torq

Future-Proofing MDR With Hyperautomation

How to boost speed and efficiency, increase margin, and scale your MDR offerings.

Opportunities and Existential Challenges in the MDR Landscape

As threats evolve, data proliferates, and organizations struggle to staff their SOCs, managed detection and response (MDR) providers have unprecedented potential for growth. As companies seek to outsource their threat detection, response, and remediation, Gartner predicts that 60% of organizations will use an MDR by 2025.[1]

60%

of organizations will use an MDR by 2025.[1]

Gartner

However, MDR providers face the same threat evolution, data volume, and talent shortage challenges as their customers. They also have to maintain customer trust and a competitive position in a crowded and dynamic market—often while using legacy solutions that can't effectively scale to meet current demands, let alone those of the future.

30%

Data volume is growing 30% year over year.[2]

IDC

To keep pace with ever-changing challenges, maintain and extend customer value, quickly develop and roll-out additional managed services and remain competitive in a highly dynamic space, MDRs should adopt hyperautomation. In this guide, we'll examine:

- Differences in value generation between legacy automation and hyperautomation
- How hyperautomation improves on SOAR (security orchestration, automation, and response) and other security functions
- The ways in which hyperautomation can deliver better business outcomes for MDR providers

By 2024, enterprises will use at least 3 hyperautomation solutions and reduce operational costs by 30%.[3]

Gartner

Hyperautomation vs. Automation: Next-Level Efficiency, Agility, and ROI vs. Taking Care of Just a Few Processes

Conventional security automation made some processes faster and easier for security teams. Hyperautomation provides exponentially more value both by addressing significantly (on two orders of magnitude) more use-cases and allowing more role-players and teams to contribute to delivering more efficient detection and response services to customers, including through:

- **Low-code / no-code** tools that democratize the access to automation, allowing security role-players with different levels of technical acumen and who are responsible for different pillars of the organizational cybersecurity policy to leverage them with **powerful simplicity**
- **Infinite integrations, extensibility and scalability,** which makes it possible to extend automation scenarios beyond those that a traditional SOAR could "dream of" and to integrate automated processes – fully autonomous or human-in-the-loop – with any technology in the ever-evolving organizational hybrid IT stack with its **radical extensibility**
- **Generative AI** that can be leveraged either during the design phase of automated processes to increase the ROI even further, or during the investigation of security signals, driving the amount of human involvement required in Tier-1 and Tier-2 analysis down by as much as 90%

The powerful benefits of hyperautomation empower MDR providers to reduce costs through unrivaled efficiency and extensibility, while also enabling them to maximize their returns by serving more customers and more effectively allocating resources. This combines to give MDR providers faster time to value and swifter ROI.

Challenge: SOAR Can't Address Growing Attack Complexity and Pace

SOAR offerings evolved as on-premises solutions to bridge the gap between incident detection and the process leading to its resolution. While SOAR can orchestrate different processes and automate a wide range of actions that are otherwise performed manually, the complexity of its operationalization is restricting its utility to a small number of use-cases, rather than being comprehensive.

> As IDC analyst Chris Kissel observes, "SOAR's rigidity in dealing with dynamic and multifaceted attacks creates another issue by frequently presenting analysis that does not fully integrate the broader context or underlying connections between different security events."[4]

MDRs that rely on legacy SOAR technology will find it difficult to identify how elements of a multi-pronged attack are related or to contextualize attacks in a timely way. Slow response times and missed connections can leave MDR customers at risk of incidents, as increasing the "depth of an investigation" might require costly customized integrations and data correlation that isn't easy to perform with traditional SOARs.

How Hyperautomation Overcomes Legacy SOAR Limitations

As hyperautomation leverages a confluence of technologies, such as, but not limited to low-code/no-code, generative AI and infinite integrations, to address the challenge of making automation of large volumes of security procedures possible, it manages to overcome the limitations presented by the traditional SOAR solutions and drive to the following outcomes:

- More processes and more scalability means that teams can process larger amounts of security alerts, driving more proactive security and preventing potential incidents at a very early stage
- Extensibility allows the automation and orchestration to encompass all components of the organizational IT and security stack, from legacy appliances to modern cloud services, which enables a much more comprehensive analysis to take place and drive to better and more accurate conclusions
- Modern cloud-native architecture – that is required to allow the desired scalability – also ensures the right balance between the infrastructure cost and the ability to process events in a timely fashion, removing the challenges of underprovisioning and overprovisioning that have traditionally impacted any SOAR deployment

These outcomes give MDR providers the ability to deliver a differentiated and competitive service to their customers while revolutionizing the managed services they provide and ultimately reducing the costs they incur providing that service.

