OMDIA UNIVERSE

Publication date:
18 Sep 2025

Author(s):
Hollie Hennessy, OT/IoT Cybersecurity Lead
Adam Etherington, Practice Leader, Cybersecurity
Jonathan Ong, Senior Analyst, Cybersecurity

Omdia Universe: Operational Technology Cybersecurity Services, 2025–26

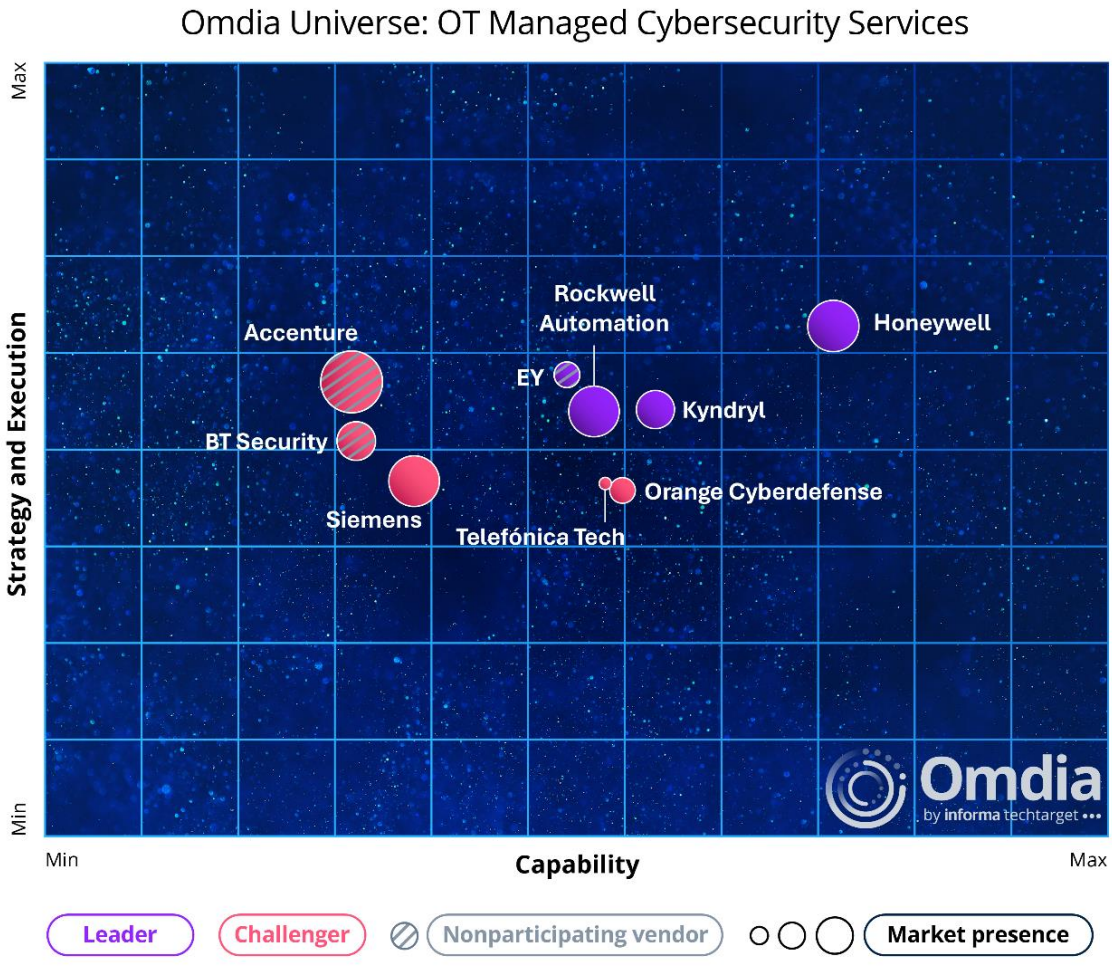
Omdia
by informa techtarget

Summary

Catalyst

Modern operational technology (OT) has evolved to connect with IT systems and the broader internet, driven by productivity demands ushered in by the age of the Fourth Industrial Revolution (Industry 4.0). However, this newfound connectivity introduces security concerns that were once limited to the domain of IT into unprepared OT environments. Amplified by tightening regulations, threat actors breaching security and privacy perimeters, and niche OT security talent requirements, OT organizations are turning to service providers that have the specialized technology and talent to bridge the IT-OT gap and continue enabling business in a secure manner.

