopsgate
London
EC2M 4RB England
Tel: +44 (01) 020 7297 7600

India Operations Headquarters

5/535, Okkiam Thoraipakkam,
Old Mahabalipuram Road,
Chennai 600 096
Tel: 1-800-208-6999
Fax: +91 (01) 44 4209 6060

APAC Headquarters

1 Fusionopolis Link, Level 5
NEXUS@One-North, North Tower
Singapore 138542
Tel: +65 6812 4000