FROST & SULLIVAN

TRANSFORMATIONAL GROWTH LEADERSHIP

A CEO Perspective

From Detection to Prevention: Reimagining Endpoint Security for the AI Era

Klaus Oestermann
Chief Executive Officer, IGEL
in conversation with
Jarad Carleton
Global Vice President of Research, Cybersecurity, Frost & Sullivan

Building the Foundation for a New Security Model

For years, enterprise cybersecurity has focused on detecting attacks after they occur. Today, that approach is being fundamentally challenged. The rapid growth of ransomware, hybrid work, cloud-native applications, and artificial intelligence has exposed the limitations of traditional endpoint security models, prompting organizations to rethink where security should begin.

At the same time, enterprise workspaces have evolved beyond the traditional desktop. Virtual desktops, DaaS, SaaS, enterprise applications, secure browsers, and operational technology (OT) environments now coexist within increasingly complex enterprise ecosystems.

In this Transformational Growth Leadership conversation, Klaus Oestermann, Chief Executive Officer of IGEL®, discusses why enterprises must rethink endpoint security from the operating system upward. He explains how prevention by design, immutable operating systems, Zero Trust architectures, and broad ecosystem integration are enabling organizations to strengthen security while improving resilience and operational flexibility.

> “The old model of building layer upon layer of security on top of Windows has declared bankruptcy. Organizations need a fundamentally different approach, one that starts with prevention.”
>
> — Klaus Oestermann, Chief Executive Officer, IGEL

From Endpoint Operating System to the Adaptive Secure Endpoint Platform™

Jarad Carleton: *Klaus, IGEL has undergone a remarkable transformation over the past few years. Looking back, what sparked the shift toward a preventative approach to endpoint security?*

Klaus Oestermann: If you look at our journey, IGEL has always had a strong heritage in endpoint operating systems. Over time, however, we saw organizations confronting a reality they could no longer ignore. Windows was no longer holding up as the security foundation enterprises expected.

At the same time, ransomware attacks were accelerating dramatically, with most compromises originating at the endpoint. Organizations responded by continuously adding more monitoring, detection, and remediation tools on top of existing operating systems. The industry became heavily invested in what I describe as a monitor, detect, mitigate, and remediate model.

Our view was different. Rather than continuing to build additional layers to an increasingly vulnerable foundation, we asked a more fundamental question: ***How do you prevent these attacks from happening in the first place?***

That thinking led us to build an immutable operating system. Because the operating system itself is designed to resist unauthorized changes, organizations can reduce their attack surface by up to 95%. From there, security becomes focused on intelligently integrating identity, endpoint management, and policy enforcement within a Zero Trust framework.

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.

That became the foundation of what we call our IGEL Preventative Security Model®. The name is intentionally descriptive because the objective is simple: to prevent attacks rather than respond after they've occurred.

Why Prevention Should Come Before Protection

Jarad Carleton: *You described an industry built around monitoring, detecting, and responding to attacks. Where do you think that model falls short, and why is prevention becoming so important?*

Klaus Oestermann: Traditional endpoint security has largely focused on protecting Windows by continuously adding more layers of monitoring, detection, and response technologies. The challenge is that the underlying operating system remains vulnerable.

We believed organizations needed a fundamentally different approach, one where security begins with the operating system itself.

An immutable operating system changes the security equation because it cannot be altered or compromised in the same way as traditional operating systems. Rather than assuming compromise will occur and planning how to detect and recover from it, organizations begin by significantly reducing the opportunity for compromise in the first place.

That philosophy becomes even more important as ransomware attacks continue to grow and organizations face increasingly sophisticated threats, including intellectual property theft. As AI becomes embedded across enterprises, protecting intellectual property, AI models, proprietary data, and other critical business assets at the endpoint becomes even more essential.

Our Preventative Security Model is built on that principle. Instead of accepting compromise as inevitable, security should focus first on preventing attacks before they succeed, while integrating identity, policy enforcement, and ecosystem partnerships into a broader Zero Trust architecture.

Hybrid Work and the Adaptive Secure Workspace

Jarad Carleton: ***As organizations embraced hybrid work, the traditional security perimeter began to disappear. How has that shift influenced the way IGEL approaches endpoint security?***

Klaus Oestermann: Hybrid work fundamentally changed enterprise security because organizations no longer control every connection between users and corporate resources. Employees now work from homes, airports, customer sites, and other remote locations, making traditional perimeter-based security insufficient.