Situation Analysis: SOAR Versus Hyperautomation

SOAR	Hyperautomation	Advantages of Hyperautomation
Reactive	Proactive	SOAR platforms are designed to initiate actions based on alerts or IoC. However, SOAR does not help preventative actions such as automated testing, cybersecurity posture assessment, and connection to identity and access management logs/behaviors (features offered by hyperautomation).
MTTD/MTTR	Mean-time-to-innocence	SOAR is designed to initiate playbooks at the time of alert and execute a workflow. Detection and response is good as far as it goes, but networks need to be returned "whole," making certain the adversary has been defeated and the company's cybersecurity posture has been returned to its golden state. Hyperautomation includes configurations, attack path analysis, and BAS.
Connects devices	Connects devices, clouds, containers, and processes	At its inception, SOAR platforms tend to be designed for on-premises use cases, but its connectivity options are only over APIs. Hyperautomation creates a connectivity mesh using API calls to connect hyperscalers, data lakes, Kubernetes, SaaS applications, SSH, and even remote shell/PowerShell.
Connectivity is as strong as the sum of its APIs	Enterprise-grade extensibility	SOAR is often prebuilt. The connections between devices are determined by code written in Python. Hyperautomation provides no-code and low-code connection offering drag-and-drop options.
Either overprovisioned or underprovisioned	Matches the resources needed for outcomes	A hidden cost in SOAR is the time and effort needed to "stand-up" the platform. Hyperautomation is deployed as a SaaS-native requiring no professional services.

Source: IDC, 2023

Challenge: Analyst Overload Threatens Efficacy

> "Alerts are **the bane** of security operations' existence"[5]
>
> IDC

Security analysts only have time to address half of the alerts they're slated to review each day, and nearly half say average detection and response time has increased within the past two years.[6]

Because MDR providers have an SLA with their customers, they are required to analyze incoming events within a specified and agreed upon time frame. Slower response times to alerts put MDR providers in the precarious position of incurring extra costs through having to hire additional analysts. The ongoing shortage of talent, as analysts burn out from a never-ending flood of high-stress, low-value rote tasks, exacerbates this challenge, as it makes finding, hiring, and training new analysts a much costlier endeavor. Fifty-five percent of SOC analysts said they have considered quitting "due to the pressure they feel,"[7] and the percentage of organizations hit by the security skills shortage has risen to 71%, up from 57% in 2022.[8]

Hyperautomation Lets Analysts Cut Through the Noise and Resolve Tickets Faster

Hyperautomation allows MDRs to:

More quickly enrich and investigate 90% of Tier-1 security alerts.

Proactively identify threats, prioritize investigations, and elevate cases to the appropriate analyst.

Free up time for analysts to focus on high-priority threats.

Provide playbook guidance to assist analysts with cases.

The result is less analyst time spent on noise, faster time to resolution, and a more rewarding work environment for analysts, which can help reduce attrition. It also leads to cost savings and SLA attainment, as MDRs do not have to add resources to combat the ongoing barrage of alerts and events their customers face.

Challenge: MDRs Need Better Visibility, Integration, and Agility

76

"The average enterprise uses 76 different security tools."[9]

panaseer

Fragmented security stack components, data, and processes are a drag on efficiency and response times, whether they occur within an organization's SOC or within an MDR provider. Inefficient SOC operations can also contribute to analyst burnout and turnover.

While enterprise organizations, at least, are at the helm when it comes to choosing their own security stack, MDRs quite often need to work (i.e., integrate) with whatever security solutions their enterprise customers already use.

Organizations have the option to outsource to get around structural challenges. MDRs must overcome their challenges in order to deliver maximum client value at the highest possible margin, so they can keep customers, retain employees, maintain cash flow, and stay competitive.

Hyperautomation Drives Better Business Outcomes for MDRs

Hyperautomation doesn't only improve SOC operations and security posture. Cybersecurity hyperautomation can also help MDRs achieve better business outcomes in several areas.