Figure 1: The Omdia Universe for OT managed cybersecurity



Source: Omdia

All providers included in the report were approached to provide input to this study. Accenture, BT, and EY either declined to participate or did not complete the full response questionnaire in time before publication. The non-participant provider evaluations are based on publicly available information,

analyst insights and feedback from their customer base sourced directly via Informa TechTarget audiences.

Omdia view

The integration of OT environments with IT systems and the internet marks a significant milestone in Industry 4.0. While this interconnectivity drives efficiency and productivity gains, it simultaneously creates substantial security vulnerabilities. Legacy systems, immature security practices, and systems historically developed in isolation and to different timescales have left the OT environments of many organizations exposed to emerging threats.

As OT systems become increasingly interconnected with IT networks, the attack surface expands dramatically, necessitating comprehensive risk assessment and mitigation strategies. The financial implications of these security gaps can be severe, potentially leading to operational disruptions with far-reaching material and physical consequences. This has led to manufacturing and critical infrastructure organizations becoming prime targets for sophisticated cyberattacks in recent years.

OT security concerns are distinct from those found in traditional IT, often involving unique protocols, older systems, and specific operational requirements. Over the past 15 years, security vendors have responded by developing specialized technologies to protect these environments, resulting in modular platforms designed to address various OT security issues.

There are fundamental cultural challenges and reasonable differences between IT and OT teams, and OT cybersecurity services are instrumental in closing the long-standing challenges between the two areas, addressing not only technical vulnerabilities but also organizational and operational challenges. As industrial systems become more interconnected, these services enable organizations to build unified security strategies that span both domains, fostering collaboration between IT and OT teams and ensuring that critical risks are identified and mitigated in real time.

By providing specialized expertise, advanced proactive and integrated threat detection, and tailored incident response capabilities, OT cybersecurity services help organizations monitor network traffic, analyze anomalies, and respond proactively to threats that could jeopardize the three priorities of an OT organization—safety, reliability, and availability.

This integrated approach is crucial for protecting critical infrastructure, as it brings together the best practices from both IT and OT, aligns security protocols, reduces risk, improves operational uptime, and ensures transparent communication and shared responsibility across teams. Ultimately, OT cybersecurity services not only safeguard industrial assets but also empower organizations to adapt to evolving cyber threats while maintaining operational resilience and business continuity.