Identity alone is no longer sufficient. Organizations must continuously evaluate three factors together: who the user is, what device they are using, and the context in which they are connecting. If any of those conditions change unexpectedly, security policies should respond immediately.

That's where contextual access becomes essential. By combining device identity, user personas, conditional access, and Secure Access Service Edge (SASE) policies, organizations can make far more intelligent decisions about granting access to enterprise resources.

At the same time, enterprise workspaces have become increasingly diverse. Applications now span virtual desktops, secure browsers, SaaS platforms, containers, and cloud-native services. Rather than treating these as separate technologies, we developed the Adaptive Secure Desktop® to provide users with a consistent experience while allowing IT teams to manage different application delivery models through a single secure platform.

As customers expanded into operational technology, that same platform also evolved to support both IT and OT environments through a common management framework, reinforcing our transition from an operating system provider to a secure workspace platform.

Prevention by Design: The Immutable Operating System

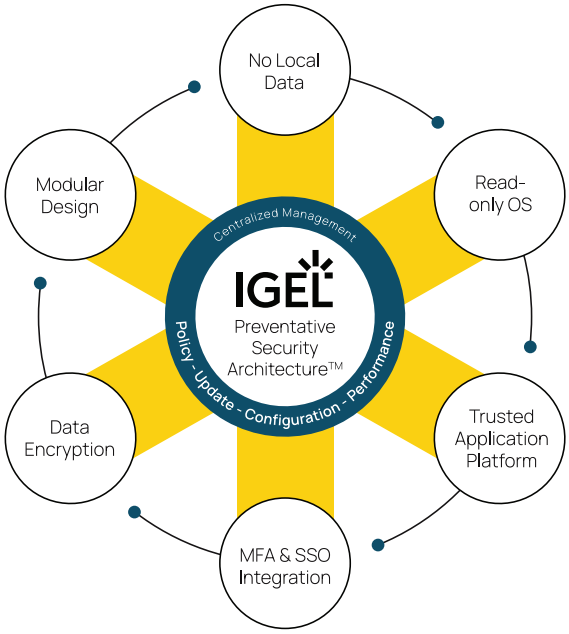
Jarad Carleton: *You keep coming back to the operating system as the foundation of security. Why is that such a critical starting point?*

Klaus Oestermann: Everything starts with the operating system. Traditional operating systems are designed to be modified. Software is installed, files are changed, configurations evolve, and over time those changes create opportunities for attackers.

Our approach is fundamentally different. An immutable operating system cannot be altered. It operates within a locked-down environment where unauthorized changes simply aren't possible. If something unexpected occurs, the system can immediately return to its original trusted state through a simple reboot.

That creates a completely different security philosophy. Rather than assuming compromise is inevitable, organizations begin with a secure foundation that dramatically reduces the opportunity for attacks. This is the foundation of our Preventative Security Model®, instead of continuously monitoring, detecting, and responding after something goes wrong, the operating system itself becomes the first layer of defense.

When combined with policy enforcement delivered through our ecosystem partners, organizations establish a security architecture that is simpler, more resilient, and fundamentally preventative rather than reactive.



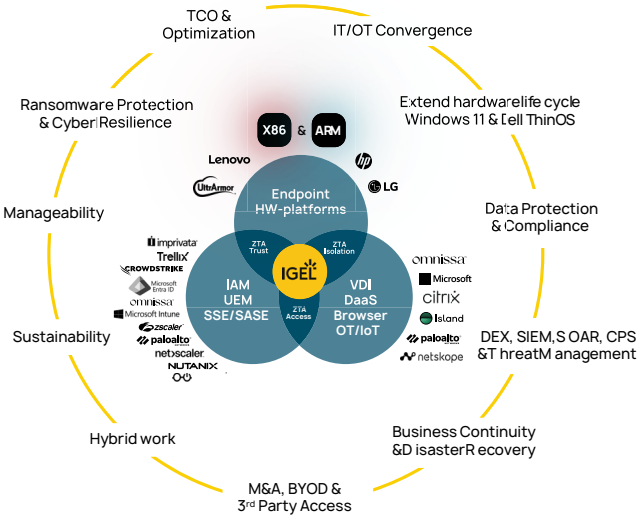
Zero Trust Through an Open Ecosystem

Jarad Carleton: *Prevention doesn't happen in isolation. How does the immutable operating system fit into a broader Zero Trust strategy?*

Klaus Oestermann: Zero Trust is not a product; it's an architectural framework. No single vendor delivers Zero Trust independently. Success comes from integrating multiple technologies that continuously verify users, devices, identities, applications, and data.

