GIGAOM

GIGAOM
CxO BRIEF

COMMISSIONED BY:
DEEPWATCH

Managed Detection and Response

SECURITY & RISK


GIGA
OM

GigaOm CxO Decision Brief: Managed Detection and Response

Solution Overview

Managed detection and response (MDR) addresses the operational, staffing, and technology challenges of running an in-house SOC. It delivers 24/7 threat monitoring, faster detection, and expert-led response without the overhead of sustaining large internal teams. MDR improves alert quality, accelerates incident handling, and strengthens resilience through repeatable processes and exposure-aware defense.

Deepwatch advances MDR with its "Precision MDR powered by AI and humans," blending exposure-based detection, customized playbooks, and collaborative response. Its model is designed to integrate seamlessly with existing tools, align to risk models and the MITRE ATT&CK framework, and deliver measurable gains in detection speed and accuracy, with around-the-clock protection from security experts who act on real-time threats, powered by AI.

Benefits

- Continuous 24/7 coverage with consistent expertise
- Proactive, preemptive, and responsive protection, tuned to the customer's environment and business priorities
- Lower operational costs than a fully staffed internal SOC
- Faster access to specialized skills without long hiring cycles
- Quicker adaptation to threats and business changes
- Significant boost in alert fidelity and reduction in noise

Deepwatch-specific:

- Up to **5×** SOC efficiency gains
- Sub-one-minute prevention, <30-minute initial response
- Up to **98%** fewer alerts
- Executive-level reports providing clarity into critical gaps and essential controls

Urgency

For most organizations, building or sustaining a full internal SOC is no longer the optimal path. MDR can be operational in weeks, replacing fragmented coverage with continuous detection and response. In 2025, even well-resourced enterprises are struggling to keep pace without facing analyst burnout, rising costs, and slower response. The decision isn't whether to leverage MDR—it's how quickly you can transition.

Impact

MDR reshapes security operations:

- **Frees up security staff** for proactive initiatives instead of round-the-clock alert triage
- **Improves detection and response times**, reducing breach impact
- **Delivers business-aligned metrics** for board and executive visibility
- **Deepwatch-specific:** Adds continuous exposure risk scoring, tailored playbooks, and integration with your current tooling to accelerate resilience gains

Risk

Delaying MDR adoption introduces measurable risk:

- **Operational** – Prolonged detection delays and uneven coverage
- **Talent** – Higher turnover, slower onboarding, morale decline
- **Strategic** – Missed opportunities to optimize tools and reduce risk
- **Reputational** – Increased exposure if a breach occurs under current SOC constraints
- **Impact** – Loss of customer trust, revenue and regulatory impacts

01 Solution Value

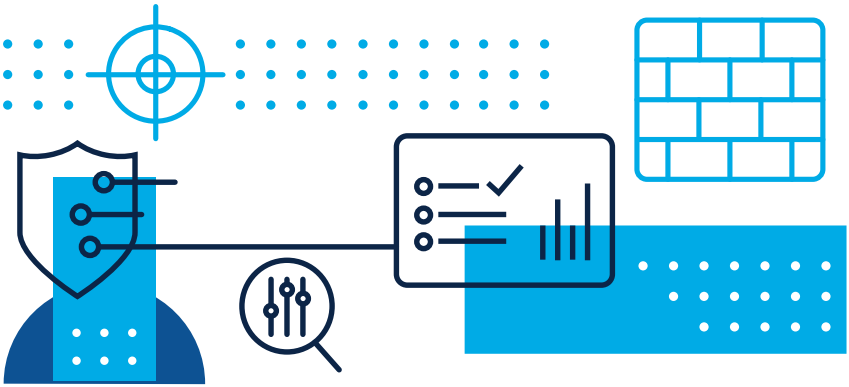
This GigaOm CxO Decision Brief was commissioned by Deepwatch

The Reality of SOC Operations in 2025

For most enterprises, operating a 24x7 security operations center in-house is a costly diversion from the organization's core mission. Even with the best intentions, in-house SOCs face the same structural challenges: persistent talent churn, gaps in specialized expertise, inability to keep pace with rapidly evolving threats, and unpredictable cost spikes driven by incident response. These aren't operational inconveniences; they are strategic risks.