Analyzing the OT cybersecurity services universe

Market definition

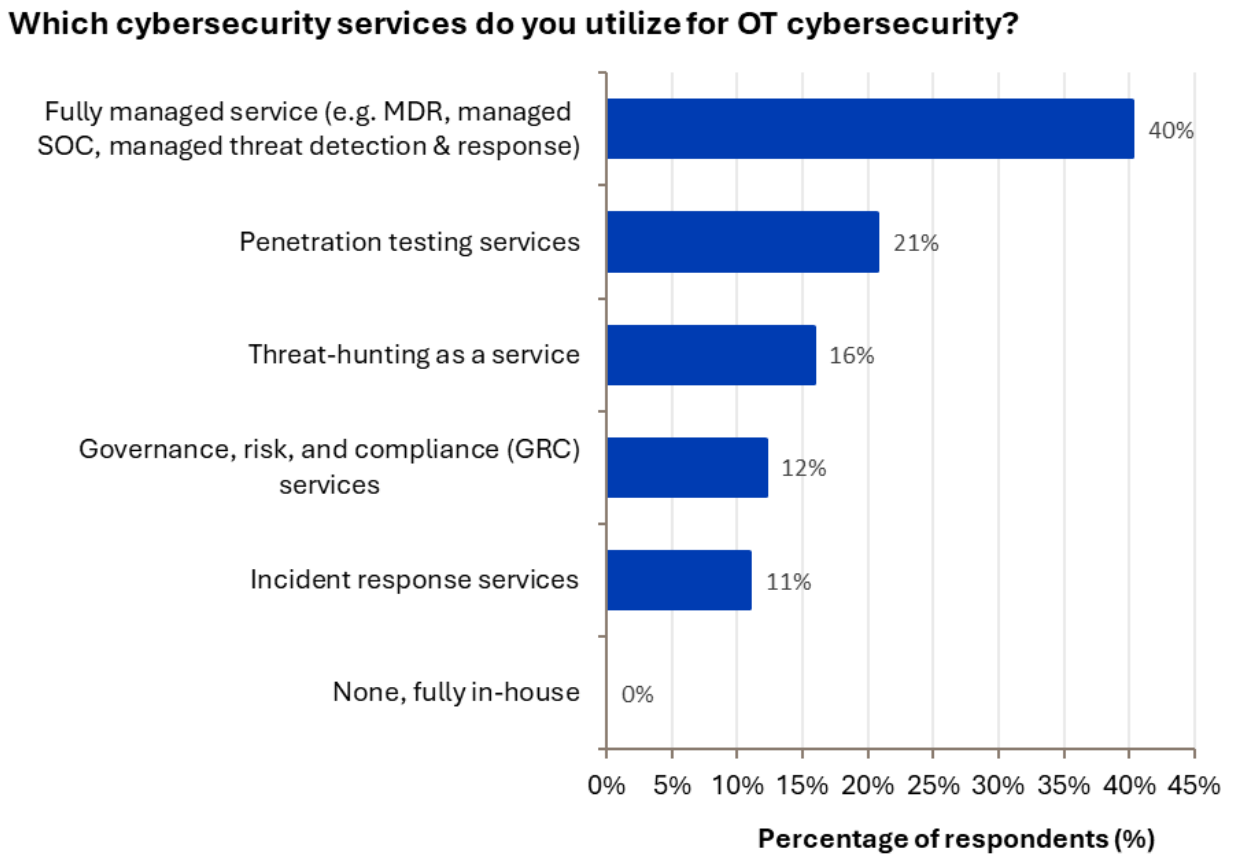
OT specialized cybersecurity services span a number of areas, falling broadly into managed security services, which include managed detection and response (MDR) and threat hunting, alongside additional and supporting services including penetration testing; governance, risk, and compliance; incident response; and maturity assessments. This report focuses on OT MDR; however, given the

importance of supporting services to OT cybersecurity practitioners and buyers, Omdia has considered a number of these capabilities alongside MDR in our research.

The OT cybersecurity services market is not as mature as the IT cybersecurity market and is served predominantly from a mixture of industrial automation vendors, communication service providers, consulting firms, and IT system integrators. Thus, there is a mix of backgrounds and approaches, with some focusing more on the compliance and regulatory angle and others more on IT/OT security integration.

Organizations are utilizing at least some form of service for their OT cybersecurity needs. In Omdia's annual Cybersecurity Decision Maker Survey (2025) of 980 OT cybersecurity decision makers, 100% of respondents surveyed use some form of cybersecurity service, of which fully managed services (e.g., MDR, managed security operations center [SOC]) were the most common at 40% of respondents (**Figure 2**).

Figure 2: Utilization of cybersecurity services for OT



Notes: n=82

Source: Omdia

That said, dedicated OT MDR offerings are somewhat less mature. The inclusion criteria for this report are limited to providers with multi-region support, and some are more mature than others, with global, well-developed SOC offerings and a relatively large number of people supporting OT in particular. Others have recently developed or are entering the managed OT cybersecurity space with clear roadmaps and strategies to excel in this market but may have less dedicated OT staff, relying on wider IT security expertise.

Omdia has identified key components of OT cybersecurity services, organized into specific groups with defined capabilities, as follows.

Service capabilities

- **Threat intelligence:** The provider should utilize a mix of open source, paid, and potentially proprietary threat intelligence feeds that are current and qualified with a focus on OT-centric tactics, techniques, and procedures (TTPs) and indicators of compromise (IOC). This proactive approach should include the integration of OT-specific threat intelligence to improve detection capabilities through industry context and trends. Threat hunting may also be included, either as an integral service or an optional add-on.
- **Incident response:** A comprehensive incident response plan covering containment and eradication should be included in the event of a breach. Identification, recovery, PR communications, and legal advice may be available at advanced tiers or as add-ons.
- **Third-party risk:** As OT organizations often have a host of third-party technologies and hardware, the service provider should be able to vet and determine their risk profile in the context of the customer's environment.
- **Compliance:** The provider should advise customers on their regulatory obligations based on industry and geography and offer roadmaps, recommendations, and measures to ensure continued compliance.
- **SOC breadth and depth:** OT cybersecurity analysts, engineers, and responders should be specialized, certified, and up to date with the current industry threats and trends. They should also be available in local or adjacent time zones. Dedicated OT-specific managed SOC capabilities should be offered with a focus on IT/OT observability, business continuity, and operational safety.
- **Multi-vendor support:** The provider should have significant integrations with multiple vendors across hardware, systems, and software capabilities.