Our role is to provide the trusted endpoint that enables that broader architecture. That's why partnerships are central to our strategy. We work closely with more than 130 organizations, such as Cisco, Forescout, and other security providers, to integrate endpoint security with identity management, policy enforcement, compliance, secure browsers, virtual desktops, and secure access technologies.

Rather than replacing existing security investments, IGEL provides the secure foundation upon which customers can build the remaining pillars of their Zero Trust architecture. As threats continue to evolve, it's the ecosystem, not any single technology, that enables organizations to build a comprehensive security model.



Turning Market Disruption into Growth Opportunity

Jarad Carleton: *As the market begins to embrace this different approach to security, where do you see the strongest momentum and growth opportunities?*

Klaus Oestermann: Over the past several years, we have invested heavily in educating customers about a different approach to endpoint security. At the same time, the market has evolved in ways that reinforce that strategy.

The continued rise in ransomware attacks, the rapid adoption of artificial intelligence, and growing concern around protecting intellectual property have created what I describe as a perfect storm. Organizations increasingly recognize that traditional security models are no longer sufficient.

We've seen this most clearly in healthcare, financial services, and government. These sectors have realized they need a new security foundation, and increasingly that realization is being driven from the boardroom. Boards are asking CIOs, CISOs, and CTOs how they are strengthening enterprise security, moving cybersecurity from an IT initiative to a strategic business priority.

Historically, organizations didn't wake up wanting to replace their operating system. Today, many understand that implementing a new security model begins with establishing a different foundation.

Combined with our partner ecosystem and focused engagement across healthcare, banking, pharmaceuticals, retail, transportation, and government, we're seeing organizations actively seeking a preventative security platform rather than incremental improvements to legacy approaches.

Delivering Security, Resilience, and Business Value

Jarad Carleton: *Customers clearly invest in IGEL for security, but what business outcomes are they realizing once the platform is in place?*

Klaus Oestermann: Security validation is naturally the priority. Customers conduct extensive penetration testing to verify that the platform performs as intended, and it's encouraging to see those results consistently confirm the effectiveness of our approach. Those engagements also provide valuable feedback that helps us continue strengthening the platform.

Beyond security, organizations are seeing significant operational and financial benefits.

Across a study of approximately 140 customers, we found average total cost of ownership savings of 62%, with some organizations reporting savings above 80% and the highest approaching 92%.

Those savings come from extending hardware life, reducing software complexity, simplifying endpoint management, and lowering help desk requirements. Because the operating system is standardized and immutable, troubleshooting becomes much simpler, and organizations spend far less time managing endpoint issues.

Extending the lifecycle of existing hardware has also become increasingly valuable. As infrastructure costs continue to rise, many customers are choosing to extend the life of existing devices rather than accelerate expensive refresh cycles. By securely repurposing existing hardware, they reduce capital expenditure while gaining greater operational flexibility and additional cost savings.

The result is a combination of stronger security, simpler operations, and measurable financial value, an increasingly important outcome as organizations seek to maximize every technology investment.

Resilience Beyond Cybersecurity

Jarad Carleton: *One theme that stood out earlier in our conversation was resilience. You've expanded that idea well beyond cybersecurity. Tell us more about that.*

Klaus Oestermann: Business continuity became a natural extension of our security model. While we initially focused on preventing ransomware, customers quickly demonstrated that the same platform could help organizations recover rapidly from a wide range of disruptions.

Whether the challenge is a cyberattack, severe weather, infrastructure failure, or another operational event, the question is always the same: How quickly can employees resume secure operations?

Healthcare provides a good example. Regulations such as HIPAA require organizations to recover critical services within strict timeframes, yet rebuilding thousands of compromised Windows devices can take weeks.

Our approach is fundamentally different. Rather than rebuilding every endpoint, organizations can simply reboot into IGEL OS and resume secure operations almost immediately. Security and business continuity become part of the same architecture instead of separate technology initiatives.

That ability to recover quickly is becoming just as valuable as preventing attacks in the first place, making resilience a core element of modern endpoint security.

Simplifying the Modern Digital Workspace

Jarad Carleton: *You have explained why security is the foundation of what IGEL does. Beyond security, what does that mean for the day-to-day experience of your customers?*

Klaus Oestermann: Security is only part of the value proposition. Today's enterprise workspace spans virtual desktops, secure browsers, Desktop-as-a-Service (DaaS), SaaS (Software as a Service) applications, and cloud-native environments. Organizations need the flexibility to support these different application delivery models without increasing complexity.

