FROST & SULLIVAN

TRANSFORMATIONAL GROWTH LEADERSHIP

A CEO Perspective

From Hyperautomation to Agentic AI: How Torq Is Advancing Cybersecurity Operations

An Exclusive Conversation Featuring



Ofer Smadari
CEO
Torq



Adrian Drozd
Associate Partner &
Practice Area Leader
Frost & Sullivan



Pranav Sahai
Analyst,
Global Security & AI
Frost & Sullivan



Cybersecurity operations are at a turning point. Artificial intelligence (AI) is accelerating software development, vulnerability discovery, and attacks, while expanding attack surfaces, rising alert volumes, and fragmented workflows are challenging traditional security approaches. Keeping pace requires more than faster detection; it demands a rethink of how security teams investigate, make decisions, and respond.

For Ofer Smadari, CEO of Torq, this shift is driving the evolution from security hyperautomation to an end-to-end AI security operations center (SOC) platform that connects detection, triage, investigation, automation, and case management. By combining deterministic workflows with AI-driven reasoning and contextual intelligence, Torq aims to apply agentic capabilities where they deliver the greatest value while balancing operational efficiency and cost.

In this Transformational Growth Leadership conversation, Smadari explores how AI is reshaping cybersecurity operations, Torq's evolution toward an integrated AI SOC platform, and the balance between agentic autonomy and operational efficiency. He also discusses why security teams need to operate at machine speed, how contextual understanding can improve automated decisions, and why innovation must be supported by sound execution and a sustainable business model.

> "We must keep reinventing ourselves to stay relevant. The opportunity lies in bringing AI-driven investigation, automated triage, and contextual intelligence together into an integrated security operations platform."
>
> — Ofer Smadari, CEO of Torq

All rights reserved ©2026 Frost & Sullivan | www.frost.com

Transformative Shifts Reshaping Cybersecurity Operations

Adrian Drozd: *What are the most transformative shifts reshaping cybersecurity operations today, and how do you expect them to change how organizations detect, investigate, and respond to threats over the next three to five years?*

Ofer Smadari: The pace of change has accelerated sharply as AI is being used to build software and to attack and defend organizations. We are facing a transformational era in which everything is changing much faster than before.

Organizations need to operate at machine speed. Static playbooks are no longer sufficient for triage, investigation, response, and automation. The number of vulnerabilities is growing, while remediation backlogs are already substantial. Attackers understand that organizations cannot address every vulnerability quickly enough.

Enterprises are also reconsidering whether to build and maintain their own security tools. Cybersecurity research, ongoing maintenance, scalability, and service delivery are difficult to sustain internally. The operating model is therefore shifting toward integrated platforms that can process growing alert volumes, apply context, automate investigation, and move toward higher levels of autonomy.

Adrian Drozd: *What remains fundamentally broken in security operations despite significant investment in SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), XDR (Extended Detection and Response), and other security tools?*

Frost & Sullivan's **Transformational Growth Leadership Program** aims to honor visionary business leaders who possess the foresight and leadership acumen to drive positive change within their organizations. The leaders we celebrate hail from diverse sectors and company sizes, yet they all share an unwavering commitment to innovation and excellence.

Ofer Smadari: One of the biggest challenges is fragmentation. Different vendors provide detection, triage, investigation, automation, remediation, and case management, but these capabilities need to work together.

Torq connects to customers' existing security and IT tools, ingests alerts, and moves them through a pipeline of triage, enrichment, investigation, and automation. Our platform uses a verdict mechanism to filter alerts before moving relevant cases through further investigation and automation, while unresolved cases are routed to human analysts with the relevant information.

Context is essential throughout this process. The same technical alert can have very different implications depending on the user's privileges, identity, affected assets, and business exposure. For example, an alert affecting a highly privileged user may carry a different level of risk from the same alert affecting a user with limited access. By connecting information across these areas through our Security Context Graph, which we strengthened through the acquisition of Jit, we can help organizations make better decisions and prioritize the threats that matter most.