Customer experience and vendor execution

- **Strategy and innovation:** As OT customers vary significantly across maturities and industries, providers should align their offerings and roadmaps with their target market segment's readiness, technologies and regulatory obligations.
- **Market momentum:** The provider should have healthy revenue growth and expanding industry coverage across new industries, as well as increasing presence in established industries.
- **Vendor execution:** As a managed service that goes beyond the technology, providers should deliver a service that works cohesively with a customer's IT and OT team and across third-party vendors.
- **Customer experience:** As part of this report, Omdia surveyed 220 cybersecurity professionals responsible for defining requirements for or purchasing OT security solutions and services. The respondents only evaluated providers that they have worked with. Omdia's scoring considers how likely the customer is to recommend the provider, as well as how they rate the provider's service quality.

Market dynamics

This debut Omdia Universe analyzes providers delivering crucial managed OT cybersecurity services and serving to facilitate collaboration between the IT and OT teams in a customer's environment. This market is fueled by digital transformation initiatives within industrial environments, alongside regulatory requirements emerging to ensure cybersecurity resilience within critical national infrastructure. Paired with this, industrial organizations are sorely lacking in internal expertise, with only 36% of respondents to Omdia's OT Cybersecurity Services study considering themselves *Very prepared* in having access to internal skilled OT security staff. This has resulted in many turning to providers to aid them in security design, deployment, and management.

That said, OT security has long been underfunded within overall IT security budgets. Although there is strong demand for OT cybersecurity services, increasing security funding and building a business case is the area respondents to our survey were least prepared for. Additionally, cost is the second most common reason for organizations to consider a service provider relationship. However, the picture is not all bad: the largest portion of respondents (61%) ranked themselves as "somewhat prepared" in this area, suggesting that the situation is improving. Nevertheless, this creates an environment where organizations look for competitive pricing and clear business benefits from their providers.

Additionally, a number of customer pain points stood out when undertaking this research. Omdia has considered these when benchmarking the providers profiled in this report.

- **IT/OT converged security:** Organizations on the whole are far less prepared when it comes to securing converged environments, with less than half of organizations considering themselves *Very prepared* for all areas. There is a particular lack of readiness when it comes to navigating cultural issues, deploying zero-trust principles, and addressing interoperability and complexity.
- **Proactive security:** Downtime in an OT environment carries a markedly higher cost, so adopting a proactive approach through third-party risk management, threat intelligence and hunting, and zero-trust strategies is necessary to identify and mitigate potential threat vectors.
- **Incident analysis and response:** The largest pain point by far for OT cybersecurity teams is noise: managing the growing volume of attacks, alert fatigue, and floods. OT organizations require a provider that can filter, categorize, investigate, contain, remediate, and restore operations under time pressure and in a safe manner.
- **Broad yet specialized services:** Organizations require specialization and industry expertise—the second-most important factor when selecting an OT security services provider. They desire a dedicated OT services team that offers a range of capabilities across consulting and management, can advise customers on applicable regulatory obligations, and bridges IT-OT communications and competing priorities between CISOs and floor managers.

Figure 3: Provider rankings in the OT cybersecurity services universe

Provider	Service(s) evaluated
Leaders	
EY (Ernst & Young Global Services)	OT Cybersecurity Services
Honeywell	OT Managed Security Services
Kyndryl	OT Security Service
Rockwell Automation	Security Monitoring and Response
Challengers	
Accenture	OT Cybersecurity Services
BT	IT/OT Cybersecurity Operations
Orange Cyberdefense	Managed Industrial Security
Siemens	Remote Industrial Operations Services
Telefónica Tech	Mission Critical SOC

Source: Omdia

Market Leaders

Leaders excel in multiple areas that we have assessed in this research report, with a number of Top-tier ratings and some being Best-in-class for multiple criteria. These providers have all scored toward the higher end with their combined scores, with impressive strategy and innovation. Omdia believes that providers in this category are worthy of a place on most technology and services selection shortlists.