Managed detection and response (MDR) addresses these challenges by design. Unlike traditional MSSPs that primarily process alerts, MDR providers deliver an integrated software platform combined with security experts. Your organization contributes the business context—the "tribal knowledge"—while the MDR delivers the scale, technical depth, and continuous modernization needed to detect and respond at speed.

This model eliminates the constant recruitment cycle, provides access to threat hunters and incident responders you could not realistically hire yourself, and ensures that your defensive posture evolves in step with the threat landscape, including AI-driven attacks. For all but the largest global enterprises, MDR is the most predictable, resilient, and cost-effective path to maintaining effective security operations.



01 Solution Value

Why MDR Outperforms an In-House SOC for Most Enterprises

- **Predictable costs** – Subscription-based model replaces unpredictable, reaction-driven spending.
- **Access to scarce expertise** – Threat hunters, detection engineers, and incident responders on demand.
- **Faster detection and response** – Integrated platform, automation, and continuous tuning reduce dwell time.
- **No talent retention battle** – Eliminates the constant churn and rehiring cycle that drains resources.
- **Continuous modernization** – Threat intelligence and detection capabilities evolve in real time.
- **Focus on core mission** – Security is handled by specialists so your team can focus on business priorities.
- **Scalable resilience** – SOC capability can expand instantly without months of hiring and onboarding.

Where Deepwatch Delivers Differently

Deepwatch approaches MDR as a precision capability, designed to complement enterprise security teams by addressing the operational and staffing challenges inherent in running an in-house SOC. Its model combines adaptive AI, accurate detection, automation, and human expertise, with a focus on aligning technical operations to business risk and priorities.

Key elements of its approach include:

- **Intelligence-driven, exposure-aware detections** – Alerts are prioritized using real-world threat intelligence, MITRE ATT&CK mappings, and contextual business risk, moving beyond static signature-based detection.
- **Streamlined triage and response** – Investigation and containment processes are designed to reduce dwell time, with SLA-backed response windows that define and enforce expected time to action.

- **Analyst expertise and tradecraft** – Deepwatch detection engineers work directly within the client's workflow, developing familiarity with the environment and its specific security requirements.
- **Business-aligned insights with metrics that matter** – Executive-ready reporting focuses on outcome-based metrics, providing measurable indicators of improvements in detection and response maturity.
- **Reduced operational burden** – By delivering 24x7 coverage as a managed service, Deepwatch minimizes the need for organizations to staff continuous shifts or expand headcount to meet operational requirements.
- **Adaptive coverage without gaps** – New log sources and assets are automatically discovered and integrated into detection logic, enabling rapid expansion of coverage without a tuning period.

Deepwatch positions its service as a means to extend and modernize SOC capabilities without requiring the client to build and maintain the full operational model internally. The emphasis is on measurable outcomes, operational predictability, and continuous alignment between detection priorities and the threat landscape.

"By delivering 24x7 coverage as a managed service, Deepwatch minimizes the need for organizations to staff continuous shifts or expand headcount to meet operational requirements."

02 Urgency and Risk

IN TODAY'S THREAT LANDSCAPE, the operational tempo of cybersecurity is dictated by speed and precision. Adversaries are leveraging automation, AI, and targeted social engineering at a pace that leaves little margin for slow detection or manual response. The decision to modernize security operations is no longer optional; it is a prerequisite for resilience, protection of critical assets, and continuity of business operations.

Urgency

Many CISOs already recognize the limitations of their current SOC model. What has shifted is that boards, executive leadership, and even regulators now see those weaknesses as well. Cybersecurity has become a board-level priority, and the ability to respond to threats, demonstrate measurable risk reduction, and maintain operational continuity is under constant scrutiny.

In this environment, maintaining a homegrown SOC with thin staffing, manual triage, and reactive processes is not resourceful; it is a strategic liability. For organizations refreshing their technology stack, struggling to sustain 24/7 coverage, or preparing for cyber insurance renewals, the time to evaluate alternatives is before a breach, not after one forces the issue.

Risk

Operating an under-resourced SOC carries structural risks that compound over time:

- **Analyst burnout** – High annual turnover increases detection and response gaps, erodes institutional knowledge, and raises legal liability in the event of delayed or inadequate incident handling.
- **Coverage gaps** – Lack of true 24/7 monitoring, inconsistent skill levels across shifts, and gaps in coverage during staff absences leave organizations exposed to threats that require constant vigilance.
- **Impact of detection delays** – Delayed or missed detections dramatically increase the cost and scope of breaches. Compared to MDR providers that operate at far greater speed, under-resourced SOCs face magnitudes higher costs due to prolonged dwell time and slower containment.

