FROST & SULLIVAN

TRANSFORMATIONAL GROWTH LEADERSHIP

Scaling Trust in Cybersecurity: How Sophos Is Redefining MDR, AI, and Cyber Leadership

An Exclusive Conversation Featuring

Joe Levy
Chief Executive Officer, Sophos

Adrian Drozd
Associate Partner, Frost & Sullivan

Lucas Ferreyra
Industry Principal, Cybersecurity Practice, Frost & Sullivan

As cyber threats accelerate in speed and sophistication, the cybersecurity industry is undergoing structural change. AI is reshaping both attack and defense. Managed detection and response (MDR) is scaling globally. And customers are demanding not just protection, but predictability and trust.

In this Transformational Growth Leadership conversation, Joe Levy, CEO of Sophos, speaks with Adrian Drozd and Lucas Ferreyra of Frost & Sullivan about the acquisition of Secureworks, the evolution of Managed Detection and Response (MDR), the scaling of cybersecurity leadership, and the transformative role of AI in shaping the next decade of cyber defense.

> “Can we scale cybersecurity leadership? I absolutely believe this is possible. Can we fundamentally change the way organizations operate so they can approximate the outcomes of world-class cybersecurity teams? I believe the answer is yes.”
>
> — Joe Levy, Chief Executive Officer, Sophos

Bringing Sophos and Secureworks Together

Lucas Ferreyra: *Joe, you brought together two of the most influential companies in cybersecurity. What drove the acquisition of Secureworks, and what has it meant for customers?*

Joe Levy: It was a very exciting moment for me personally. I have been in cybersecurity for nearly three decades, and both Sophos and Secureworks are venerable brands in this industry. When the opportunity arose, we evaluated it through one primary lens: how does this benefit customers?

That's what drives all our organic and inorganic growth. When we examined Secureworks more closely, we discovered that over the previous five years they had undergone a significant transformation. They were already pioneers in managed security services, but they had also built an impressive advisory services portfolio and an exceptional platform – **Taegis**.

Taegis stood out immediately. It delivered strong XDR (Extended Detection and Response) capabilities, next-generation SIEM (Security Information and Event Management) functionality, and ultimately supported managed XDR and MDR services. When we evaluated what combining platforms and practices would mean, we estimated it accelerated our roadmap by two to three years.

Equally important was cultural alignment. Cultural fit doesn't guarantee integration success, but lack of cultural fit almost guarantees failure. We saw strong alignment.

We have now passed the one-year mark. Integration is ahead of milestones. Products are fully integrated, and we are finalizing MDR service integration.

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.

Integration Philosophy: "Rip Off the Band-Aid"

Adrian Drozd: *You are well advanced in integration. What excites you most about full integration?*

Joe Levy: Our integration philosophy is simple: rip off the Band-Aid. Get as much done as quickly as possible, without causing harm.

We moved quickly to eliminate uncertainty. On day one, employees knew their roles. We integrated CRM (Customer Relationship Management) and ERP (Enterprise Resource Planning) systems early. The goal was to avoid an information vacuum. For customers, our message was clear: first, do no harm. I personally sponsor several Secureworks customers, and the first assurance we gave them was that nothing working for them would be disrupted.

We didn't force change. If a customer preferred Microsoft Defender or another EDR (Endpoint Detection and Response) product, that was fine. We would continue delivering excellent MDR. We expanded their options but didn't twist arms.

Secureworks customers were pleased to discover Sophos' broader portfolio, including next-gen firewalls, email security, Sophos Central, without being forced into changes.

Taegis as the Operational Bedrock

Lucas Ferreyra: ***Beyond Taegis, what other Secureworks assets were particularly valuable?***

Joe Levy: Taegis will become the bedrock of our XDR and MDR (Managed Detection and Response) operations. It is already operational within Sophos Central, and customers will experience continuity.

But Secureworks brought even more than Taegis. Their advisory services were outstanding; blue team, red team, purple team capabilities including incident response, penetration testing, application security, wireless security, and Active Directory testing.

They also brought Identity Threat Detection and Response (ITDR), built atop Taegis, combining practitioner experience with platform integration. When services and products are tightly looped together, you get precision and predictability for customers.

Other capabilities like iSensor will integrate with our network detection response. Vulnerability detection will merge with Managed Risk. Not every component survives in identical form, but every capability persists in some hybridized or standalone way.

