



converⁱnt[®]

Genetec[™]

2026 Technology Modernization Outlook

The Next Lap Forward



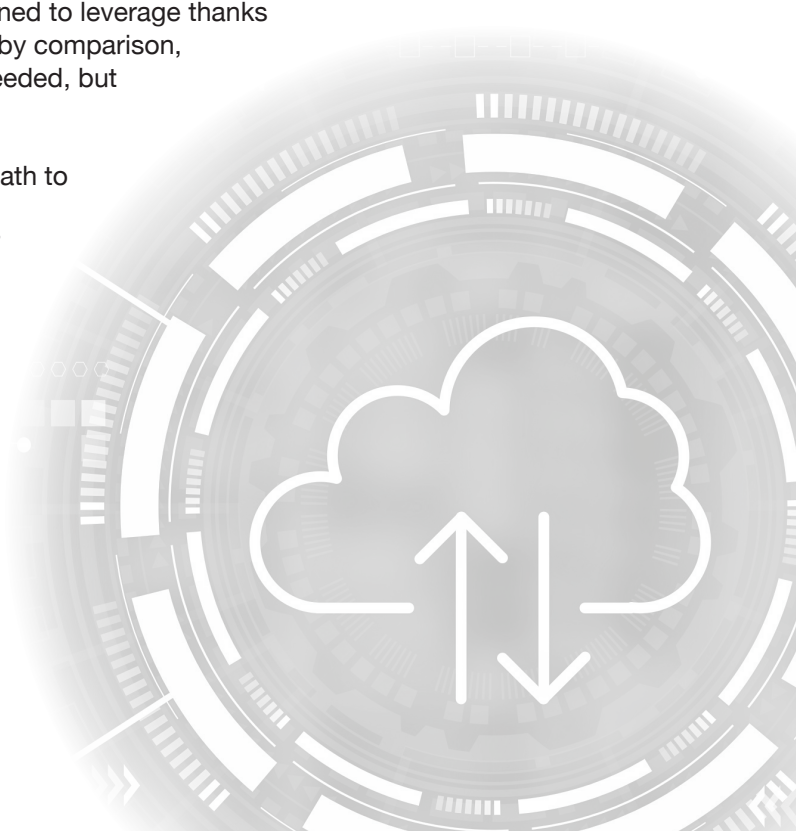


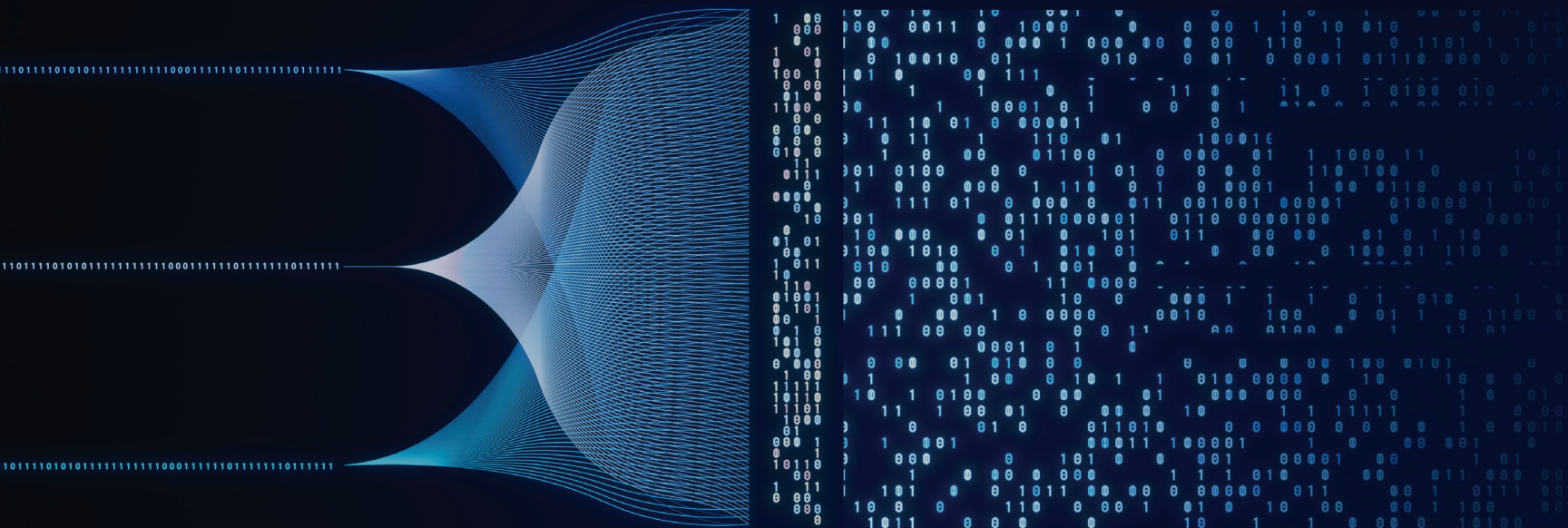
Why 2026 Will Be the Year of Modernization