- **Tool underutilization** – SIEM, XDR, and SOAR platforms often operate far below capacity, producing low-quality alerts that consume analyst time without improving security outcomes.
- **Compliance exposure** – Gaps in incident readiness and reporting processes increase the probability of failed audits, regulatory fines, and operational disruption.

The cost of these risks is rarely confined to IT budgets; they directly influence business performance, brand reputation, and the confidence of customers, partners, and investors.

Deepwatch Perspective on Urgency and Risk

Deepwatch frames urgency and risk in terms of **cyber resilience**: the ability to anticipate, withstand, recover from, and adapt to adverse conditions in an environment where attack speed, automation, and complexity are accelerating. From the company's perspective, the operational pressures on security teams are no longer just about detecting threats quickly; they are about sustaining effective operations under constant stress while aligning security actions to business risk.

Several factors shape this urgency:

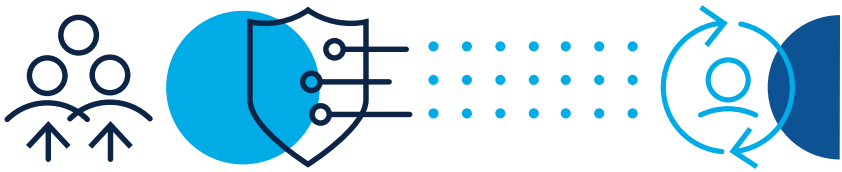
- **Attack velocity** – Deepwatch notes that compromise can occur in under 10 minutes, with identity-based attacks and cloud-targeted incidents increasing at double-digit rates year over year.
- **Talent scarcity** – The security skills gap continues to widen, making it difficult for organizations to build and maintain the level of expertise required for 24x7 SOC operations.
- **Data overload** – Expanding attack surfaces and tool sprawl generate overwhelming alert volumes, increasing the risk of missed signals and delayed response.
- **Board-level scrutiny** – Executives and directors expect measurable visibility into business risk reduction and operational readiness.

02 Urgency and Risk

In response to these pressures, Deepwatch's model focuses on:

- **Exposure-aware detection** – Prioritizing alerts by contextual business risk, mapped to frameworks like MITRE ATT&CK, to ensure high-fidelity detection over noise.
- **Accelerated response** – Embedding SLA-backed triage and containment processes to reduce dwell time and improve operational predictability.
- **Integrated AI and human capabilities** – Leveraging AI and automation for scale while retaining analyst-led investigation and decision-making to address complex cases.
- **Operational continuity** – Reducing the dependency on overstretched internal teams by providing continuous coverage without requiring constant expansion of headcount.
- **Business-relevant reporting** – Delivering outcome-focused metrics that link security activity directly to posture improvement, enabling clearer communication with leadership and boards.
- **Customer alignment** – Aligning customized security services to the client's priorities and existing tech investments.
- **Being tuned to the customer's environment** – Training on the customer's priorities and the stack they've invested in to strengthen its defenses and focus on the risks that matter most.

Deepwatch positions this approach as a way to help clients move beyond reactive security operations and toward a sustained state of resilience—one that can adapt to the evolving threat landscape while meeting business and compliance expectations.



03 Benefits

Benefits of MDR

MDR provides an alternative to operating an in-house SOC that addresses persistent challenges in staffing, technology maintenance, and incident readiness. Common advantages include:

Access to specialized expertise – Around-the-clock monitoring, detection engineering, and incident response without the need to recruit and retain scarce talent.

Improved detection and response speed – Integrated platforms and automation reduce dwell time and accelerate containment.

Operational predictability – Service-based delivery offers a defined cost structure, replacing unpredictable, incident-driven spending.

Continuous capability evolution – Providers integrate new detection capabilities, threat intelligence, and tooling without requiring the client to manage the engineering effort.

Reduced staffing burden – Eliminates the need to staff 24x7 shifts internally, allowing in-house teams to focus on strategic initiatives.

"MDR provides an alternative to operating an in-house SOC that addresses persistent challenges in staffing, technology maintenance, and incident readiness."

03 Benefits

How Deepwatch Extends MDR Value

Deepwatch's approach builds on the foundational benefits of MDR with a precision-oriented model that combines intelligence-driven detection, embedded expertise, and outcome-focused reporting:

Intelligence-driven, exposure-aware detections – Alerts are prioritized using real-world threat intelligence, MITRE ATT&CK mappings, and contextual business risk—going beyond static signatures.