All rights reserved ©2026 Frost & Sullivan | www.frost.com

Adrian Drozd: *Where will AI create the most meaningful impact, and which outcomes will distinguish genuine transformation from incremental improvement?*

Ofer Smadari: Automated investigation is one of the most important capabilities. Alert volumes are increasing and handling that growth with people alone is not sustainable.

The meaningful shift is from simply adding AI features to redesigning the operating model. AI can investigate alerts, apply context, and support decisions at a scale that would be difficult to achieve through manual processes alone. That is why we built Torq SOC Brain, which learns from every analyst's decision and applies that knowledge at machine speed. We are moving toward higher levels of autonomy in security operations, but that transition will happen in stages.



Scaling AI-powered Cybersecurity: Innovation and Growth

Adrian Drozd: *You have moved from a security hyperautomation platform toward an end-to-end AI SOC platform. What drove that evolution, and what is your vision for Torq over the next few years?*

Ofer Smadari: When a technology emerges that can redefine your category, you either lead the shift or get disrupted by it. We chose to lead. After generative AI emerged, we began developing agentic capabilities. We started with an investigation agent and then expanded into automated triage, contextual capabilities, the Agentic Builder, Socrates as our agent orchestrator, and AI-enabled case management. We must keep reinventing ourselves to stay relevant. The opportunity lies in bringing these capabilities together into an integrated platform. With around 300 enterprise customers, we must continue to reinvent ourselves rather than rely on what made us successful initially.

Adrian Drozd: *Where do you see the biggest opportunities for growth?*

Ofer Smadari: North America remains our largest market, while EMEA is our second largest and an important area of investment. We also see opportunities in replacing incumbent security operations platforms, as organizations seek better ways to connect workflows and manage growing alert volumes.

AI is accelerating attacks and increasing the urgency to strengthen defense. The federal sector is another important opportunity for us. Torq holds FedRAMP Moderate authorization, and government agencies face the same need to operate at machine speed. We see significant room to grow as organizations reassess how they manage their security operations and respond to an increasingly complex threat environment.

All rights reserved ©2026 Frost & Sullivan | www.frost.com

Adrian Drozd: ***What are the biggest roadblocks that could slow your growth?***

Ofer Smadari: The biggest risk is our own execution. As a fast-growing company, we need to scale our organization and operating cadence to match our product velocity across marketing, sales, customer operations, and other functions.

Ultimately, we can become a constraint on our own growth if we do not execute well. We must build the right organizational capabilities to support the next stage of the business.

From Automation to Agentic Security Operations

Pranav Sahai: ***Many vendors describe their platforms as AI-native. What architectural choices and customer outcomes must be present for that claim to be credible?***

Ofer Smadari: A major consideration is how the platform is built and how it performs at scale. Torq has rebuilt its core around agents: SOC Brain, which learns from analyst decisions; the Security Context Graph; runtime automation; the Agentic Builder; investigation; and automated triage. We also rebuilt our data layer, because building agents is not simply a matter of connecting a model to a task. Agents need the right data and infrastructure to use information effectively.

However, AI-native architecture does not mean making every step agentic. Agentic capabilities are particularly valuable when workflows require investigation, contextual understanding, or reasoning. Deterministic steps and API calls remain useful for predictable tasks with clearly defined processes.

Torq combines these approaches in a hybrid architecture, introducing AI where it adds value while retaining structured workflows for other tasks. Running every investigation entirely through AI can become prohibitively expensive at enterprise scale. A platform must therefore balance agentic reasoning with operational efficiency and sustainable economics to deliver meaningful customer outcomes.

Pranav Sahai: ***Torq uses specialized HyperAgents across triage, investigation, and response. Which workflows benefit most from this multi-agent architecture?***

Ofer Smadari: Torq is seeing strong adoption of HyperAgents, particularly in hybrid workflows. Socrates, our orchestrator, coordinates them across triage, investigation, and response. The platform helps users generate the tools and instructions needed to build agents rather than requiring every component to be assembled manually.

HyperAgents can be introduced where additional reasoning or decision-making is needed, while deterministic steps and API calls handle predictable tasks. Torq also helps customers build agents for specific use cases, fine-tune them, and maintain them over time.

