Cognizant's Secure Cloud Services powered by Microsoft Defender

Industry Overview

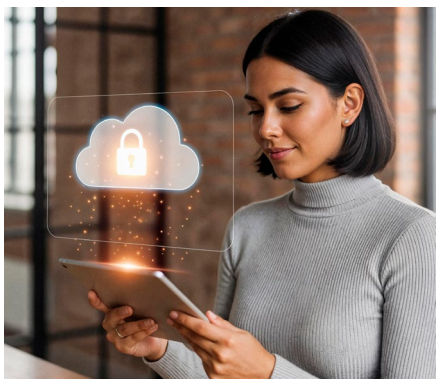
Cloud adoption is accelerating at an unprecedented pace, redefining how modern enterprises operate and innovate. Organizations across all sectors are strategically embracing hybrid and multicloud environments to maximize agility, scalability, and cost efficiency. This transition is vital for enabling faster application deployment, delivering superior customer experiences and seamlessly integrating emerging technologies. By strategically migrating critical workloads to the cloud, businesses unlock powerful opportunities for global expansion, ensure operational resilience, and enhance data-driven decision-making capabilities. Cloud platforms serve as the essential engine for digital transformation, empowering enterprises to modernize legacy infrastructure, optimize IT investments, and respond decisively to evolving market demands, thereby securing a definitive competitive advantage through enhanced collaboration and the ability to scale securely across global geographies. While hyperscalers provide robust infrastructure-level security and identity controls, organizations remain responsible for managing access, governance, and compliance at the data layer, ensuring Zero Trust principles adoption to provide secure, granular, and auditable access, sharing, and collaboration across multi-cloud and hybrid environments.

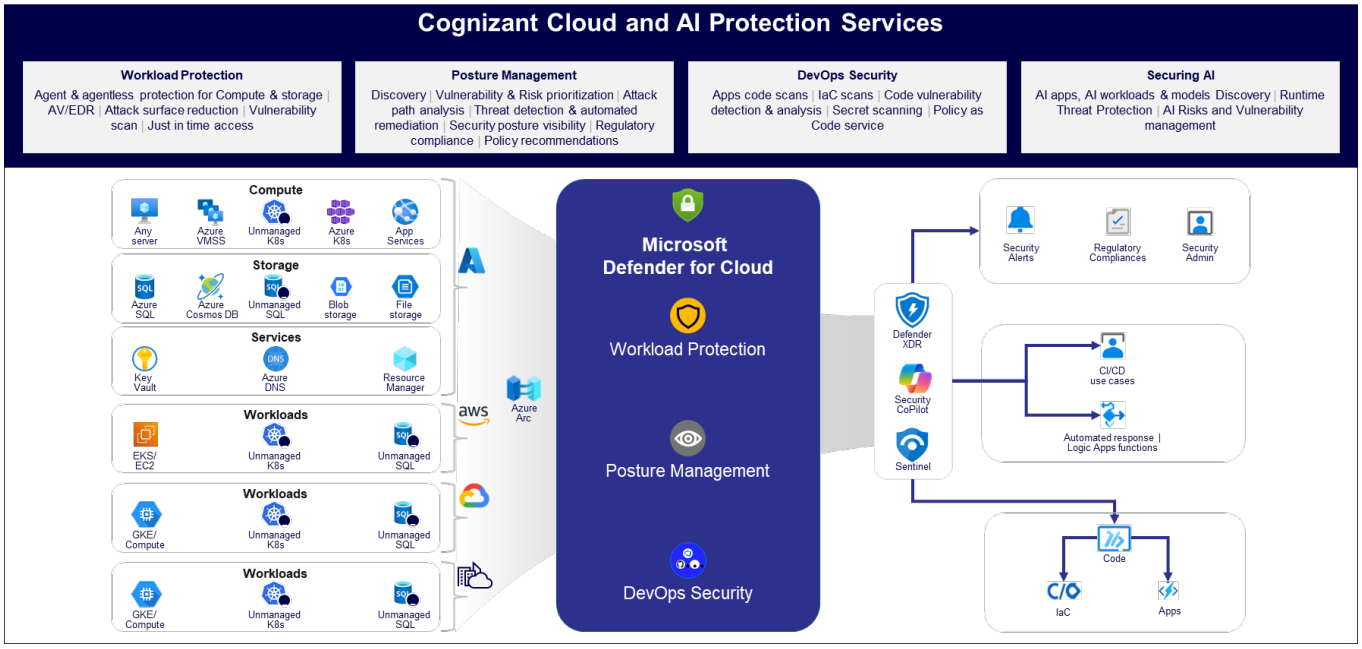
Key Challenges:

