ALLIED UNIVERSAL®

There for you.

Supporting Your Organization with Integrated Security Technology

8 Must-Haves for a Smarter Security Ecosystem

aus.com

Table of Contents

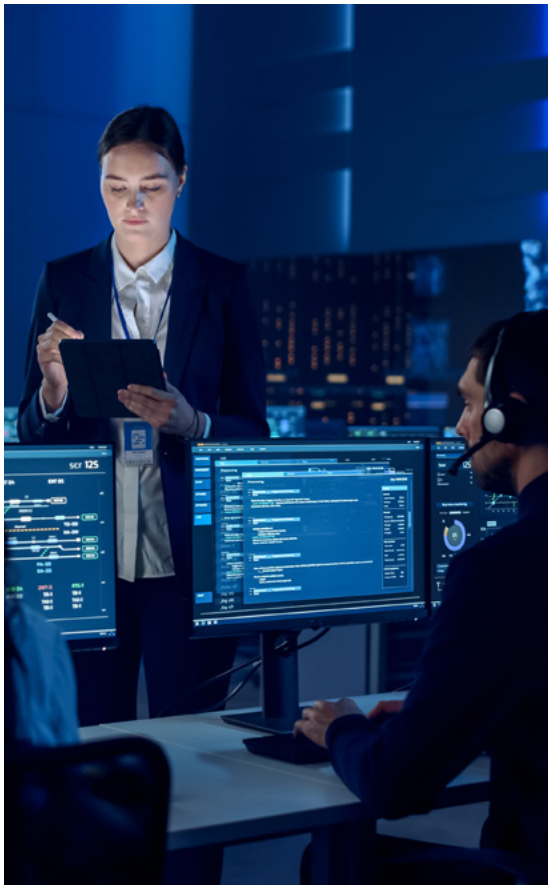
Introduction

Security today is not just about guards, card readers, and cameras. The threat landscapes and business risks are more complex, more coordinated, and more capable of disrupting operations, damaging assets, and eroding public trust.

For organizations that care about protecting physical assets, brand reputation, business continuity, and stakeholder confidence, security must evolve from isolated efforts into an intelligent, connected ecosystem.

A strong security ecosystem brings together people, technology, and expertise designed not only to help reduce risk, but also to advance business objectives and strengthen brand resilience. It is not about a single system, but how well the entire solution works together.

This guide outlines eight must-haves for building a security ecosystem that actively supports your organization's mission, adapts to changing risks, and strengthens brand resilience in an unpredictable world.



#1: Unified Strategy Across Technology & Physical Security

Many organizations still rely on fragmented security strategies where physical guarding and security technology operate in silos. This disconnect creates costly vulnerabilities that weaken the entire security posture.

Gap	Impact
Manual Workflows	Duplicated effort, human error, and inefficient resource use.
Outdated Monitoring Practices	Reduced situational awareness and delayed detection. High detection failure rate.
Siloed Teams and Operations	Missed information sharing and slower response coordination. Non-value added competition for budget.
Limited Cross-Functional Training	Inconsistent protocols, reliance on individuals instead of systems and workflow automation.
Disconnected Platforms	Inability to consolidate data or act quickly on real-time intelligence.

What This Means for Organizations

- Operational Inefficiency: Redundant tools and fragmented processes
- Heightened Vulnerability: Threats may bypass detection in systems that are unmonitored or lack integration.
- Delayed Incident Response: Inefficient communication and manual or poorly integrated workflows hinder timely resolution
- Missed Insights: Real-time analytics and automation cannot function without integration

Why Integration Matters

Building a smart, scalable security ecosystem starts with closing these gaps. When systems, people, and processes are aligned, organizations benefit from:

- Improved coordination and coverage
- Reduced inefficiencies and downtime
- Stronger resilience across evolving threats
- Greater reputation protection amid uncertainty

#2: A Seamless Security Model Combining People, Technology, and Expertise

Security becomes more effective when it operates as one connected system. A seamless model, or integrated security solution, brings together people, technology, and expert processes to deliver consistent coverage, better communication, and faster response across all touchpoints.

What This Approach Can Include

- 24/7 monitoring and coordinated response through Global Security Operations Centers (GSOCs)
- AI-enabled video surveillance for proactive threat identification
- Access control systems with biometric authentication and centralized visibility
- Emergency communication tools that improve coordination and accelerate response
- Technology-supported staff with access to alerts and security information

Why Seamless Security Elevates Outcomes

- Improves coordination between teams, systems, and protocols
- Enhances responsiveness and reduces duplicated efforts
- Helps maximize the return on both human and technology investments

This unified structure supports operational alignment, reduces redundancies, and helps ensures that everyone from frontline system operators to remote analysts are working from the same playbook.

