July 22, 2026

CR PULSE

Modernizing Cyber Defense With Cognizant Cybersecurity Services

How Cognizant Helps Enterprises Move From Fragmented Security to Cyber Resilience Through Neuro Cybersecurity and AI-Infused Workflows



Chirag Mehta
VICE PRESIDENT AND PRINCIPAL ANALYST

constellation™ RESEARCH

Produced exclusively for Constellation Research clients

EXECUTIVE SUMMARY

Cybersecurity services are entering a new phase as enterprises face faster attacks, expanding digital environments, persistent talent shortages, and rising pressure to improve resilience. Security leaders are moving beyond traditional managed detection and response toward operating models that connect telemetry, context, reasoning, action, and verification across the security program.

This Constellation Research Pulse report explores Cognizant Cybersecurity Services and its approach to helping enterprises modernize security operations, improve resilience, and manage emerging AI-related risk. The report highlights Cognizant's managed cybersecurity capabilities, Neuro Cybersecurity, Cyber Defense Centers, agentic security workflows, and security for AI, along with buyer considerations for organizations seeking to strengthen cyber defense across complex, hybrid, and AI-enabled environments.

BUSINESS THEMES

- New C-Suite
- Technology Optimization
- Digital Safety and Privacy

© 2026 Constellation Research Inc. All rights reserved.

MARKET DESCRIPTION

Cybersecurity services help organizations design, implement, operate, and improve security programs across complex digital environments. The market remains anchored in two major service categories: implementation services and managed services. Implementation services focus on security architecture, technology deployment, integration, modernization, and transformation. Managed services focus on continuous monitoring, detection, investigation, response, threat hunting, exposure management, and program operations.

The category has expanded as enterprise security programs have become harder to run with internal teams alone. Organizations now operate across cloud, software as a service, identity platforms, endpoints, networks, operational technology, data platforms, and AI systems. They must also respond to new regulatory requirements; increased board scrutiny; persistent talent shortages; and attackers that can move across identity, applications, infrastructure, and software supply chains. As a result, buyers look for cybersecurity service providers that can combine technical depth, operational maturity, global delivery, and measurable security outcomes.

The market is also moving beyond traditional managed security services. Buyers no longer want only alert monitoring or staff augmentation. They want security partners that can help connect telemetry, context, reasoning, action, and verification across the security environment. This creates demand for providers that can modernize the security operations center (SOC), integrate DevSecOps practices, apply threat intelligence to business risk, and bring automation into routine security work without losing control, auditability, or human judgment.

AI is now a core market shift. Service providers are using AI-assisted analytics, copilots, and agent-based workflows to improve detection, reduce manual investigation, summarize evidence, recommend response actions, and support continuous validation. The next phase will be more architectural than tool-driven. Agentic SOC models will coordinate work across detection, investigation, response, reporting, and verification. Autonomous security systems, including Mythos-class[1] vulnerability discovery and validation systems, will raise expectations for continuous testing, exploitability analysis, remediation prioritization, and secure software delivery. This will also increase the need for governance, policy enforcement, and clear human-in-the-loop controls.

Cybersecurity services now sit at the intersection of security operations, engineering, compliance, resilience, and AI governance. Leading providers will be judged less by the number of tools they operate and more by their ability to improve security posture, reduce dwell time, accelerate response, support secure development, validate controls, and help customers adapt to a threat landscape where attackers as well as defenders are using AI.

TRENDS

Based on recent conversations with C-suite technology and security leaders in Constellation's BT150[2] and AX100[3] networks, plus ongoing customer and vendor briefings, primary research, and cybersecurity services market analysis, Constellation observes clear patterns in how organizations are rethinking security operations. The trends below capture what is driving strategy, investment, and adoption as enterprises move from human-orchestrated security workflows toward AI-assisted, agentic, and autonomous security operating models.

The security operating model becomes agentic: SOC teams are moving from alert queues to coordinated workflows across telemetry, context, reasoning, action, and verification.

AI-assisted services shift from productivity to outcomes: Buyers expect AI to reduce false positives, accelerate triage, shorten response times, and improve analyst consistency.

© 2026 Constellation Research Inc. All rights reserved.

Autonomous security raises the bar for DevSecOps: Mythos-class systems point to a future in which exploit validation, vulnerability prioritization, and remediation guidance become continuous parts of software delivery.