Market Challengers

Solutions offered by providers in the Challenger category provide a good set of capabilities across technology and services. Although providers with this ranking do not commonly offer the more advanced capability set or have the same market momentum and strategy and innovation as those marked as Leaders, Omdia recommends that they should still be considered as part of the technology and services selection process, especially by midsize organizations.

Market outlook

In the short term, we will see fast development from providers, given how nascent a number of the managed OT security offerings in this report are, specifically in the OT technology or platforms capabilities. Omdia expects that providers will expand partnerships, integration, and platform development to aid customers in building and utilizing their OT security stack. Omdia will be keeping a close eye on this category and publishing a 2025 market sizing of the OT and IoT cybersecurity services market.

The market is full of opportunities. Increasing engagements with third-party providers for OT security is among the top three actions that are paramount to reducing cybersecurity risk in the next 12–18 months, according to Omdia's OT Cybersecurity Services study, conducted alongside this Omdia Universe report. That said, to capitalize on this opportunity and provide clarity, providers must enhance and streamline their OT specific messaging, approach, and pricing structures to effectively position and differentiate.

Looking toward future capabilities, inspiration can be drawn from the evolution of IT MDR. Omdia expects incident response will—and must—expand beyond detection and basic response capabilities as organizations look to service providers for more proactive and comprehensive support. Based on Omdia's findings in this report, a number of providers are limited to supporting with specific OT incident response, limiting themselves to Level 1 or 2 SOC support and leveraging IT, rather than OT talent, for Level 3 and above. However, customers will eventually expect OT-specific responses, which may take the form of containment actions such as microsegmentation, process control, and incident response playbooks that prioritize OT objectives such as safety and uptime. These OT-specific responses are vital for providers offering specialized support for critical information industries (CII).

This follows a similar trajectory of incident response in IT. Initial IT MDR offerings struggled to gain traction as customers were primarily concerned about response capabilities. This has resulted in modern MDR, whereby a robust response function is table stakes for a provider, whether as in-house capabilities or through channel partners. For those who do not plan to have this capability, we will likely see more partnerships develop to round out the "R" in MDR offerings.

Additionally, there are a number of emerging technologies such as artificial intelligence (AI), secure remote access, modern microsegmentation, and autonomous response, that are increasingly utilized and offered from a technology perspective. Compared to other areas, such as security leadership and visibility, for example, organizations are much less prepared when it comes to leveraging these emerging technologies. Only 47% stated they were *Very prepared* in this category, with 1 in 10 *Not prepared at all*. Service providers should look to integrate these into their SOC and service offerings to fill this gap.

AI technology is one of the hottest topics in the IT and OT security software space, and this will extend into the services realm. From a technology perspective, this includes enhancing the SOC capabilities that the provider can offer. Alongside using AI for cybersecurity, industrial organizations must also consider the security of AI deployed in their environments. In the longer term, AI will transform industrial organizations in a similar way to how it is already transforming enterprises, and there is an opportunity for providers to deliver services across IT/OT convergence and AI deployment.

Provider analysis

Provider accolades

Within the provider analysis section, there are two types of accolades that can be awarded to providers:

The **Best in class** accolade is awarded to the provider(s) with the highest score (highest outright, tied highest, or within <1% of the highest score) for each of the scoring categories that make up this Universe topic:

- OT platforms
- OT MSS
- Solution breadth
- Strategy and innovation
- Market momentum

- Vendor execution

The **Top-tier** accolade is given to providers falling within the upper tercile (top third) of the scores within the comparison group, for each of these same scoring categories.

Honeywell (Omdia recommendation: Leader)

Honeywell should appear on your shortlist if:

- You are looking for an established organization with a deep history in OT and an integrated approach to cybersecurity.