#3: A Security Program That Powers Business Performance

When implemented strategically, security becomes a powerful performance driver. A thoughtfully designed program not only helps to mitigate risk, but it also optimizes operations, safeguards revenue, and supports long-term business success.

A high-performing security program is proactive, data-informed, and aligned with the organization's mission. It goes beyond traditional guard posts and static systems by becoming a living part of daily operations that is adaptable, resilient, and built to scale.

What Sets a Performance-Driven Security Program Apart

- Operational Alignment: Security processes are tailored to support business workflows, not interrupt them.
- Risk-to-Outcome Translation: Threats are prioritized based on how they impact business continuity, customer trust, and revenue protection.
- Efficiency through Integration: Reduces duplicated effort and improves response by aligning people, processes, and platforms.
- Measurable Impact: Security investments are evaluated based on their contribution to uptime, compliance, and stakeholder confidence.

How to Activate Security as a Performance Driver

Taking the following steps will help ensure that security is not only a reactive activity, but also a powerful, adaptive value generator that drives business performance.

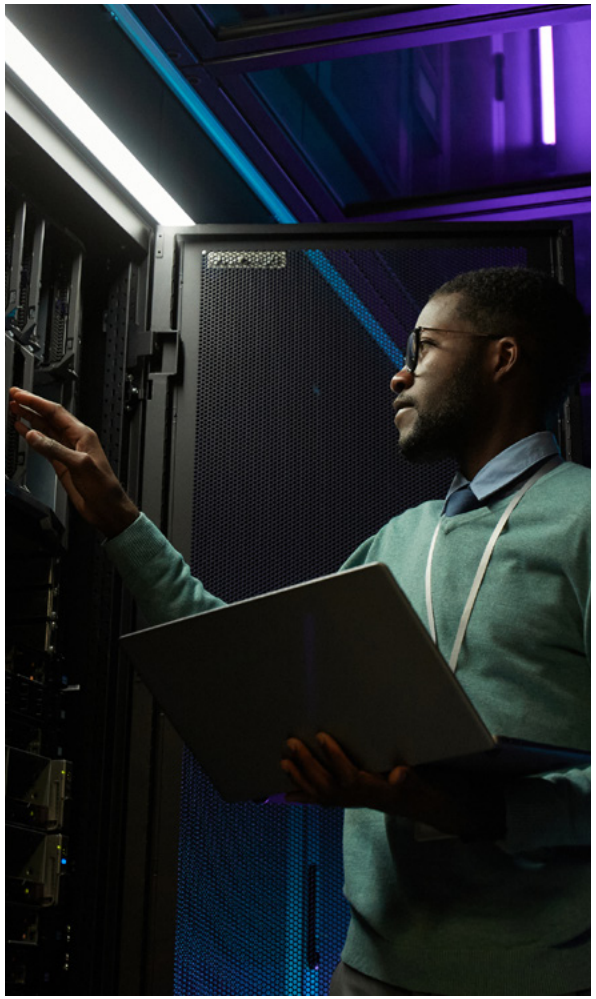
Tie Security Metrics to Business KPIs

Track how your program reduces downtime, improves compliance rates, or supports employee safety—metrics that matter to leadership.

- **Design for Agility**
  Make sure your program can adapt as your operations scale, risks evolve, or technology advances.
- **Embed Security in Strategic Planning**
  Security leaders should be involved in annual business planning and cross-functional initiatives to increase alignment and early risk mitigation.
- **Demonstrate Business Value**
  Tie security decisions to operational improvements, revenue growth, improved customer experience, compliance, innovation, or increased productivity. Further illustrate value by using real-world examples with tools like dashboards, reports, and case studies.

Why This Matters

Gone are the days of people paying for guards and security systems just to help keep people and assets safe. Customers want guards and systems to also improve business processes. It's important to not only create a more secure environment, but to also use security to reduce operating expenses, improve core business operations, and optimize customer / employee experiences.



#4: Checklist of Key Assets to Safeguard

A smart security ecosystem begins with knowing what you are securing. Use this checklist to identify and prioritize the critical assets that your security strategy should cover, from people and infrastructure to data and brand reputation.