Streamlined triage and response – Accelerated investigation and reduced dwell time deliver measurable improvements in response speed.

Analyst expertise and tradecraft – Skilled security professionals deliver tailored insights and operate as a seamless extension of the internal team.

Business-aligned insights with metrics that matter – Executive-ready reporting provides clear, outcome-focused indicators of security posture improvement, bridging the gap between technical operations and strategic priorities.

Reduced operational burden – Removes the need to staff 24x7 shifts or expand headcount, freeing up internal resources for high-impact initiatives and strategic projects.

AI initiatives to augment the human in the loop – Deepwatch is pursuing multiple AI initiatives to augment human expertise:

- AI SOC analyst: Automates investigations with playbooks, guides response actions, and delivers explainable context to accelerate analyst decision-making.
- Reimagined customer experience: Natural language copilots and collaborative AI workflows that enhance how customer teams interact with and act on intelligence from Deepwatch.

04 Best Practices

Five Stages to Building a Comprehensive, Modern SOC (Security Response Program)

1. STRATEGIC FOUNDATION

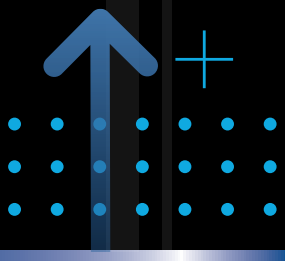
- Define a modern security response program rather than defaulting to a traditional SOC buildout.
- Align objectives with business priorities and the organization's risk appetite.
- Ensure executive and board-level understanding of security's purpose, metrics, and value.

2. PEOPLE AND PROCESS DESIGN

- Build a structure that mitigates analyst burnout and turnover, with clear roles for threat hunting, incident response, and risk analysis.
- Develop operational playbooks for detection, investigation, and containment.
- Foster cross-departmental engagement between IT, compliance, risk, and business stakeholders.

3. TECHNOLOGY AND TELEMETRY INTEGRATION

- Map current data sources, gaps, and toolsets (e.g., SIEM, EDR, CNAPP, vulnerability management, identity systems).
- Ensure your partner is tuned to your business, your priorities, and the stack you've invested in.
- Integrate new capabilities into workflows without creating alert fatigue.
- Leverage automation and AI for scale, keeping human analysts in the loop for context and decision-making.
- Develop a strategy that includes preemptive, proactive, and responsive security measures.
- Ensure your cybersecurity strategy maps to MITRE and other relevant frameworks.



4. OPERATIONALIZATION AND CONTINUOUS IMPROVEMENT

- Establish 24x7 monitoring with clearly defined SLAs for triage, escalation, and response.
- Implement a continuous tuning process to adapt detections to the evolving threat landscape.
- Use outcome-based metrics and regular reporting to demonstrate improvements in security posture.

5. RESILIENCE AND ADAPTATION

- Evolve beyond detection and response to include proactive capabilities such as threat hunting, attack surface management, insider threat detection, and vulnerability reduction.
- Conduct regular assessments and readiness drills, and integrate new tools or methods as the threat landscape changes.
- Maintain flexibility so the SOC can adapt to technology shifts, business changes, and regulatory demands.

"Engaging with Deepwatch is not a 'set-and-forget' transaction. It is an operational partnership that works best when built on clear objectives, shared accountability, and continuous alignment between security priorities and business outcomes.'

04 Best Practices

Best Practices for Maximizing Value from Deepwatch

Engaging with Deepwatch is not a "set-and-forget" transaction. It is an operational partnership that works best when built on clear objectives, shared accountability, and continuous alignment between security priorities and business outcomes. Organizations that see the greatest returns treat Deepwatch as a strategic extension of their SOC, integrating processes, tools, and people into a unified operational model.