- Fragmented security landscape: Organizations depend on multiple, siloed tools to secure workloads across hybrid and multicloud environments, creating complexity and visibility gaps. The lack of a centralized security platform makes it challenging to enforce consistent policies and maintain unified oversight across servers, containers, and applications.
- Limited visibility across environments: Enterprises lack unified visibility and control, making it challenging to consistently monitor and secure assets across on-premises, cloud, and edge environments due to siloed tools and fragmented data
- Inconsistent compliance posture: Maintaining regulatory compliance becomes complex when policies are applied unevenly across hybrid infrastructures, leading to audit failures and increased risk exposure.
- Traditional threat response: Security teams face delays in mitigating threats because of fragmented workflows and lack of automation, resulting in prolonged dwell times and higher breach impact.
- Cloud misconfiguration risks: Manual processes and inconsistent configurations expose sensitive data and increase breach likelihood.
- Scalability challenges: Traditional security solutions fail to scale with dynamic workloads and containerized applications, creating blind spots and operational inefficiencies.
- Dev SecOps integration gaps: Security checks are often applied late in the development lifecycle, leaving IaC templates and CI/CD pipelines vulnerable and slowing secure application delivery.

Solution

Cognizant strengthens its Secure Cloud Services by leveraging Microsoft Defender for Cloud's advanced capabilities, including Cloud Workload Protection (CWP). CWP delivers real-time threat detection and protection for virtual machines, containers, Kubernetes clusters, and databases, ensuring workloads remain secure across multi-cloud and on-premises environments. By extending coverage through Azure Arc, Cognizant provides centralized security and compliance controls across hybrid deployments simplifying posture management with continuous visibility, enforcing consistent policies and enabling automated remediation at scale.





To strengthen security throughout the development lifecycle, the solution leverages Defender for Cloud's built-in DevSecOps capabilities to embed security checks from code to cloud. It scans Infrastructure-as-Code templates and application code in repositories like GitHub and GitLab for vulnerabilities and compliance gaps, while CI/CD pipelines enforce pre-deployment security validations, secret scanning, and policy controls to block insecure deployments. Runtime protections, including image scanning and container security, safeguard Kubernetes workloads and registries, ensuring vulnerabilities are addressed early without slowing innovation.

The approach also addresses emerging risks in AI-driven environments by leveraging Defender for Cloud's AI-integrated security capabilities. These features identify generative AI resources, workloads, and models in use, providing visibility into potential risks. Threat protection for AI services, vulnerability detection in container images and AI code repositories, and data security for Azure AI interactions ensure safe adoption of AI technologies. Real-time dashboards deliver compliance posture and risk insights, enabling enterprises to innovate confidently while maintaining trust and regulatory adherence.

Key Capabilities

- Cloud Security Posture Management (CSPM): Continuous assessment of cloud environments with vulnerability detection, attack path analysis, compliance enforcement, and security posture improvement.
- Cloud Workload Protection (CWP): Advanced protection for VMs, servers, Kubernetes clusters, containers, and databases, including image scanning and runtime threat detection.
- Cloud DevOps Security: Security integrated into CI/CD pipelines with IaC scanning, code vulnerability analysis, pre-deployment checks, secret scanning, and policies to block insecure deployments.
- AI Security (via Microsoft Defender for Cloud): Advanced protection for AI workloads and services, including identification of generative AI models, vulnerability detection in container images and code repositories, and threat protection for AI interactions.
- Multicloud & On-Prem integration: Unified visibility and control across AWS, GCP, Azure, and on-premises environments via Azure Arc, covering servers, containers, applications, and databases.
- Actionable insights & dashboards: Real-time discovery of data and AI resources, prioritized security risks, and vulnerability snapshots for proactive threat management and compliance.

Use Cases

- Enforcing zero trust across hybrid and multi-cloud environments to prevent unauthorized access and insider threats
- Maintaining consistent security posture across Azure, AWS, and GCP for global enterprises adopting multi-cloud strategies
- Automating compliance reporting for regulated industries to reduce audit preparation time and avoid penalties
- Improving cloud security posture using CSPM to continuously assess, prioritize, and remediate risks across cloud platforms.
- Detecting and remediating cloud misconfigurations to prevent data exposure and reduce attack surface.
- Integrating secured DevOps practices to embed security into CI/CD pipelines and ensure secure code delivery.