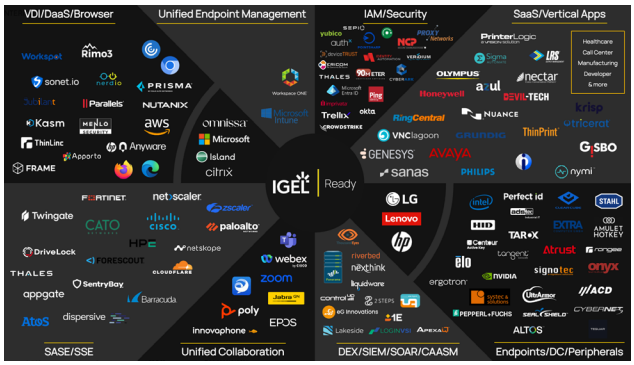
Our platform gives organizations the flexibility to move between those technologies without rebuilding the endpoint. New applications can be deployed based on user personas rather than device configurations, allowing organizations to adapt quickly as business requirements change.

That flexibility is especially valuable in environments such as contact centers, where employees may need to switch between different customer environments several times a day. Instead of rebuilding desktops, administrators simply apply a different persona and workspace configuration.

Customers also choose how they deploy IGEL. Some use it alongside Windows for business continuity and disaster recovery, while others replace Windows entirely and run IGEL as their primary operating system.

Regardless of the deployment model, the objective remains the same: deliver one secure, consistent workspace that gives users seamless access to applications while simplifying management for IT. Whether applications are delivered through virtual desktops, secure browsers, SaaS platforms, or containers, users experience a single Adaptive Secure Desktop® built on a secure foundation.

The same platform also extends into operational technology environments, enabling organizations to manage both IT and OT through a common management framework while reducing complexity across the enterprise.



Leading Transformation Through Platform Thinking

Jarad Carleton: ***Looking ahead, as IGEL enters its next phase of growth, where are you focusing your attention as CEO?***

Klaus Oestermann: As we continue to grow, our focus is on scaling the business while remaining true to the platform strategy that has defined our transformation. Product innovation remains important, but long-term success also depends on expanding our ecosystem and deepening our engagement across the industries we serve.

Healthcare, financial services, government, manufacturing, retail, and other regulated industries each face unique security and compliance requirements. Rather than taking a one-size-fits-all approach, we're continuing to build deeper industry expertise so we can address the specific challenges and use cases of each vertical.

Equally important is strengthening our partner ecosystem. Zero Trust and preventative security are delivered through collaboration, not by a single technology

provider. By continuing to expand our relationships with leading infrastructure, identity, and security partners, we enable customers to build comprehensive security architectures around a trusted endpoint.

Ultimately, our objective is to continue evolving IGEL as a secure workspace platform that helps organizations simplify endpoint security while adapting to the changing needs of modern enterprises.

AI Will Demand Security by Design

Jarad Carleton: ***We can't talk about the future of enterprise technology without talking about AI. How do you see it reshaping endpoint security over the next few years?***

Klaus Oestermann: AI represents both tremendous opportunity and significant responsibility. It has the potential to improve productivity, automate decision-making, and accelerate innovation across every industry.

At the same time, AI significantly increases the value of intellectual property and proprietary enterprise data. Organizations are investing heavily in AI models, research, and confidential business information, making those assets increasingly attractive targets for attackers.

That makes endpoint security even more critical. If organizations cannot protect the devices employees use to access AI systems and sensitive data, the risks increase dramatically.

The industry therefore needs to shift from assuming compromise is inevitable to building secure foundations that reduce the likelihood of compromise from the outset. Prevention, rather than detection alone, will become increasingly important as AI adoption accelerates.

AI will undoubtedly transform cybersecurity itself, but it also reinforces a principle that has guided our strategy from the beginning: security must be built into the foundation, not added after the fact.

Looking Ahead: The Next Generation of Enterprise Security

Looking ahead, Klaus believes enterprise security will continue moving toward simpler, more integrated, and more preventative architectures.

Rather than managing an ever-growing collection of independent security tools, organizations will increasingly look for platforms that combine secure endpoints, identity, policy enforcement, Zero Trust principles, and ecosystem integrations into a cohesive operating model.

For IGEL, that evolution is about enabling secure digital workspaces that protect users across increasingly complex IT and operational technology environments while giving organizations the flexibility to adapt as business needs change.