KEY PRACTICES

- **Align security to business priorities** – Define objectives that reflect broader strategic goals so detection and response activities focus on the most material risks.
- **Establish transparent communication channels** – Treat Deepwatch's analysts and detection engineers as part of the internal team. Maintain regular, candid dialogue to surface challenges, clarify priorities, and share threat intelligence.
- **Leverage AI and human expertise for continuous assessment** – Use Deepwatch's combined AI-driven and human insights to regularly review detection coverage, vulnerability exposure, and emerging threats, enabling proactive tuning of defenses.
- **Integrate internal and external playbooks** – Align internal incident response protocols with Deepwatch's automated and analyst-led processes to reduce friction during critical events.
- **Invest in staff enablement** – Provide ongoing training so internal teams understand Deepwatch's workflows, escalation processes, and context.
- **Continuously monitor and adapt** – Collaborate with Deepwatch to evaluate performance metrics, incident data, and evolving threats, adapting both service configurations and internal processes accordingly.

By approaching the engagement as a true operational partnership, CISOs can extend the reach of their SOC, reduce costs and operational risk, and ensure security operations evolve in step with both the threat landscape and business priorities.

05 Organizational Impact

MDR in General

Engaging with an MDR provider drives changes that extend well beyond the security operations function. It often prompts:

- **Structured change management** – Training programs to familiarize staff with new systems, processes, and escalation pathways.
- **Cultural shift** – Security reframed from a technical afterthought to a core business function, fostering an enterprise-wide culture of vigilance.
- **Cross-department collaboration** – Improved coordination between IT, compliance, risk, and business units, breaking down operational silos.
- **Operational adjustments in adjacent teams** – Help desk workflows updated to address security-related queries; executives briefed on new metrics and risk reporting frameworks.
- **Customer trust gains** – Enhanced ability to demonstrate improved security posture to clients, partners, and regulators.

From a people perspective, MDR adoption changes how security teams operate:

- Analysts move from high-volume alert triage to more strategic threat hunting, intelligence analysis, and advisory roles.
- Burnout and turnover are reduced, improving staff retention and institutional knowledge.
- Overtime and baseline monitoring training costs are replaced by investments in higher-value skill development.

Financially, MDR can offset multiple cost centers—reducing recruitment needs, lowering tool management overhead, and stabilizing long-term SOC expenses—while allowing security leadership to redirect resources toward risk-reduction initiatives aligned with business priorities.

05 Organizational Impact

Deepwatch Perspective

Deepwatch's operating model reinforces and accelerates these organizational impacts by working as an extension of the customer's team.

This approach enables:

- **Faster role evolution for internal teams** – Deepwatch assumes the burden of 24x7 monitoring, allowing internal analysts to focus on proactive threat hunting, purple team exercises, and security architecture improvements.
- **Deepwatch expertise for skill development** – Ongoing collaboration with Deepwatch's team creates opportunities for internal staff to expand their capabilities in threat intelligence, incident response, and compliance readiness.
- **Operational efficiency and retention** – AI-assisted triage and exposure-aware detection reduce noise, helping keep workloads manageable and turnover low.
- **Clear business communication** – Executive reports tie security activities to posture improvements, giving leadership tangible, business-aligned outcomes to track and communicate externally.
- **Optimized investment profile** – Licensing models tailored to scope and scale help right-size tool usage, streamline operations through the unified platform, and lower the sustained cost of running a 24x7 SOC.

For many organizations, Deepwatch's model doesn't just modernize SOC operations—it acts as a catalyst for broader security maturity, creating operational headroom for strategic initiatives and resilience planning, while providing cost savings in addition to these improvements.

06 Solution Timeline

Typical MDR Implementation

Most MDR transitions follow a structured, phased process designed to minimize operational disruption while accelerating time to value:

- **Discovery** – Assess current security environment, mapping telemetry sources, identifying coverage gaps, and establishing an exposure baseline.
- **Integration** – Connect MDR services to the existing security stack (e.g., SIEM, EDR, vulnerability management, CNAPP) to preserve prior investments.
- **Deployment** – Validate core detection and response workflows in a controlled environment before full rollout.
- **Operationalization** – Establish regular reporting, tune detection rules, and align incident response playbooks with business priorities.

Deepwatch Implementation

Deepwatch's process mirrors the general MDR model but is designed for accelerated execution and earlier operational value:

- **Rapid deployment** – Proof of concept in under 48 hours, enabling early validation of detection logic and workflows.
- **Continuous tuning and accountability** – Weekly executive reporting and ongoing optimization of detections, response actions, and business-aligned metrics.

This approach allows organizations to reach full operational maturity more quickly while maintaining continuous alignment between Deepwatch's platform and the client's security priorities.