Accelerate Time to Value

For MDRs, onboarding a new customer to their service means executing repetitive provisioning of various integrations and automations in that particular customer's environments. This process contributes to higher customer acquisition costs for an MDR, and dictates both the pace with which the MDR provider can onboard new customers and the speed of ROI it provides to its subscribers.

Implementing hyperautomation for customer onboarding – even before any actual detection and response take place – ensures a reduction in CAC for an MDR provider and improvement on ROI for the service subscribers.

Increase Margins

In addition to reducing customer acquisition costs through less costly onboarding, hyperautomation allows MDRs to automate more components in their alert investigation, analysis and response, and handle security events more efficiently with less human involvement.

> "By 2024, organizations will lower operational costs by 30% by combining hyperautomation technologies with redesigned operational processes."[10]
>
> Gartner

Automated workflow management across the customer base, combined with fine-grained customization, helps MDRs improve operational efficiency.

Maximize Security Investments

Hyperautomation's extensibility and limitless integrations give MDRs the ability to easily work with multiple security and other solutions deployed by their customers, leading to greater efficiency and lower costs. An ideal hyperautomation solution will support this process by enabling:

- API calls for anything
- Pre-configured API connectors for the most widely used security solutions
- No-code, low-code, and full-code support for extending any existing connectors or providing new ones with ease and flexibility
- Support for any command line interface, platform, and programming or scripting language

This ease of comprehensive integration can protect the investment they've made in their own security stack, while also more easily working with their customers' stacks.

With hyperautomation, MDRs can also automate workflow management across their entire customer base with the added flexibility of fine-tuned customization.

Accelerate Analyst Response

Hyperautomation empowers an MDR's analysts to respond to threats much more quickly and process more security alerts. This allows the MDR to work with more customers without increasing expenses and adding more analysts.

Building automation of the socio-technical processes involving human analysts also ensures consistency when hiring and ramping up new analysts, providing more growth flexibility to MDR organizations.

Improve Analysts' Experiences

Hyperautomation that leverages AI automates repetitive tasks rapidly and at a massive scale, so your analysts can address the threats that matter, faster. Accelerated case management with AI can also provide necessary context for more strategic threat responses.

> "Growth in the cybersecurity workforce gap once again outpaced growth in the active workforce. The shortfall between the number of workers needed and the number available grew 12.6% year-on-year to 4 million worldwide."[11]
>
> ISC2

Alleviating the drudgery of rote work allows analysts to focus on solving more challenging problems, which makes work more engaging. Freed-up time can also be used to improve the employee experience and reduce attrition by addressing the skills gaps and providing other professional development. Taken together, these improvements can reduce employee turnover and save MDRs from having to spend the time and money finding, hiring, and training new analysts to replace those who leave.

11 ISC2 Cybersecurity Workforce Study

Boost Customer Satisfaction and Deliver a Differentiated Service

Delivering exceptional service is always a competitive differentiator. It's even more critical now, as many organizations take a closer look at their budgets and vendors—and have many options to choose from if they feel their current MDR isn't meeting their expectations.

78%

of business buyers say their company "is more careful about spending money than before."[12]

salesforce

76%

say their company "extracts maximum value from every purchase."[12]

salesforce

Hyperautomation's benefits for MDRs create more positive experiences for their customers, including better and more consistent SLA attainment, more comprehensive event detection, and greater availability of analyst resources to address the highest-priority issues faster.

Hyperautomation also helps MDRs deliver a more differentiated managed service to their customers. The ability to easily integrate with more signals and enrichment, and the ability to rapidly roll out more automated processes gives MDRs an edge over their competitors. Developing automations in an agile way, connecting to more tools, and pulling in more aspects of data to consider gives MDR providers a more specialized and differentiated service, leading to deeper value with their customers and increased satisfaction.

These experiences strengthen customer loyalty, reduce customer churn, and position the MDR as a true partner in value creation, rather than simply a vendor.

How Torq Hyperautomation Enables MDRs to Optimize Their Security Environment

Torq Hyperautomation makes it easy for MDRs to:

Integrate Security Stack Components

In the complex world of cybersecurity, onboarding and keeping up with API changes across numerous third-party security tools can be daunting, often resulting in automations breaking at the worst and unexpected times.

Torq solves this challenge by continuously monitoring APIs from various third-party security vendors, detecting any changes or updates, and then automatically adjusting the integrations with the affected third-party APIs. The update is done without any need for manual intervention, ensuring that automations remain uninterrupted and functional, this also saves time and resources but also reduces the likelihood of human error.