Overview

Honeywell, founded in 1906, is one of the world's largest automation and control system providers. Built from its expertise in industrial automation and building control systems, Honeywell has a comprehensive portfolio of OT cybersecurity solutions and services that consists of the following:

- **Cyber Insights:** Asset discovery, network monitoring, and intrusion detection
- **Cyber Proactive Defense:** An AI-powered OT solution designed to deliver continuous monitoring, advanced threat hunting, and analysis
- **Cyber Watch:** Enterprise-wide (multi-site) visibility and continuous monitoring of compliance status
- **Secure Media Exchange:** Enforceable USB and removable media protection
- **Managed Security Services:** Patch and AV management, secure remote access, and an OT-specific SOC
- **Professional Security Services:** Offers more than 30 services, including site assessments, penetration testing, network design, remediation, employee training, third-party integration, and more

Honeywell's technology and services are vendor-agnostic and can support customers with multiple control system environments. For example, the Honeywell OT SOC is a vendor-agnostic, OT-specific security operations center solution that can integrate with an IT SOC and provide incident response services, incident response recovery management, tabletop exercises, in-depth incident investigation, and orchestrated response. It also offers an onsite incident response retainer.

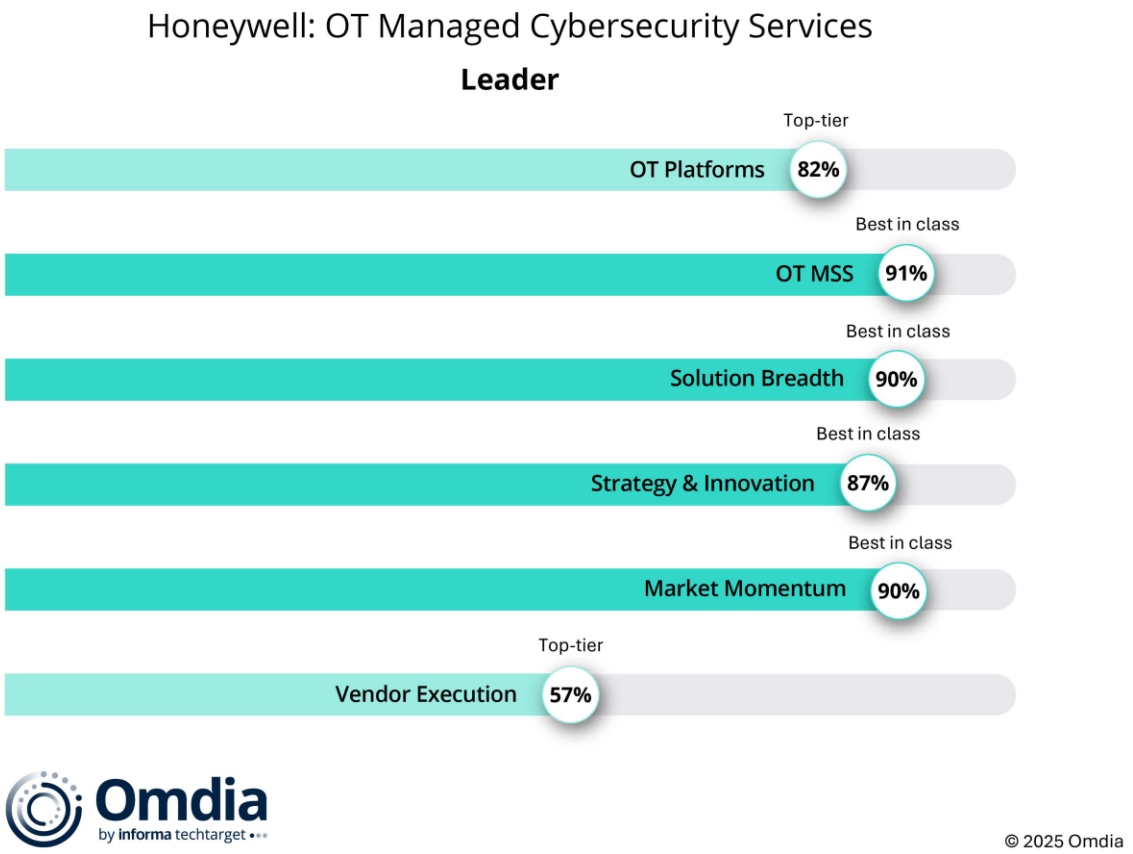
Honeywell's OT Managed Security Services focus on cybersecurity and operational resilience, addressing both the IT and OT domains. The provider does this by focusing on the key outcomes of business continuity, risk reduction, compliance, operational safety, workforce development, and resiliency within OT environments.