07 Future Considerations

For MDR in General

The threat landscape will continue to evolve rapidly, with attackers leveraging automation, AI, and increasingly targeted tactics. MDR providers are expanding their capabilities beyond detection and response, moving "left" in the security lifecycle toward proactive risk identification and exposure reduction. For CISOs, this shift requires:

- **Regular capability assessments** – Evaluating whether the MDR service continues to address the organization's most material risks as threats and business priorities change.
- **Proactive engagement** – Maintaining an ongoing dialogue with the provider to understand and leverage new capabilities as they are introduced.
- **Strategic integration planning** – Ensuring that evolving MDR capabilities align with the broader security architecture and technology roadmap.
- **Business alignment** – Framing MDR enhancements in terms of measurable risk reduction and resilience improvements that resonate with executive leadership and boards.

Organizations that take a forward-looking approach—anticipating changes rather than reacting—are better positioned to sustain resilience, reduce long-term costs, and maximize the return on their security investments.

"The threat landscape will continue to evolve rapidly, with attackers leveraging automation, AI, and increasingly targeted tactics. MDR providers are expanding their capabilities beyond detection and response, moving 'left' in the security lifecycle toward proactive risk identification and exposure reduction."

07 Future Considerations

Deepwatch Perspective

Deepwatch is expanding its Guardian MDR Platform to incorporate capabilities that address threats earlier in the security lifecycle, with the goal of moving from reactive containment to proactive prevention. This "shift-left" strategy includes:

- **Attack surface management** – Collaborating with clients to map external exposures, continuously monitor for emerging vulnerabilities, and provide prescriptive recommendations to reduce risk.
- **Insider threat detection** – Leveraging behavioral analytics and threat hunting to identify and respond to insider risks that may evade traditional security controls.
- **Dark web monitoring and response** – Providing actionable intelligence on criminal activities targeting the organization's assets across the open, deep, and dark web.
- **Managed vulnerability management** – Identifying critical assets, prioritizing vulnerabilities based on business risk, and guiding remediation to address the most significant threats.
- **Incident response "zero to retainer" model** – Offering immediate access to incident commanders and expert resources during high-impact security events to contain and analyze threats before they escalate.
- **Advanced isolation and containment** – Integrating capabilities to rapidly isolate compromised assets and limit lateral movement during an attack.
- **AI-driven risk and exposure management** – Strengthened by the acquisition of Dassana, enabling deeper automation, real-time visibility, and agentic AI-driven decision support in security operations.

Deepwatch positions these capabilities not as discrete services, but as integrated elements of a broader resilience strategy—aligning proactive threat identification, continuous monitoring, and rapid response with the organization's operational priorities. This trajectory reflects a fundamental industry trend: MDR evolving into a full-spectrum resilience platform that blends prevention, detection, and response into a single, continuously improving capability.

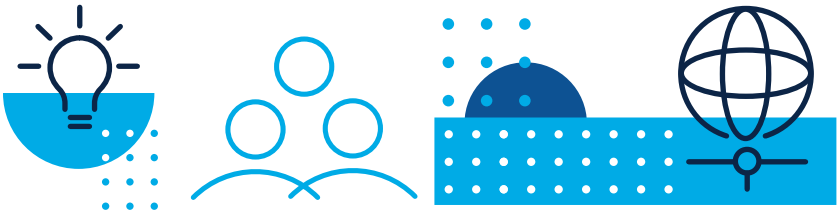
08 Analyst's Take

IT'S NOT BRAVE to keep running your own SOC in 2025—it's reckless and expensive.

The threats have changed. The pressure has changed. The economics have changed. What hasn't changed is the expectation: respond fast, reduce risk, prove resilience.

Deepwatch gets this right, not just with better technology, but with a better philosophy: one that treats detection and response as a resilience function, not a staffing function.

You don't need more analysts. You need the right partner.



Report Methodology

DEEPWATCH

THIS GIGAOM CXO DECISION BRIEF ANALYZES a specific technology and related solution to provide executive decision-makers with the information they need to drive successful IT strategies that align with the business. The report is focused on large impact zones that are often overlooked in technical research, yielding enhanced insight and mitigating risk. We work closely with vendors to identify the value and benefits of specific solutions, and to lay out best practices that enable organizations to drive a successful decision process.

About Chris Ray

CHRIS RAY IS A VETERAN OF THE CYBERSECURITY DOMAIN. He has a collection of experiences ranging from small teams to large financial institutions. Additionally, Chris has worked in healthcare, manufacturing, and tech. More recently, he has acquired an extensive amount of experience advising and consulting with security vendors, helping them find product-market fit as well as deliver cybersecurity services.