The key is to apply agentic reasoning where it is useful, rather than making every operation dependent on AI. The results are measurable: SOC Brain matches analyst verdicts 85% of the time and keeps learning from every correction.

All rights reserved ©2026 Frost & Sullivan | www.frost.com

Building Trust in Increasingly Autonomous Security Operations

Pranav Sahai: *As AI systems move from recommending actions to acting and closing cases, what must be in place before organizations can safely trust autonomous security operations?*

Ofer Smadari: We are moving from a human-in-the-loop model, where people review individual actions, toward a human-on-the-loop model, where people monitor automated activity.

The level of autonomy should depend on the potential impact of a decision. For example, if a cloud security tool identifies an internet-facing asset, shutting it down may address immediate exposure. But what happens to the business if that asset is taken offline?

Our Security Context Graph helps organizations understand the potential blast radius of an action before it is taken. That context can increase confidence in automated decisions and help determine when human intervention is necessary.

Trust will also grow as organizations compare the performance of autonomous investigations with human-led processes, including the time required to respond, the quality of decisions, and the mistakes made during case management. These comparisons can help organizations assess where automation is performing well and where further oversight or improvement is needed.

Leadership, Innovation, and Sustainable Growth

Adrian Drozd: *As CEO, what leadership principles are most important to sustaining Torq's innovation, culture, and competitive advantage as the company scales?*

Ofer Smadari: We must keep building and keep executing. Execution means delivering more value to customers every day.

As the company grows, we need to introduce processes that help us prioritize. We receive many requests from customers, but not all of them can become immediate engineering priorities. We must distinguish between requirements that benefit a broad customer base and those that are more specific to individual organizations.

Our value engineering team helps us understand customer needs and determine where product investment will have the greatest impact.

We must also make sure customers can adopt new capabilities successfully. When we release a major innovation, we need to consider how customers will use it, what changes may be required, and how we can help them realize its value.

Finally, we must ensure that innovation is reflected in a sustainable business model. We cannot keep adding capabilities without considering their costs and the value they deliver to customers.

All rights reserved ©2026 Frost & Sullivan | www.frost.com

Adrian Drozd: *What is your approach to driving innovation? Is there a structured process, and how do you handle failures on the path to success?*

Ofer Smadari: Innovation requires continuous reinvention. As AI evolved, we expanded beyond traditional security automation into AI-driven investigation, automated triage, the Agentic Builder, and AI-enabled case management. The key is to recognize disruptive changes early, act quickly, and keep improving the platform to stay relevant and deliver greater value to customers.

Adrian Drozd: *What is your strategy for staying ahead of the competition, and what have you learned from competitors?*

Ofer Smadari: Staying ahead requires continuous innovation and a willingness to rethink existing products as the market evolves. We are focused on building an integrated platform that connects security operations end to end, rather than simply extending legacy capabilities. Many AI SOC vendors focus on investigation alone. Torq combines reasoning and memory with the action layer, so an investigation ends in a response, not in a ticket. Ultimately, vendors must keep adapting to remain relevant while ensuring their solutions deliver value and remain economically sustainable.

Adrian Drozd: *Finally, what is the one message you want security leaders to take away about the future of AI-powered cybersecurity operations?*

Ofer Smadari: Attackers already operate at machine speed, and many organizations do not yet realize how fast the gap is widening.

Defenders who do not match that speed will fall behind, not eventually, but now. There's no other choice.

Closing Reflection: Building Security Operations for an AI-driven Threat Landscape

Cybersecurity operations are moving toward integrated platforms that connect investigation, risk prioritization, automation, and response. For Ofer Smadari, this shift calls for combining hyperautomation, agentic reasoning, and contextual intelligence to help security teams manage growing alert volumes and respond to increasingly sophisticated threats.

Realizing this potential requires balancing autonomy with operational efficiency, manageable AI costs, and appropriate human oversight. Organizations must also build confidence in automated decisions by evaluating their accuracy, response times, and operational impact. For technology vendors, continuous innovation must go hand in hand with strong execution, customer value, and sustainable growth.