Honeywell also demonstrates a focus on governance and compliance with Cyber Watch. Recently, it launched a suite of AI-powered offerings across its Cyber Proactive Defense, OT SOC, and Digital Prime Ecosystem.

As of 2025, Honeywell has expanded into being both an OT organization and a cybersecurity vendor, with hundreds of its 102,000 employees focused on cybersecurity. These employees have a direct presence in 40 countries and have delivered thousands of projects across 130 countries. Its primary industries include aerospace technologies, building automation, energy and sustainability, and industrial automation.

In addition to its latest managed security service center in Saudi Arabia, which opened in 2025, Honeywell plans to launch another OT SOC to bolster services with a new Cyber Proactive Defense software on the technology side.

Figure 7: Omdia Universe ratings—Honeywell



Source: Omdia

Strengths

- Overall, Honeywell's customers are very satisfied with the quality of the service received and are generally comfortable recommending the provider.
- Based on Omdia's customer survey, Honeywell's customers engage the provider for its breadth and depth of security services, OT security expertise, and flexible and favorable delivery model.
- The results align with Honeywell's project portfolio of thousands of projects delivered and significant global presence in more than 40 countries.
- Honeywell is a system integrator with the ability to deliver vendor-agnostic OT cyber solutions for both Honeywell and third-party solutions to help meet customer needs.
- Honeywell is also increasing its focus on governance and compliance, as demonstrated by its acquisition of SCADAfence in 2023 and the release of offerings that support governance, risk, and compliance tracking.

- The provider also has robust and modular prevention and hardening capabilities that include network segmentation and micro segmentation at the individual device and application levels by device type, user role, and/or application requirement.
- Adaptive segmentation can be automated based on near-real-time assessments of device and network behaviors. Given Honeywell's deep expertise in OT and industrial automation, this can be done while ensuring operational availability and reliability.
- Honeywell's incident response capabilities focus on supporting personnel safety and minimizing operational disruption, demonstrating its understanding of the competing priorities of OT environments.
- Additionally, Honeywell tailors investigation techniques to the specific customer system and network configurations and utilizes predefined, OT-specific incident response playbooks.

Limitations

- Honeywell would benefit from increasing the range of OT-specific software that it integrates and supports, as customers cited a lack of software support as one of the top three reasons for provider reconsideration. Expanding beyond its current range of partners to other OT vendors would enable its customers to enjoy best-of-breed technologies with Honeywell's integrative experience.
- Customers also mentioned a focus on compliance when selecting a new provider, and Honeywell has a strong opportunity to get ahead of this with its acquisition of and integration with SCADAfence.
- Similar to other providers included in this assessment, Honeywell may want to revisit its pricing structure to ensure competitiveness. Based on Omdia's customer study, customers cited cost as one of the factors for reconsidering the provider relationship.

Appendix

Methodology

Omdia Universe

Omdia's rigorous methodology for the Universe product involves the following steps:

- Omdia analysts perform an in-depth review of the market using Omdia's market forecasting data and Omdia's enterprise insights survey data.
- Omdia creates a matrix of capabilities, attributes, and features that it considers to be important now and in the next 12–18 months for the market.
- Providers are interviewed, and in-depth briefings are provided on current solutions and future plans.
- Analysts supplement these briefings with other information obtained from industry events and user conferences.

- The Universe is peer-reviewed by other Omdia analysts before being proofread by a team of dedicated editors.
- The service is subject to ranking and feedback by a survey of current customers, rigorously vetted, conducted, and validated independently by Omdia.

Inclusion criteria

Omdia has closely tracked the OT cybersecurity services segment from multiple angles. Inclusion criteria were determined by Omdia's research and customer requirements with a focus on OT specialization:

- OT-specific technologies and services
- Global presence with multiple SOCs
- Coverage of multiple industries
- Significant OT-specific security revenue

Further reading

2025 Trends to Watch: IoT Cybersecurity (September 2024)

Omdia Market Radar: OT Cybersecurity Platforms, 2025 (January 2025)

Author

Hollie Hennessy, OT & IoT Cybersecurity Lead

Jonathan Ong, Senior Analyst, Managed Security Services

Adam Etherington, Practice Lead, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com