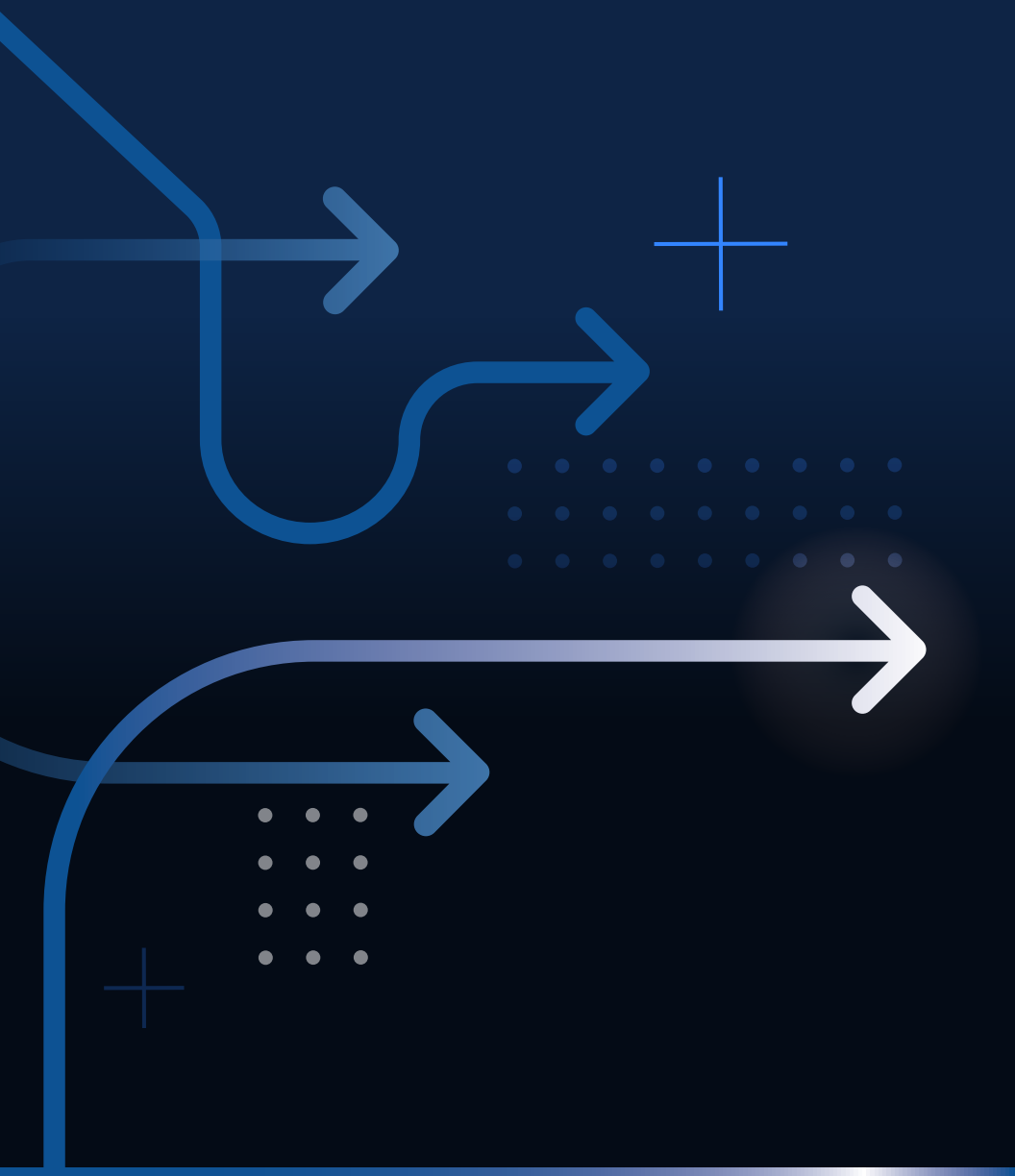
GIGAOM

About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.



GIGAOM

GigaOm democratizes access to strategic, engineering-led technology research. We enable businesses to innovate at the speed of the market by helping them to grasp new technologies, upskill teams, and anticipate opportunities and challenges. The GigaOm platform changes the game, by unlocking deep technical insight and making it accessible to all.