Addressing a Cybersecurity Market Failure

Adrian Drozd: ***You recently announced another acquisition, Arco Cyber. What strategic gap does that address?***

Joe Levy: Arco Cyber strengthens our Governance, Risk, and Compliance capabilities. Their platform maps security controls to compliance regimes and simplifies resilience assessments. This ties directly to what I consider a longstanding market failure in cybersecurity.

There are three economic forces working against the industry:

1. **Information asymmetry** — buyers struggle to differentiate vendor claims. Everything sounds the same.
2. **Cyber leadership scarcity** — of roughly 359 million organizations globally, only about 32,000 have CISO-level leadership. That's fewer than one in 10,000.
3. **Cybersecurity poverty line** — most organizations cannot reliably produce good cybersecurity outcomes, regardless of budget.

Our goal is to scale cybersecurity leadership itself. That's where our upcoming CISO Advantage offering comes in, combining control measurement, risk quantification, compliance automation, and platform intelligence.

It's novel, needed, and only possible because of Sophos Central, Taegis, generative AI, and our global partner network.

Cultural Fusion: Service, Innovation, Entrepreneurship

Lucas Ferreyra: *You mentioned culture earlier. Have the two organizations blended successfully?*

Joe Levy: Yes, and there was no tissue rejection. Secureworks brought strong adversarial skills; hacker-oriented innovation, which complemented Sophos' threat intelligence and X-Ops capabilities.

Our cultural pillars are:

- A culture of service
- A culture of innovation
- A culture of entrepreneurship

We encourage risk-taking. But if you encourage risk and punish failure, innovation dies. We encourage graceful failure, which sustains innovation cycles.

The Evolution from Product to Platform + Service

Adrian Drozd: *You have been at Sophos for 11 years and CEO since 2024. What major shifts have you observed?*

Joe Levy: The first five years required a shift in risk appetite. We needed to take chances, enter new markets, and innovate beyond pure product.

Around 2018, we explored combining technology with services, specifically MDR, without harming our 25,000 channel partners. "First do no harm" applied here as well. Once we confirmed MDR would strengthen rather than compete with partners, we launched it. Initially Sophos-only, then vendor-agnostic. Secureworks accelerated that shift significantly.

Fundamentally, I believe the fusion of technology and services is the prevailing model for cybersecurity. It delivers predictability, and customers demand predictability.

AI: The Most Exciting Era in 30 Years

Adrian Drozd: *We've managed to avoid the AI topic so far but it's impossible to ignore. How central is AI to your path forward?*

Joe Levy: AI is transformational.

We have invested in AI for nearly 10 years. In 2017, we acquired Invincea, bringing deep learning for classification tasks. With transformer models, we saw a step-function improvement in detecting phishing and business email compromise.

Now, large language models are embedded within Sophos Central. Customers can use natural language queries instead of domain-specific syntax.

The latest frontier is agentic AI, embedding the intuition of a threat hunter into the platform. AI can pre-triage cases, enrich data, and even perform remediation autonomously, while keeping humans accountable in the loop.

We are at the point where many operations can be autonomous. The question is how to maintain customer comfort and accountability.

It's the most exciting time in my 30 years in cybersecurity.

Risk Appetite and AI Adoption

Adrian Drozd: *Are some industries more cautious about AI automation?*

Joe Levy: It's less about size or sector and more about risk appetite. Organizations operating in Operational Technology (OT) environments, for example, tend to be more risk-averse and for good reason. They may welcome the reaction-time benefits that AI provides but hesitate to allow autonomous change operations within their environments.

By contrast, organizations with higher risk tolerance are more willing to lean into automation. Ultimately, this cuts across verticals and geographies, it's about the operational risk characteristics of the organization rather than the industry itself.

The AI Arms Race

Lucas Ferreyra: *What transformative forces will shape cybersecurity over the next five years?*

Joe Levy: It's difficult to separate AI from everything else because it enables us to do things that previously might have been purely aspirational. We have already demonstrated the ability to scale managed detection and response, we now support 36,000 MDR customers out of 600,000 globally. The next act is scaling cybersecurity leadership itself.

Later this year, we're bringing Sophos CISO Advantage to market, an approach designed to democratize cybersecurity leadership and address what I have long considered a market failure in this industry.

At the same time, AI is accelerating attackers. What we're seeing is not a change in the novelty of attacks, it's an acceleration of the attack itself. Threat actors are using multiple AI platforms to automate full attack chains, from vulnerability enumeration to lateral movement.