As AI reshapes both attacks and defense, Smadari's message to security leaders is clear: operating at machine speed is becoming essential to keeping pace with adversaries. The ability to combine intelligent automation with contextual decision-making and responsible autonomy will be critical to strengthening security operations.



All rights reserved ©2026 Frost & Sullivan | www.frost.com



Ofer Smadari | CEO, Torq

Ofer Smadari, CEO and **co-founder** of **Torq**, founded the company in 2020 and has led its evolution from no-code security automation to an AI SOC platform. Under his leadership, Torq raised a $140 million Series D at a $1.2 billion valuation and acquired Jit to strengthen its Security Context Graph.

An infrastructure strategist, Smadari combines deep technical expertise with experience in sales leadership and go-to-market strategy. Over the past 20 years, he has held senior security operations roles at leading financial services organizations, managed sales and business operations at Adallom (acquired by Microsoft), and co-founded Luminate Security, a Zero Trust access company acquired by Symantec just two years after its founding.



Adrian Drozd | VP Research, Associate Partner & Practice Area Leader, Frost & Sullivan

Adrian Drozd is an **Associate Partner & Global Practice Area Leader at Frost & Sullivan**, guiding global strategy and research initiatives across the security and ICT landscape. With more than two decades of experience in market intelligence and strategic consulting, he supports leading technology providers in defining growth pathways, refining market positioning, and navigating emerging trends. Adrian is known for his analytical depth, commitment to evidence-based insight, and ability to translate complex technology developments into clear strategic direction. He collaborates closely with senior executives to shape forward-looking decisions and drive measurable business impact.



Pranav Sahai | Analyst, Global Security and AI, Frost & Sullivan

Pranav Sahai is an **Analyst within Frost & Sullivan's Global Security and AI practice**, specializing in commercial public security and cybersecurity markets. His expertise spans AI across physical security, cybersecurity, identity security, robotics, drones, surveillance systems, and intelligent security operations, helping global clients evaluate emerging technologies and growth opportunities across the evolving security ecosystem.

He specializes in research, market intelligence, competitive strategy analysis, technology assessment, and identifying innovation-led growth opportunities across global security markets. Pranav also leads business intelligence and dashboard development initiatives for Frost & Sullivan's Growth Generator platform to enhance market visibility and strategic decision support

All rights reserved ©2026 Frost & Sullivan | www.frost.com

Ready to Lead the Transformation?

- **Schedule a Growth Strategy Dialog:** Align your growth roadmap with Frost & Sullivan's Visionary Growth Pipeline™ Dialog.
- **Engage with Growth Experts:** Co-design AI-enabled, data-driven operating models that scale industry-specific and commercial impact.
- **Showcase Your Transformational Leadership:** Position your organization as a transformation leader through Frost & Sullivan's Transformational Growth Leadership platform.
- **Join the Growth Council:** Collaborate with industry leaders shaping the future of your ecosystem.
- **Explore Best Practices Recognition:** Be recognized for excellence in growth strategy, execution, and customer impact.
- **Benchmark Your Industry Positioning on the Frost Radar™:** Benchmark your growth performance and innovation strength against industry competitors.
- **Tell Your Story:** Accelerate awareness, engagement, and revenue growth through integrated brand and demand generation strategies.



All rights reserved ©2026 Frost & Sullivan | www.frost.com

Appendix: AI-powered Cybersecurity Operations

Cybersecurity operations are evolving as AI accelerates attacks, increases alert volumes, and challenges traditional, manual approaches to threat detection and investigation. Organizations are moving toward integrated, AI-powered security operations that combine hyperautomation, agentic reasoning, and contextual intelligence to improve investigation, response, and operational efficiency.

To support this transformation, Frost & Sullivan provides forward-looking intelligence across:

- AI Usage for Cybersecurity Operations, 2026–2030
- OT Cybersecurity Solutions Market, Global, 2024-2030
- AI Usage in Security Operations, Global, 2025-2030

Together, these perspectives reinforce the key themes of this Transformational Growth Leadership discussion: advancing AI-driven security operations, balancing agentic autonomy with cost and human oversight, integrating security workflows, and enabling organizations to respond at machine speed as the threat landscape evolves.

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. →

FROST & SULLIVAN