Continuous verification becomes core to managed services: Customers want evidence that controls are working across identity, cloud, endpoints, applications, data, and networks.

Identity, cloud, data, and application security converge: Providers must connect these domains as attackers move across permissions, misconfigurations, exposed data, and software weaknesses.

AI security becomes a services growth area: Enterprises need help securing copilots, agents, retrieval-augmented generation (RAG) systems, AI data flows, and agent tool use.

Managed services move from labor scale to platform-enabled delivery: Providers are using automation, playbooks, shared telemetry, and AI-assisted workflows to improve scale and service quality.

Governed autonomy becomes a buyer requirement: Customers need clear approval flows, audit trails, rollback options, and human oversight for AI-assisted and automated actions.

Threshold Criteria

Constellation considers the following criteria for these solutions:

- **Security architecture and implementation expertise across hybrid, multicloud, identity, endpoint, network, data, and application environments**
- **Integration discipline across security tools, IT systems, DevSecOps pipelines, cloud platforms, and existing SOC workflows**
- **Managed detection, response, threat hunting, and incident response maturity**
- **AI-assisted security operations, including detection, investigation, summarization, enrichment, and response recommendations**
- **Agentic SOC and workflow automation capabilities with appropriate human oversight and auditability**
- **DevSecOps, application security, and autonomous vulnerability validation readiness**
- **Continuous control validation, exposure management, and measurable posture improvement**
- **Scalable global delivery, regulatory expertise, operational maturity, and customer references**

© 2026 Constellation Research Inc. All rights reserved.

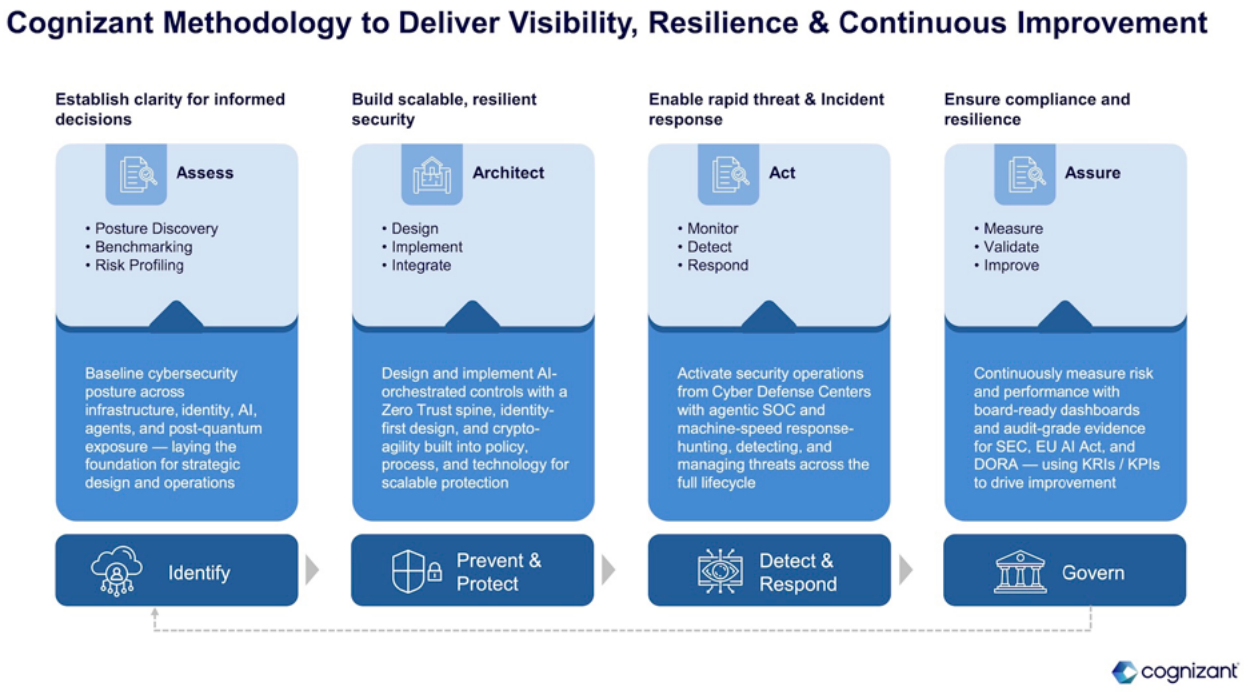
VENDOR UPDATE

Cognizant Cybersecurity Services is positioning its offering around "cyber resilience, delivered," with a focus on helping enterprises modernize security programs across cloud, infrastructure, identity, data, applications, AI systems, and security operations. The offering is designed for organizations grappling with fragmented security architectures, tool sprawl, alert fatigue, limited context, governance gaps, and rising board-level pressure to improve resilience. Cognizant maps these challenges to a model built around consolidated architecture, contextual intelligence, and continuous cyber defense.