It becomes a foot race. Who can get to the defect faster and who can fix it faster? Defenders must counter speed with speed.

Trust as Currency

Lucas Ferreyra: *In three words, how would you like Sophos to be perceived?*

Joe Levy: Most trustworthy brand.

Trust is the currency in cybersecurity. As supply chain dependencies become more complex and cascading failures more visible, a customer's ability to evaluate the trustworthiness of their vendors becomes increasingly important. Transparency, ultimately, will define the brands that are most successful.

Aspirational Goal: Democratizing Cybersecurity

Adrian Drozd: *What's your big five-year aspiration?*

Joe Levy: Addressing what I have described as a cybersecurity market failure. Can we democratize cybersecurity leadership and hygiene for hundreds of millions of organizations globally? Can we approximate the kind of outcomes that world-class organizations with world-class CISOs can expect for organizations that previously could only afford endpoint protection and a firewall? **I believe the answer is yes.**

A Message for the World

Adrian Drozd: *One final message?*

Joe Levy: We are about to live through some of the most interesting times in human history. For those who have been close to the advancements in AI, what's happening and what's about to happen is becoming clear. For others, it will become clear very soon.

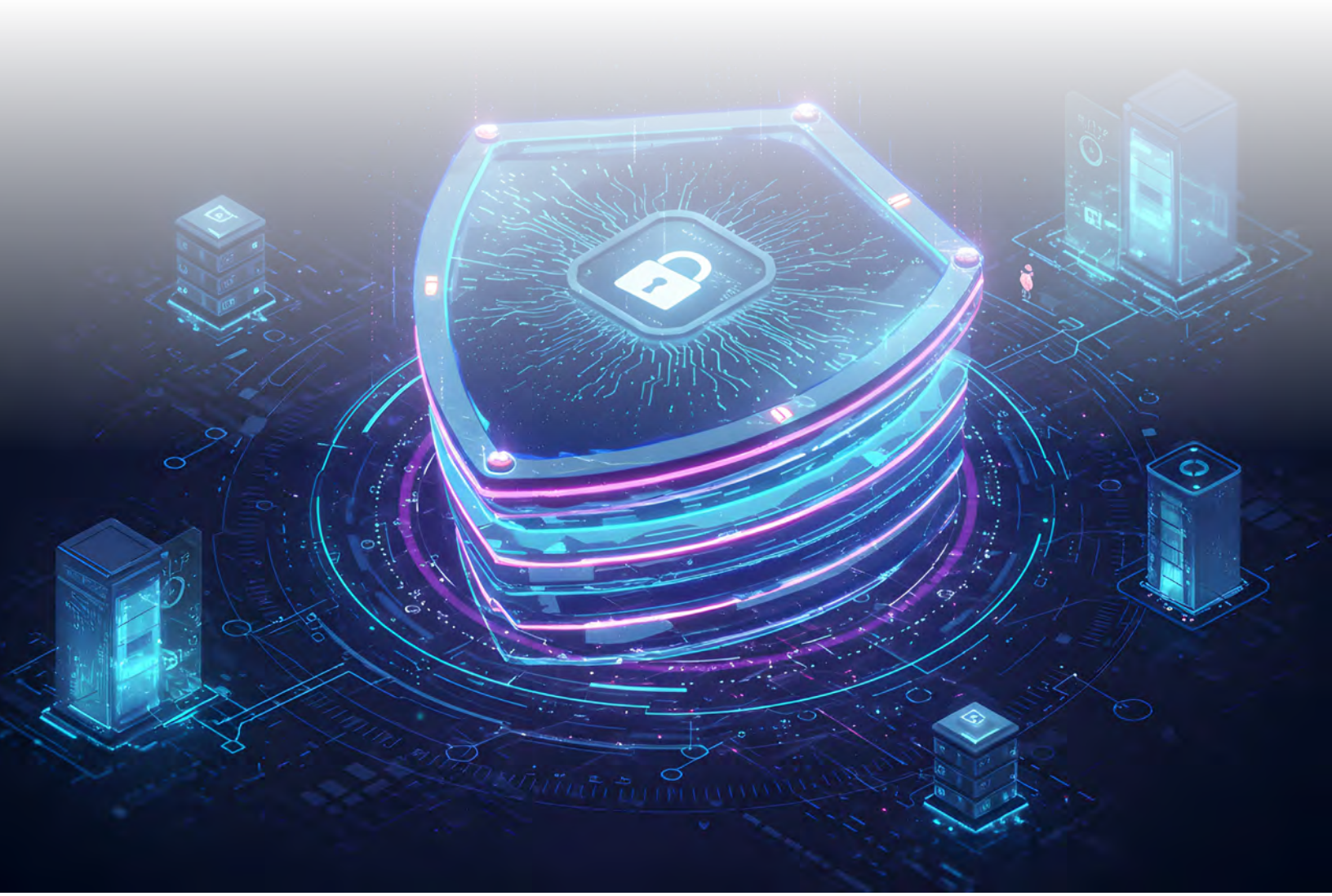
My personal emotional anchor through these times is a sense of optimism and wonder about what we are about to make happen. I would encourage everyone to try to hold onto that mindset over the next five years.