Our Offerings:

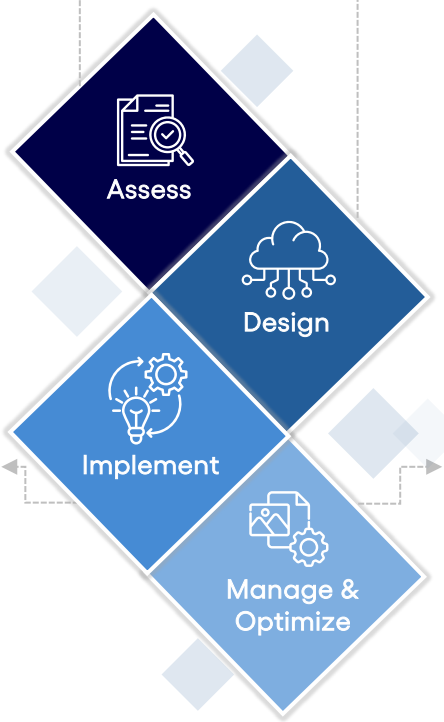
Cognizant helps organizations evaluate their cloud security posture, define a target state, and implement a transformation roadmap powered by Microsoft Defender for Cloud. Our methodology and approach span four key stages:

Assess: Analyse workloads across Azure, hybrid and multicloud to determine security needs by:

- Reviewing network architecture, threat protection needs, and just-in-time access.
- Perform risk and compliance evaluations.
- Set baseline Secure Score and identify protection gaps
- Define security policies and agent requirements.

Implement: Enable Defender for Cloud across and automate:

- Deploy extensions, subscriptions and agents.
- Configure workloads for Zero Trust across environments.
- Integrate Azure Logic Apps for automated remediation.
- Enforce policies and Identity management.



Design: Create a Defender for Cloud blueprint based zero trust principles:

- Document high/low-level designs for containers & Kubernetes
- Define hybrid/multi-cloud architecture
- Align compliance strategy with business goals via workshops
- Establish foundation for implementation

Manage & Optimize: Ensure continuous security and efficiency:

- 24x7 proactive threat monitoring and alert prioritization.
- Monitoring Azure and non-Azure resources for vulnerabilities.
- Generate posture reports with actionable insights.
- Automate remediation to improve Mean Time to Resolution (MTTR).
- Continuous compliance and control optimization.

Benefits:

Architectural benefits:

Design Efficiency: Standardized templates for reduced design time and consulting costs, accelerating project delivery.

Platform-Native Threat Intelligence: Integration with Microsoft Defender for Cloud enhances threat detection and response capabilities, reducing dependency on third-party tools and streamlining security operations across cloud environments.

Future-Proof Investment: Modular architecture supports evolving business needs, protecting long-term IT investments.

Business Continuity Assurance: Resilient infrastructure ensuring uptime for critical workloads, minimizing revenue disruption.

Deployment benefits:

Faster Time-to-Value: Pre-built blueprints and automation accelerate deployment, reducing onboarding costs and enabling quicker ROI.

Operational Cost Savings: Auto-remediation and policy enforcement limiting manual effort and lowering operational overhead.

Improved SLA Performance: Proactive monitoring and reduced MTTR help meet service-level commitments and avoid penalties.

Commercial benefits:

Unified risk management: Gain centralized oversight across cloud environments, reducing the cost and complexity of managing fragmented security tools.

Accelerated Compliance Readiness: Automated regulatory checks help avoid fines and reduce audit preparation time, improving time-to-market for regulated workloads.

DevOps Cost Optimization: Early detection of misconfigurations in Infrastructure as Code (IaC) reduces rework and deployment delays, saving engineering hours.

Zero Trust-Driven Risk Mitigation: Strengthens data protection and operational integrity, helping organizations maintain compliance, reduce cyber insurance costs, and enhance stakeholder confidence.

Cost reduction: Security controls scale with workloads, allowing predictable budgeting and cost management.

Cloud Investment Protection: Seamless multi-cloud coverage ensures consistent security posture across Azure, AWS, and GCP—maximizing existing cloud investments.

Why Choose Cognizant

Cognizant is a Global Systems Integrator (GSI) and a specialized partner across all four Microsoft Security solution areas—Threat Protection, Cloud Security, Identity & Access Management, and Information Protection & Governance. With deep domain expertise and a proactive approach to cybersecurity, Cognizant helps enterprises build a robust security posture and accelerate digital trust. Our certified security professionals and analysts deliver scalable, compliant and resilient solutions tailored to industry-specific needs. To know more contact – cybersecuritypulse@cognizant.com

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

cognizant®