Cognizant's delivery model comprises an assess, architect, act, and assure lifecycle (see Figure 1). Customers can use this model to baseline cybersecurity posture; design and integrate controls; operate detection and response via Cognizant Cyber Defense Centers; and continuously measure risk, performance, compliance, and resilience. The approach spans infrastructure, identity, AI, agents, and postquantum exposure, giving Cognizant a broad services entry point across security modernization and managed cybersecurity.

The company's managed cybersecurity offering is powered by Cognizant Neuro Cybersecurity, an AI orchestration layer across Cyber Threat Defense, Cyber Threat Intelligence, Cyber Workload Protection, Cyber Vulnerability Management, and Cyber Risk Management. Cognizant supports this model through Cyber Defense Centers in Bengaluru and Chennai, India, and Denver, Colorado. The result is a modular managed service model that helps customers connect SOC operations, risk visibility, workload protection, vulnerability management, and threat intelligence without requiring a full replacement of their existing security stack.

Figure 1. Cognizant's Methodology Moves Customers From Assessment and Architecture to Active Cyber Defense and Continuous Assurance, Connecting Visibility, Resilience, Response, and Governance



Source: Cognizant

© 2026 Constellation Research Inc. All rights reserved.

Offering Highlights

Cognizant organizes its cybersecurity services around seven service areas, or "seven towers of cyber-resilience": governance, risk, and compliance; data security and privacy; identity and access management; cloud, infrastructure, and network security; threat and vulnerability management; incident management and response; and security for AI (see Figure 2). These areas give Cognizant multiple entry points into a customer's security program, from compliance and data protection to zero trust, vulnerability management, incident response, postquantum readiness, and AI security.

The managed services anchor is Cognizant Managed Cybersecurity, powered by Neuro Cybersecurity. Cognizant positions Neuro Cybersecurity as an AI orchestration layer across five managed service modules: Cyber Threat Defense, Cyber Threat Intelligence, Cyber Workload Protection, Cyber Vulnerability Management, and Cyber Risk Management. These modules support SOC and risk operations center use cases such as user and entity behavior analytics (UEBA); security orchestration, automation, and response (SOAR); next-generation security information and event management (SIEM); threat intelligence; dark web monitoring; endpoint protection; extended detection and response; attack surface management; application scanning; infrastructure vulnerability management; regulatory compliance; risk quantification; and risk reporting. Cognizant supports this model through Cyber Defense Centers in Bengaluru, Chennai, and Denver.

Cognizant's AI-for-security approach is staged across assisted, augmented, and autonomous use cases. The assisted stage focuses on practical improvements such as alert enrichment, incident summarization, and vulnerability threat correlation. The augmented stage expands into risk-based vulnerability prioritization,

Figure 2. Cognizant Organizes Its Cybersecurity Services Into Seven Towers of Cyber Resilience, Supported by Neuro Cybersecurity Orchestration and a Staged Path From Assisted to Autonomous AI