When security leaders discuss challenges, they start with the volatility of today's threat landscape: real risks, real time, and the need to act decisively. Then they confront the drag of reality: legacy, siloed systems that don't connect, overextended teams across dozens of sites, and compliance chores that complicate even routine operations.

At the same time, they see powerful new capabilities arriving quickly; automation, AI, centralized operations, and platforms that deliver real-time intelligence across the enterprise. These are advances that other business functions, such as IT and operations, are already well positioned to leverage thanks to years of investment in modernization and cloud adoption. Security, by comparison, risks being left behind. The question is no longer if modernization is needed, but how quickly security organizations can act.

2026 marks the inflection point. Every enterprise now requires a clear path to technology modernization as the foundation for AI and intelligent automation. Without it, systems remain siloed, reactive, and ill-equipped for real-time threat detection, analysis, and mitigation. With IT mandates, regulatory requirements, and breakthrough technologies converging, 2026 is the year security must accelerate, transforming fragmented operations into unified, cloud-enabled intelligence ecosystems. The opportunities ahead are wide open, and the winners will be those who move now.





Interoperable Architecture Fuels Real-Time Intelligence

Enterprises weighed down by disparate legacy systems, sprawling hardware, and siloed operations across multiple sites and geographies face mounting pressure to modernize. Growth through acquisition and years of hardware investment have created fragmented environments that struggle to deliver real-time intelligence or scale to meet the demands of a rapidly evolving global threat landscape.

The path forward is clear: flexible architecture that integrates existing systems, unifies data flows, and establishes the foundation for automation and real-time threat detection. True AI outcomes - such as anomaly detection, natural language search, and predictive threat mitigation - require more than algorithms. They demand unified data streams, interoperability, and governance to ensure resilience and adaptability. Modernization does not require ripping and replacing entire infrastructures; instead, organizations can augment existing systems with new technologies that unlock needed capabilities, provided those systems are interoperable and able to evolve alongside IT standards.





The Tangible Results of Modernization

Modernization delivers measurable business value, transforming security from a fragmented cost center into a unified, intelligence-driven partner to the enterprise. Its impact can be seen across four critical dimensions:

- **Unified Security Intelligence** - Modern platforms enable real-time situational awareness across global sites, seamlessly integrating with HR, compliance, and facilities to elevate security into a strategic business partner. Consolidated “single-pane-of-glass” monitoring, supported by AI tools, shifts security operations from reactive alarm response to proactive prevention and coordinated action.
- **Flexible Deployment and Faster Realization of Capabilities** - Modernization doesn’t mean ripping and replacing overnight. Enterprises can retire legacy systems on their own schedule, extend the life of existing investments through SaaS and cloud-managed appliances, and unlock new capabilities without disruption. Flexible deployment models accelerate time to value, adapt dynamically to regulatory and operational shifts, and allow organizations to set modernization pacing that aligns to organizational priorities.
- **AI as the Accelerator** - With the right flexible, interoperable foundation, AI and intelligent automation extend what operators can achieve by streamlining investigations, enabling natural language search, and surfacing anomalies faster through sensor fusion. Intelligent automation reduces manual tasks and delivers richer, enterprise-wide insights, while responsible AI frameworks ensure humans remain in control. When supported by interoperable and open platforms, AI can drive resilience, agility, and measurable outcomes.
- **Lower Total Cost of Ownership** - Modernization replaces rigid capital refreshes with predictable OPEX models that scale with users, devices, and sites. Smarter staffing, licensing flexibility, and multi-year budget roadmaps aligned with IT strategy improve efficiency and financial planning while reducing operational overhead.