Unify Data and Processes

Unifying data and processes is fraught with challenges, often organizations grapple with integrating diverse and siloed data sources, leading to fragmented security visibility and insights. Additionally, maintaining scalability and performance with an exponential growth in the number of security events while effectively parsing the data to identify the latest evolving cyber threats with high accuracy to avoid false positives.

Torq addresses these challenges with hyperautomation by offering seamless integration capabilities to effortlessly consolidate data from diverse security tools and sources, ensuring a unified and comprehensive security view. Unique in its approach, Torq simplifies the complexity of security hyperautomation by

dramatically elevating non-technical user capabilities, providing them with the power of a developer when interacting with APIs and services, while providing no-code, low-code, and full-code support for power users.

Torq Hyperuatomation can handle unlimited events and sort through the noise better than any human team could. It can find the “needle in the haystack” at scale, and send them to human operators for more advanced automated analytics.

Improve Operational Efficiency and Reduce SOC Costs

SOCs face significant challenges in managing operational efficiency and controlling costs, particularly in the context of managed detection and response (MDR) services. The complexities of customer onboarding and offboarding, maintaining consistent global policies across diverse customer environments, and the need for continuous monitoring and management of security events place a substantial burden on a SOC’s operational efficiency. Coupling this with managing an overwhelming volume of security alerts while maintaining many complex processes makes MDR’s lives more challenging.

Torq’s hyperautomation platform is designed to be flexible and adaptive, enabling MDRs to rapidly adjust by automating many of the essential yet time-consuming tasks, while minimizing the potential for human error. Additionally, Torq Hyperautomation has many MDR-specific functions like:

- The ability to apply global security policy enforcement across customers, while allowing for customizations to individual tenants.
- Cases Omniview allows for a consistent and unified case management lifecycle, while keeping the data across different customer environments strictly segregated.
- AI-driven intelligent threat identification, prioritization, and analysis utilizes generative large language models to analyze data sets and disparate events from security tools and other sources to make correlations to identify and prioritize threats.

- Generative AI takes this a step further by automating the triage and resolution of common SOC requests and security events, which typically consume a significant portion of SOC resources. This AI-driven automation not only speeds up response times but also ensures consistent and accurate handling of security events

Torq's unique value in reducing SOC costs lies in its ability to automate and optimize critical processes, enhance operational efficiency, and ensure a high standard of security and compliance with fewer resources. This makes Torq's solution not just a tool for managing security threats, but also a strategic asset for cost-effective managed detection and response operations

The result is a more agile MDR that's better positioned to adapt as new threats, technologies, and best practices emerge.

Torq Delivers Industry-leading Hyperautomation for MDRs

The AI-driven enterprise-grade Torq Hyperautomation platform unifies and automates the entire security infrastructure to deliver unparalleled protection and productivity.

> **"By leveraging Torq Hyperautomation, we're able to help our customers gain better evidence, analysis, and control over their cybersecurity, ensuring rapid, complete responses while staying protected from external threats and operational risks."**
>
> **Charlie Thomas**
> CEO, Deepwatch

Torq allows MDRs to drive maximum value and efficiency from existing security investments and to supercharge their security teams.

With Torq:

- Up to 90% of all Tier-1 case analysis tasks can be performed by an autonomous AI agent
- MDRs can onboard and provision new customer environments 10 times faster
- MDRs can handle up to 5 times more events without growing their teams, which improves margin

Torq offers MDRs unprecedented value by providing a scalable and resilient infrastructure-as-a-service, which takes the pressure off MDRs to build and host their own infrastructure for their customers. Torq also helps MDRs develop additional managed and automated procedures for their customers and safely roll them out to production, which helps them develop more services and grow their business – a process that was often slow and more costly with legacy SOAR solutions.