As enterprises continue to navigate AI, hybrid work, cloud transformation, and an increasingly sophisticated threat landscape, success will depend not only on detecting attacks but also on preventing them through secure foundations designed for resilience from the outset.

Closing Reflection: Building the Foundation for Preventative Security

Preventative Security represents more than the next evolution of endpoint protection. It reflects a fundamental shift from reacting to cyber threats to building resilient security architectures that reduce the opportunity for compromise from the outset. As AI adoption, hybrid work, and distributed enterprise environments continue to grow, organizations will need security strategies built on trusted endpoints, Zero Trust principles, and connected ecosystems.

For IGEL, the opportunity lies in helping organizations simplify endpoint security through immutable operating systems, intelligent policy enforcement, and an open partner ecosystem. Rather than adding layers of complexity, this approach strengthens resilience, improves operational efficiency, and enables secure digital workspaces.

As highlighted throughout the discussion, the future of endpoint security belongs to organizations that prioritize prevention by design, embrace ecosystem collaboration, and build secure foundations that are ready for the demands of the AI era.

About IGEL®

IGEL® is a global software company delivering the IGEL Adaptive Secure Endpoint Platform™, a trusted and governed endpoint platform for secure access to cloud, VDI, DaaS, SaaS, Secure Browsers, enterprise applications, as well as OT endpoints. At its foundation is IGEL OS, an immutable operating system that helps reduce endpoint attack surface, preserve a known-good endpoint state, and support secure access across distributed work environments. Through the IGEL Preventative Security Model®, the platform adds attested workload delivery, centralized governance, and contextual enforcement, aligning endpoint security with Zero Trust and SSE/SASE architectures from key IGEL Ready partners.

IGEL Business Continuity & Disaster Recovery™ (BC&DR) helps organizations restore secure access on Windows endpoints affected by ransomware, other cyberattacks, or outages. Founded in 2001, IGEL is headquartered in Germany with U.S. offices in San Francisco and Fort Lauderdale, and collaborates with an ecosystem of 130 leading technology brands. Learn more at www.igel.com.

Windows is a trademark of the Microsoft group of companies.

Klaus Oestermann | Chief Executive Officer, IGEL

Klaus Oestermann is **CEO of IGEL® and a technology executive** with more than 30 years of experience in cybersecurity, networking, cloud infrastructure, and enterprise software. Since joining IGEL in 2023, he has led the company's transformation into a leading secure endpoint OS platform, advancing a cybersecurity- and resilience-led strategy for IT and OT environments.

Prior to IGEL, Klaus was part of Citrix's executive leadership team, where he led the Networking and Security business. He is also an active Silicon Valley investor, advisor, and board member, supporting startups across cybersecurity, AI, cloud, infrastructure, IoT, and enterprise software.

Jarad Carleton | Global Vice President of Research, Cybersecurity, Frost & Sullivan

Jarad Carleton brings 25+ years of experience in the USA and Europe to his role. He works with organizations in Israel, North America, Europe, and Asia, focusing on various security domains such as Active Directory, zero-trust enterprise browsers, managed security services, digital risk protection, digital trust, IoT security and privacy, encrypted voice and text messaging, automated security validation, vulnerability management, IT/OT security convergence, fraud detection and prevention, and CSP security services. His quantitative research on security trends, maturity, services, and products informs legislators, regulatory bodies, and CXOs, helping them make data-driven decisions that enhance growth.

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.

Annexure: Advancing Preventative Endpoint Security

Enterprise security is entering a new era, driven by AI, hybrid work, and increasingly distributed IT environments. Organizations are shifting from reactive security models to prevention-first strategies that strengthen cyber resilience through secure endpoints, Zero Trust architectures, immutable operating systems, and connected security ecosystems.

To support organizations navigating this transformation, Frost & Sullivan provides forward-looking intelligence across endpoint security, Zero Trust architectures, AI-driven cybersecurity, secure digital workspaces, and enterprise resilience, including:

- Zero Trust Architecture: Next-Generation Cybersecurity Framework for Digital Enterprises
- Zero-Trust Browser Security Market, Global, 2025–2030
- Frost Radar™: Zero Trust Browser Security, 2025
- Endpoint Security Industry, Global, 2024–2028
- Frost Radar™: Endpoint Security, 2025

Together, these perspectives reinforce the central themes of this Transformational Growth Leadership discussion: building security from the endpoint upward, embracing prevention by design, and leveraging connected ecosystems to create resilient, AI-ready enterprise security architectures.

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