Modernization is not a single leap but a journey. It requires alignment with IT standards, a clear definition of desired capabilities, and a roadmap delivered one budget cycle at a time. With the right architecture and strategy, organizations can move from fragmented systems to cloud-enabled intelligence engines that power resilience, efficiency, and enterprise-wide value.

Cloud Native vs Legacy On-Premises



Cloud

On-Premises



Cost

Pay as You Go OpEx

Large Upfront CapEx
and Maintenance



Interoperability

Flexible and Scalable

Data Integration Barriers



Security

Automated, Actionable in
Real-Time

Rigid, In-House Protocols,
Complex Networking



Maintenance

Continuous Monitoring and
Automated Updates

Manual Updates and
Potential for Downtime



Accessibility

Remote Client and
Mobile Access

Limited Network, Slowed
Response, Siloed Work



The Road Ahead: Design a Phased Roadmap for 2026

To capture the full value of cloud migration, AI, and intelligent automation, enterprises should prepare in four critical areas:

- **Align Security with your Organization's IT Standards:** Ensure security strategy is integrated with IT's cloud and IoT roadmap and embrace interoperability and open standards to avoid new silos.
- **Define Capabilities to Unlock:** Identify the business outcomes you want to achieve beyond security, such as cross-departmental value in HR, facilities, compliance, and operations. Prioritize real-time threat intelligence and data-driven insights as core deliverables.
- **Build a Realistic Roadmap:** Treat modernization as a journey, not a rip-and-replace by designing a 3-5 year roadmap that outlines capability milestones, pilots, and expansion, delivered one budget cycle at a time. In addition, use road-mapping to move from "A to B" with clarity, illustrating how modernization unlocks tangible operational gains.
- **Evolve the Budget and Licensing Model:**
 - **Phased Modernization Reshapes Budgeting** - Modernization is best approached incrementally, one capability, one site, one cycle at a time. This phased approach not only reduces disruption but also drives a fundamental restructuring of how organizations plan and allocate budgets. Instead of large, infrequent capital expenditures tied to hardware refresh cycles, modernization enables predictable, flexible operating models that scale with business needs.
 - **The Shift from CAPEX to OPEX** - Legacy approaches have long relied on CAPEX-heavy refresh cycles, requiring major upfront investments every few years as systems reached end-of-life. By contrast, modernization introduces consumption-based OPEX models that flex with users, devices, and sites. This shift allows for greater financial agility, aligning spend with evolving requirements, and smoother forecasting through subscription and licensing structures. Workforce realignments reflect the needs of a cloud-first strategy.

The Bottom Line: Enterprises must view modernization as more than just updating technology. It is about building the right architecture, aligning with IT, and setting a roadmap that transforms fragmented security into a unified, cloud-enabled intelligence platform. Those who plan deliberately - one cycle, one capability, one win at a time - will move faster and extract far greater value than those who keep patching together outdated systems.



Crossing the Finish Line: From Security to Strategic Value

Enterprises don't want fragmented systems, they want one platform that works across every environment, without compromise. In 2026, modernization isn't optional; it is the foundation for real-time threat detection, unified visibility, and AI-powered intelligence. Those who align with IT, evolve their SOC, and embrace flexible, hybrid deployment will be best positioned to reduce complexity, unlock enterprise-wide insights, and accelerate their path to automation.

As modernization advances, the budget model itself becomes a strategic enabler transforming unpredictable capital spikes into flexible, recurring investments that drive long-term resilience and scalability.

Now is the time to assess where your organization stands, define the capabilities you want to unlock, and build a modernization roadmap. With **Genetec Security Center SaaS and Convergent as your partners**, you gain a trusted path forward, one that reduces sprawl today while preparing for the intelligent, resilient security operations of tomorrow.

Build the foundation for tomorrow's security. Begin your modernization roadmap today!

convergent®

Genetec™