Source: Cognizant

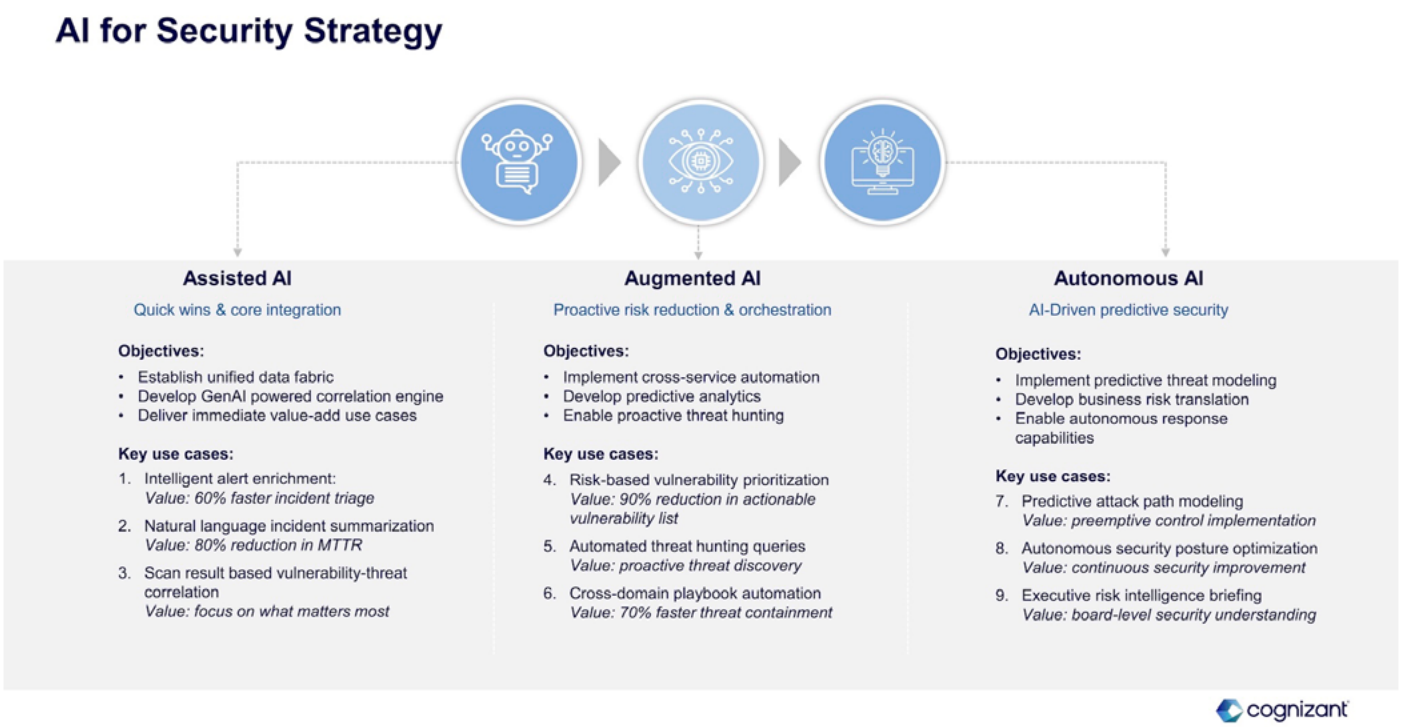
© 2026 Constellation Research Inc. All rights reserved.

automated threat hunting queries, and cross-domain playbook automation. The autonomous stage focuses on predictive attack path modeling, posture optimization, and executive risk intelligence. This staged model is useful, because most enterprises need a controlled path from AI-assisted analyst work to more-advanced agentic workflows.

Cognizant is also building agentic security workflows across several domains. In security operations, agents can support triage; root cause analysis; indicator of compromise (IOC) enrichment; response workflows; and SOAR automation. In vulnerability management, agents can help score vulnerabilities, validate exploitability, generate remediation tickets, and route work to the right teams. In infrastructure security, agents can support firewall policy checks, posture review, cloud misconfiguration detection, drift detection, and containment. In identity, agents can help discover and govern human, machine, and AI agent identities; support just-in-time access; and reduce standing privilege. In governance and risk control (GRC), agents can help map controls, identify policy gaps, and gather audit evidence.

For customers adopting AI, Cognizant offers a Security for AI testing framework (see Figure 3) that covers governance and risk, threat modeling, data security testing, model robustness, system and pipeline testing, red-teaming, continuous monitoring, and assurance reporting. The framework is designed to help customers secure AI across data, models, pipelines, and operations, with support for AI inventory, use case criticality, privacy leakage testing, poisoning detection, adversarial testing, runtime monitoring, and reporting for chief information security officers (CISOs), regulators, and auditors.

Figure 3. Cognizant's AI for Security Model Shows a Progression From Assisted AI for Faster Triage to Augmented AI for Orchestration and Autonomous AI for Predictive Security



Source: Cognizant

© 2026 Constellation Research Inc. All rights reserved.