Closing Reflection

From integrating Secureworks to embedding AI across detection, response, and leadership layers, Sophos is redefining cybersecurity around predictability, scalability, and trust.

In a world where attackers move faster and uncertainty rises, the organizations that prevail will be those that scale both technology and leadership without sacrificing transparency.

For Joe Levy, the mission is clear: democratize cybersecurity, counter speed with speed, and above all, earn trust as the most trustworthy brand in the industry.



Joe Levy | **Chief Executive Officer,** Sophos

Joe Levy is the **Chief Executive Officer of Sophos**, a global leader in cybersecurity. A 30-year industry veteran, he combines deep technical expertise with strategic vision to advance how organizations defend against modern cyber threats. Since becoming CEO in 2024, he has expanded Sophos into one of the largest dedicated Managed Detection and Response (MDR) providers globally.

Previously serving as President and Chief Technology Officer, Joe unified Sophos' endpoint, network, cloud, and security operations capabilities under the Sophos Central platform. Earlier in his career, he held senior leadership roles at Solera Networks, Blue Coat Systems, and SonicWALL, helping shape innovations in next-generation firewalls and secure networking.

A recognized authority on agentic AI and cyber risk, Joe is a member of the Aspen U.S. Cybersecurity Group and serves on advisory councils across the security ecosystem.

Adrian Drozd | **Associate Partner,** 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.

Lucas Ferreyra | **Industry Principal, Cybersecurity Practice,** Frost & Sullivan

Lucas Ferreyra is an **Industry Principal in Frost & Sullivan's Cybersecurity practice**, leading research and strategic initiatives focused on MDR, XDR and security operations platforms, managed security services (MSS), and the evolution toward Autonomous Security Operations Centers (SOCs). With more than 12 years of experience across consulting, market research, and industry analysis, he supports cybersecurity and technology providers in refining growth strategies, strengthening market positioning, and translating complex security trends into actionable direction. Lucas collaborates across global teams on advisory and consulting engagements and regularly engages industry audiences through event speaking, executive briefings, and webinars with leading cybersecurity vendors.

Ready to Lead the Transformation?

- **Book a Growth Strategy Session:** 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.
- **Share Your Transformation Story:** 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.
- **Nominate for Best Practices Recognition:** Be recognized for excellence in growth strategy, execution, and customer impact.
- **Demonstrate Industry Positioning on the Frost Radar™:** Benchmark your growth performance and innovation strength against industry competitors.
- **Activate Brand & Demand Growth:** Accelerate awareness, engagement, and revenue growth through integrated brand and demand generation strategies.

Appendix: Scaling the Future of Cybersecurity Leadership

As cyber threats accelerate in scale and sophistication, organizations are seeking integrated cybersecurity partners that combine advanced platforms, expert services, and trusted advisory. AI-driven attacks, leadership shortages, and regulatory pressures are reshaping cyber resilience strategies. MDR, XDR, and AI-enabled security platforms are transforming security operations. Organizations are shifting from standalone tools to integrated security ecosystems. Frost & Sullivan provides forward-looking intelligence across cybersecurity platforms, managed services, and AI-driven security operations.

- Managed Detection and Response, Global
- Frost Radar™: Extended Detection and Response (XDR) Platforms
- Frost Radar™: OT Cybersecurity Solutions, 2025

Together, these analyses reinforce key themes explored in this Transformational Growth Leadership discussion, including the scaling of cybersecurity leadership, the convergence of platforms and services, and the growing role of AI in enabling faster, more predictable cyber defense.

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