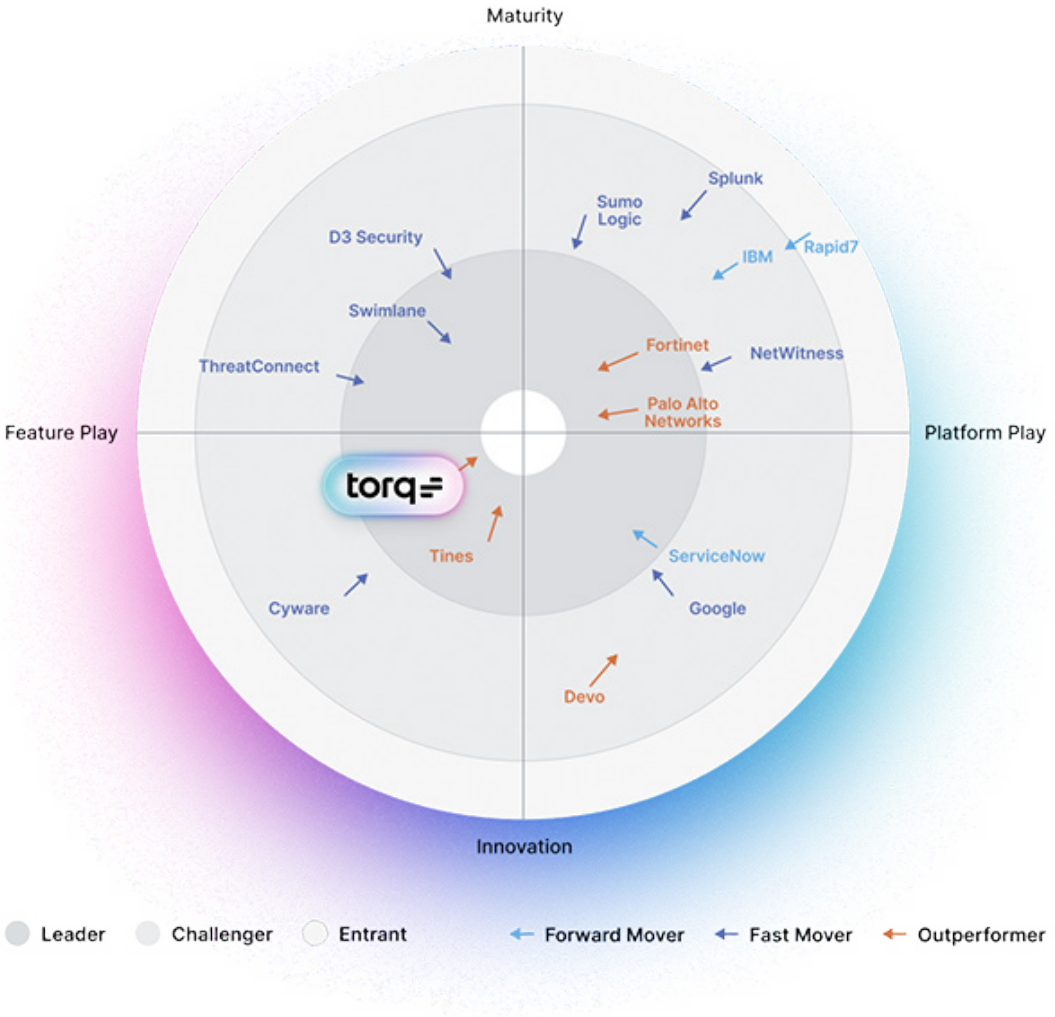
Additionally, Torq gives MDRs:

- **No-code, low-code, and full-code support,** which helps automate more detection and response processes to drive efficiency and increase margin
- **Accelerated case management,** which empowers MDRs to handle more security events for more customers with the same number of analysts, while also improving the quality of response, cutting down heavily on manual effort
- **Limitless extensibility** through the ability to integrate with various security systems at the customer side, which increases business value and widens an MDR's total addressable market
- **Automated customer onboarding and ramp-up,** which is a departure from legacy SOAR, which forced MDRs to copy automations between services and maintain multiple servers

> "Torq scores high on a number of key criteria, including case management and collaboration, automated alert prioritization, triage and curation, autonomous operations, and validation and red teaming."
>
> **GigaOm Radar Report**

GIGAOM

The latest GigaOm Radar Report describes Torq as a leader in the space, placing Torq in its leader's circle for features and innovation.



Torq also earned a positive assessment for its comprehensive features from IDC in its Spotlight Report, "How Hyperautomation Is Used to Reduce Gaps and Inefficiencies in Network Cybersecurity."

> "The Torq hyperautomation approach is more comprehensive than what is offered in contemporary cybersecurity tooling."
>
> IDC

Enhance and Future-Proof Your MDR Services

See how Torq Hyperautomation can accelerate your time to value, reduce your costs, improve your agility, and increase the value you deliver to your customers, so you can stay competitive now and be prepared for what's next.

Schedule a Demo