Cognizant is also extending its cyber defense model to frontier AI risk and remediation. Its blueprint brings together Neuro Cybersecurity, Cyber Defense Centers, remediation teams, partner platforms, and governance frameworks to help customers identify, prioritize, test, and remediate AI-related risk. The model includes AI runtime security, shadow AI detection, AI red-teaming, AI-assisted penetration testing, AI governance, AI inventory and lineage, agentic guardrails, continuous compliance, patchless automation, autonomous patch management, and configuration compliance.

Taken together, Cognizant's offering is less about a single managed SOC service and more about a security modernization model. The company combines consulting, implementation, managed operations, partner integration, Cyber Defense Centers, Neuro Cybersecurity, and AI-infused workflows to help customers improve cyber resilience across the enterprise

Notable Wins

Cognizant highlights several customer examples across zero trust, postquantum readiness, network security, cloud security, and SOC modernization:

- A large multinational enterprise worked with Cognizant to modernize branch security through a zero-trust architecture. The engagement focused on reducing reliance on legacy virtual private network (VPN), proxy, Domain Name System (DNS), and network access control tools while improving security, simplifying operations, and supporting a more scalable global access model.
- A regulated wealth and investment firm worked with Cognizant on postquantum readiness. Cognizant helped establish postquantum cryptography (PQC) governance, create a cryptography center of excellence, discover cryptographic assets across hybrid environments, build a cryptographic bill of materials (CBOM), map crypto dependencies to application owners, and define a phased transition roadmap.
- A global fast food enterprise worked with Cognizant on cyber and network security transformation across a distributed operating environment. The engagement focused on firewall policy tuning, log architecture modernization, centralized management, market-specific policy design, SOC validation, and proactive detection of high-risk traffic.
- A global life sciences organization worked with Cognizant to improve cloud security across Amazon Web Services (AWS) and Azure. Cognizant helped deploy cloud security posture management, workload protection, asset discovery, vulnerability scanning, runtime protection, identity risk controls, and compliance-aligned cloud policies.
- A global biopharmaceutical company worked with Cognizant to modernize security operations via a next-generation SIEM and security operations platform. Cognizant helped onboard applications, tune detection rules, build dashboards, integrate with IT service management and access systems, and automate response workflows.

OFFERING ANALYSIS

Cognizant's Cybersecurity Services offering aligns with the direction of the cybersecurity services market. Buyers are moving beyond point services and managed alert monitoring toward partners that can help them modernize security operations, reduce fragmentation, improve resilience, and connect cyber risk to business outcomes. Cognizant's approach is strongest when viewed as a services-led modernization model that combines consulting, implementation, managed operations, Cyber Defense Centers, partner platforms, and AI-infused workflows.

The most compelling part of the offering is Cognizant Managed Cybersecurity, powered by Neuro Cybersecurity. It gives Cognizant a clear operating model across threat defense, threat intelligence, workload protection, vulnerability management, and cyber risk management. This structure is important, because

© 2026 Constellation Research Inc. All rights reserved.

customers not only desire to improve SOC performance but also need to connect exposure, workload risk, threat activity, remediation, and executive reporting into one operating rhythm. Cognizant's model is designed to support that broader requirement while enabling customers to build on existing security tools and partner platforms.

Cognizant's seven-tower services model also gives customers multiple entry points. A buyer can begin with SOC modernization, cloud security, zero trust, identity, GRC, vulnerability management, postquantum readiness, incident response, or security for AI. This is useful for large enterprises, because cybersecurity modernization rarely starts from one clean starting point. Most customers have a mix of legacy tools, regulatory pressure, cloud expansion, identity risk, vulnerability backlogs, and new AI security requirements.

The offering is especially relevant for customers that want to move from tool-by-tool security operations to a more integrated cyber resilience program. Cognizant's Cyber Defense Centers provide the delivery backbone, Neuro Cybersecurity provides the orchestration layer, and its partner ecosystem provides coverage across major security platforms. This gives Cognizant a practical role as an integrator and operator for complex environments, rather than as a provider asking customers to standardize on a single proprietary stack.

With dozens of global players in cybersecurity services, customers are challenged in choosing a trusted partner. Here are the strengths and weaknesses of Cognizant's offering:

Strengths

- **Broad portfolio provides a clear managed services model:** Cognizant covers governance, risk, and compliance; data security and privacy; identity and access management; cloud, infrastructure, and network security; threat and vulnerability management; incident management and response; and security for AI. Its managed cybersecurity model is organized around Cyber Threat Defense, Cyber Threat Intelligence, Cyber Workload Protection, Cyber Vulnerability Management, and Cyber Risk Management. This gives buyers a broad services partner with a modular structure that is easy to understand, phase, and expand.

- **Neuro Cybersecurity and Cyber Defense Centers provide the delivery backbone:** Cognizant positions Neuro Cybersecurity as the AI orchestration layer across managed cybersecurity services. This helps connect threat detection, intelligence, exposure, workload protection, and risk reporting in a more unified operating model. Cognizant supports this model via Cyber Defense Centers in Bengaluru, Chennai, and Denver, giving customers a delivery base for scale, coverage, and consistent operating processes across regions.

- **Customers gain a practical path from AI-assisted work to agentic workflows:** Cognizant's assisted, augmented, and autonomous AI model gives customers a staged adoption path. Buyers can start with alert enrichment, incident summarization, and vulnerability/threat correlation before expanding into threat hunting, playbook automation, predictive attack path modeling, and posture optimization. Cognizant also extends agentic workflows across security operations, vulnerability management, infrastructure security, identity, and GRC, which reflects how security work actually spans remediation, posture, access, policy, evidence, and reporting.

- **Security for AI is treated as a lifecycle problem:** Cognizant's Security for AI testing framework covers governance, threat modeling, data security, model robustness, pipeline security, red-teaming, continuous monitoring, and assurance reporting. This helps customers think beyond prompt-level controls and address AI security across data, models, applications, pipelines, and operations.

- **Postquantum readiness creates a differentiated entry point:** Cognizant's work on crypto discovery, CBOM, governance, certificate lifecycle management, and PQC roadmaps gives regulated customers a practical way to begin postquantum planning before migration becomes urgent.

© 2026 Constellation Research Inc. All rights reserved.

- **Partner-led integration protects existing investments:** Cognizant works across major security platform ecosystems and can help customers operationalize partner technologies. This is important, because most large enterprises already have investments in SIEM, extended detection and response (XDR), cloud-native application protection platforms (CNAPPs), secure access service edge (SASE), identity, vulnerability management, IT service management, and cloud platforms.

Opportunities for Improvement

- **Clarify maturity, availability, and buyer journeys:** Cognizant presents a broad vision across managed cybersecurity, agentic SOC, autonomous remediation, frontier AI risk, and security for AI. Buyers will need a clearer view of which capabilities are production-ready, which are partner-dependent, which are delivered as custom engagements, and which are still emerging. Cognizant should also package these capabilities into repeatable buyer journeys across SOC modernization, zero trust, cloud security, PQC, AI security, and vulnerability management, with defined prerequisites, timelines, metrics, deliverables, and expected outcomes.

- **Define autonomy levels with buyer-ready controls:** Cognizant should make the control model more explicit. Buyers need to know which actions are AI-assisted, which require human approval, and which can be executed automatically. This is especially important for identity changes, endpoint containment, firewall policy updates, cloud configuration changes, and remediation actions. Cognizant should also show how approval flows, policy gates, exception handling, decision logs, evidence capture, rollback, and reporting work inside agentic workflows.

- **Normalize outcome metrics:** Cognizant should make outcome evidence easier for buyers to compare across use cases and service modules. Customer-facing material should distinguish between realized customer outcomes, representative targets, internal benchmarks, and generally expected benefits. This will help buyers understand the likely business case for SOC modernization, vulnerability prioritization, remediation, cloud security, AI security, and managed cyber defense.

- **Clarify services-led differentiation:** The partner ecosystem is a strength, but buyers also need to understand the provider's own operating model, Neuro Cybersecurity, delivery methodology, Cyber Defense Center processes, governance model, accelerators, and security engineering depth. This will help buyers see what Cognizant uniquely brings above partner platform implementation and operations.

- **Connect security for AI to enterprise AI programs:** Cognizant's AI security framework is strong, but buyers will need practical guidance on how it connects to AI governance, model inventory, data governance, software engineering, procurement processes, legal and compliance teams, and business-led AI adoption initiatives. This will be important as AI security becomes a cross-functional program, not just a CISO-owned control.

BUYING CONSIDERATIONS

Customers and prospects evaluating Cognizant should use the following considerations to identify the right entry point, assess fit, and plan implementation:

- **Start with managed cybersecurity modernization:** Cognizant Managed Cybersecurity provides a practical entry point for buyers that need to improve SOC operations, threat intelligence, workload protection, vulnerability management, and risk reporting without rebuilding the entire security program. Neuro Cybersecurity can help connect detection, intelligence, exposure, workload protection, and risk visibility across current tools and data sources.

© 2026 Constellation Research Inc. All rights reserved.

- **Modernize without a full rip-and-replace:** Cognizant's model is partner-led and integration-focused. This is relevant for enterprises with existing investments in SIEM, XDR, cloud security, identity, vulnerability management, IT service management, and cloud platforms. Buyers should evaluate how Cognizant integrates with their current stack and where its managed services model improves operations.

- **Evaluate security for AI and PQC readiness:** Enterprises deploying copilots, agents, AI-enabled applications, and model APIs should evaluate Cognizant's AI security testing framework, including governance, threat modeling, model robustness testing, red-teaming, runtime monitoring, and assurance reporting. Regulated organizations should also consider Cognizant's approach to crypto discovery, CBOM development, crypto governance, certificate lifecycle improvement, and phased PQC roadmaps.

- **Ask for clear maturity and autonomy mapping:** Buyers should ask Cognizant to distinguish between assisted AI, augmented AI, autonomous AI, production capabilities, partner-dependent capabilities, and custom engagements. They should also ask where human approval is required, how decisions are logged, how exceptions are handled, and how rollback works.

- **Validate proof points by domain:** Cognizant has examples across zero trust, PQC, network security, cloud security, and SIEM modernization. Buyers should ask for anonymized but detailed proof points relevant to their own industry, technology stack, regulatory environment, and operating model.

- **Test the operating model, not just the platform fit:** Cognizant's value depends on integration, delivery discipline, governance, talent, and operational maturity. Buyers should evaluate onboarding, run-book redesign, metrics, escalation paths, reporting, and continuous improvement processes before scaling managed services.

© 2026 Constellation Research Inc. All rights reserved.

RECOMMENDATIONS

Constellation offers the following recommendations for CxOs seeking cybersecurity services that help their organization modernize security operations, improve resilience, and move from human-orchestrated workflows toward governed, AI-assisted, and autonomous security operating models:

- **Define the autonomy roadmap around business pain:** Establish where autonomy can create the most value first, such as SOC overload, identity sprawl, exposure prioritization, cloud drift, data exposure, or compliance evidence. Use these priorities to sequence the roadmap rather than starting with technology selection.
- **Treat autonomous security as an operating model:** Assign owners for policy, oversight, architecture, digital worker operations, validation, and exception management. Autonomy requires changes across people, process, technology, governance, and measurement.
- **Start with bounded, measurable workflows:** Choose use cases with clear inputs, repeatable actions, defined approval paths, and measurable outcomes. Alert triage, enrichment, threat hunting, detection tuning, vulnerability prioritization, and compliance evidence collection are practical starting points.
- **Build the enterprise context layer first:** Autonomous systems need reliable context across assets, identities, vulnerabilities, controls, telemetry, tickets, business services, and risk. Poor context will limit decision quality and increase manual review.
- **Separate recommendations from autonomous actions:** Define which tasks agents can summarize, recommend, execute with approval, or execute autonomously. High-impact actions, such as disabling access, changing cloud configurations, isolating endpoints, or modifying production controls, require explicit guardrails and rollback paths.
- **Measure, validate, and avoid lock-in:** Track outcomes such as mean time to detect, mean time to investigate, mean time to respond, false positive reduction, exposure reduction, and audit readiness. Use red-teaming, purple-teaming, control validation, and independent review to confirm that autonomous workflows behave within policy. Prioritize open integration, exportable data, flexible model choices, and interoperability with existing systems.

© 2026 Constellation Research Inc. All rights reserved.

ENDNOTES

[1] Chirag Mehta, "Claude Mythos and the New Cybersecurity Operating Model," Constellation Research, May 27, 2026. *https://www.constellationr.com/research/claude-mythos-and-new-cybersecurity-operating-model*

[2] Constellation Research, The Business Transformation 150™, 2024. *constellationr.com/business-transformation-150*

[3] Constellation Research, Ambient Experience 100 2024, 2024. *constellationr.com/work-constellation/ax-leaders/ax100-2024*

© 2026 Constellation Research Inc. All rights reserved.

ANALYST BIO

Chirag Mehta

Vice President and Principal Analyst

Chirag Mehta is a vice president and principal analyst focusing on cybersecurity, next-gen application development, and product-led growth.

With more than 25 years of experience, he has built, shipped, marketed, and sold successful enterprise SaaS products and solutions across startups as well as midsize and large companies. As a product leader overseeing engineering, product management, and design, he has consistently driven revenue growth and product innovation. He has also held key leadership roles in product marketing, corporate strategy, ecosystem partnerships, and business development, leveraging his expertise to make a significant impact on various aspects of product success.

His holistic research approach to cybersecurity is grounded in the reality that as sophisticated AI-led attacks become increasingly prevalent and as organizations aspire to empower their workforce—to work from anywhere with access to all their data and applications on their preferred devices—CISOs and CIOs are facing challenges to reimagine a cybersecurity landscape in the hybrid computing world. His aim is to help technology leaders navigate the complex cybersecurity landscape and mitigate risks while empowering business leaders to get work done.

Through his extensive hands-on experience as a technology practitioner—in designing, building, and running SaaS applications used by billions of users—his research on next-gen application development platforms focuses on challenges organizations face in delivering highly performant, innovative products at a rapid pace and scale. He helps chief product officers and chief technology officers strike a delicate balance where they can continue to solve critical problems and delight their customers while effectively managing technology debt.

@Chirag_Mehta *constellationr.com/users/chirag-mehta* *linkedin.com/in/mehtachirag*

© 2026 Constellation Research Inc. All rights reserved.

ABOUT CONSTELLATION RESEARCH

Constellation Research is an award-winning, Silicon Valley–based research and advisory firm that helps organizations navigate the challenges of digital disruption through business model transformation and the judicious application of disruptive technologies. Unlike the legacy analyst firms, Constellation Research is disrupting how research is accessed, what topics are covered, and how clients can partner with a research firm to achieve success. Over 350 clients have joined from an ecosystem of buyers, partners, solution providers, C-suites, boards of directors, and vendor clients. Our mission is to identify, validate, and share insights with our clients.

Organizational Highlights

- Institute of Industry Analyst Relations (IIAR) New Analyst Firm of the Year in 2011 and #1 Independent Analyst Firm for 2014 and 2015
- Experienced research team with an average of 25 years of practitioner, management, and industry experience
- Organizers of the Constellation Connected Enterprise—an innovation summit and best practices knowledge-sharing retreat for business leaders
- Founders of Constellation Executive Network, a membership organization for digital leaders seeking to learn from market leaders and fast followers

www.ConstellationR.com | @ConstellationR

info@ConstellationR.com | sales@ConstellationR.com

Unauthorized reproduction or distribution in whole or in part in any form, including photocopying, faxing, image scanning, emailing, digitization, or making available for electronic downloading is prohibited without written permission from Constellation Research Inc. Prior to photocopying, scanning, and digitizing items for internal or personal use, please contact Constellation Research Inc. All trade names, trademarks, or registered trademarks are trade names, trademarks, or registered trademarks of their respective owners.

Information contained in this publication has been compiled from sources believed to be reliable, but the accuracy of this information is not guaranteed. Constellation Research Inc. disclaims all warranties and conditions with regard to the content, express or implied, including warranties of merchantability and fitness for a particular purpose, and it does not assume any legal liability for the accuracy, completeness, or usefulness of any information contained herein. Any reference to a commercial product, process, or service does not imply or constitute an endorsement of the same by Constellation Research Inc.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold or distributed with the understanding that Constellation Research Inc. is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought. Constellation Research Inc. assumes no liability for how this information is used or applied, and it does not make any express warranties on outcomes. (Modified from the Declaration of Principles jointly adopted by the American Bar Association and a committee of publishers and associations.)

Your trust is important to us, and as such, we believe in being open and transparent about our financial relationships. With our clients' permission, we publish their names on our website.

San Francisco Bay Area | Boston | Colorado Springs | Denver | Ft. Lauderdale | New York Metro
Northern Virginia | Los Angeles | Portland | Pune | San Diego | Sydney | Washington, D.C.

© 2026 Constellation Research Inc. All rights reserved.