Physical Infrastructure

- ❑ Buildings – Offices, data centers, warehouses, and other facilities with perimeter access points
- ❑ Equipment – Proprietary machinery, servers, tools, and critical infrastructure
- ❑ Materials – High-value raw materials or regulated substances on-site
- ❑ Product or Service – Goods, services, or software that are in production or delivery stages.

People & Personnel

- ❑ Key Personnel – Executives, researchers, and individuals with privileged access or institutional knowledge
- ❑ Employees – General workforce, especially those in high-traffic or sensitive areas
- ❑ Contractors – On-site vendors, technicians, or third-party service providers
- ❑ Visitors – Guests, partners, and delivery personnel requiring secure access and monitoring

Information

- ❑ Intellectual Property – Proprietary designs, processes, patents, and trade secrets
- ❑ Client Data – Customer records, contact information, and communications
- ❑ Business Data – Financials, contracts, operational plans, and internal reporting
- ❑ Product Data – Technical specifications, manufacturing instructions, and supply chain records

Ask Yourself

- ❑ What incidents could compromise our brand?
- ❑ Do we understand how physical and digital threats are connected?
- ❑ Are there assets or vulnerabilities we have overlooked?

Knowing what matters most is the first step toward building a security ecosystem that helps protect your people, operations, and brand.

#5: Scalable Technology for Stronger Security

Technology plays a critical role in helping organizations detect threats earlier, respond faster, and manage resources more effectively. But not all tools deliver equal value. The right technology should not just be integrated, scalable, and aligned with your security goals.

A strong technology foundation multiplies the impact of your security team and supports more consistent, informed decision-making across locations.

Core Technologies That Power a Security Ecosystem

- Cloud-based access control and identity management for centralized oversight
- Intrusion detection and emergency notification systems to increase awareness and shorten response times
- GSOC as a Service and remote monitoring to extend visibility without requiring full in-house infrastructure
- AI-enabled video analytics to identify threats before they escalate

These tools function as strategic extensions of your security team, enabling smarter coverage with fewer blind spots.

What Scalable Technology Makes Possible

- Centralized oversight of multi-site operations without redundant infrastructure
- Faster, more consistent incident response through integrated monitoring
- Flexible expansion of coverage and services as the organization grows

#6: Data-Driven Insights for Smarter Security Decisions

Modern security technologies generate a constant stream of data from access logs and video feeds to alarm triggers and incident reports. When used strategically, this information can move your organization from reactive decision-making to a more proactive, informed approach, improving response times and mitigating risk.

Too often, valuable insights remain siloed or underutilized. By connecting, automating, and analyzing systems, people, and processes, organizations can uncover risks, monitor performance, and make faster, smarter decisions that support both daily operations and long-term goals.

Impactful Security Data Insights

- Visibility into access trends, incident frequency, and emerging risks
- Benchmarking across teams, facilities, and time periods
- Faster, more accurate incident response through centralized reporting
- Continuous improvement through historical analysis and trend identification

Why Data-Driven Security Insights Make a Difference

- Supports timely, evidence-based responses to security events
- Helps identify operational blind spots before they escalate
- Provides a foundation for continuously improving your program

Data does not replace experience, it enhances it. When teams can visualize performance, detect patterns, and act on what the data reveals, they are better equipped to help protect people, assets, and brand reputation.

#7: Maturity Targets Using a Security Ecosystem Scorecard

Use this weighted scorecard to assess your organization's readiness across three key dimensions of future-focused security: Scalability, Resilience, and Innovation. Assign a score from 1 (Not in Place) to 5 (Fully Implemented) for each item. Multiply each score by the assigned weight to calculate your total.

Scoring Guidance

1 – Not considered 2 – In early planning 3 – Partially implemented 4 – Mostly implemented 5 – Fully implemented across all relevant areas

Category	Assessment Area	Your Score (1–5)	Weight	Weighted Score
Scalability & Adaptability	Technology scales with business growth or geographic expansion		3	
	Hosted or managed services reduce internal infrastructure burden		2	
	Tech refreshes and upgrade planning is built into our roadmap		2	
Resilience & Redundancy	Backup power and communication failover systems are in place		3	
	Monitoring is geographically redundant (on-site + remote)		3	
	Business continuity plans cover outages and disasters		2	
Innovation & Automation	Robotics or autonomous devices are part of our future planning		2	
	AI/predictive analytics support early threat detection		3	
	Emerging threats are formally reviewed in annual risk assessments		2	

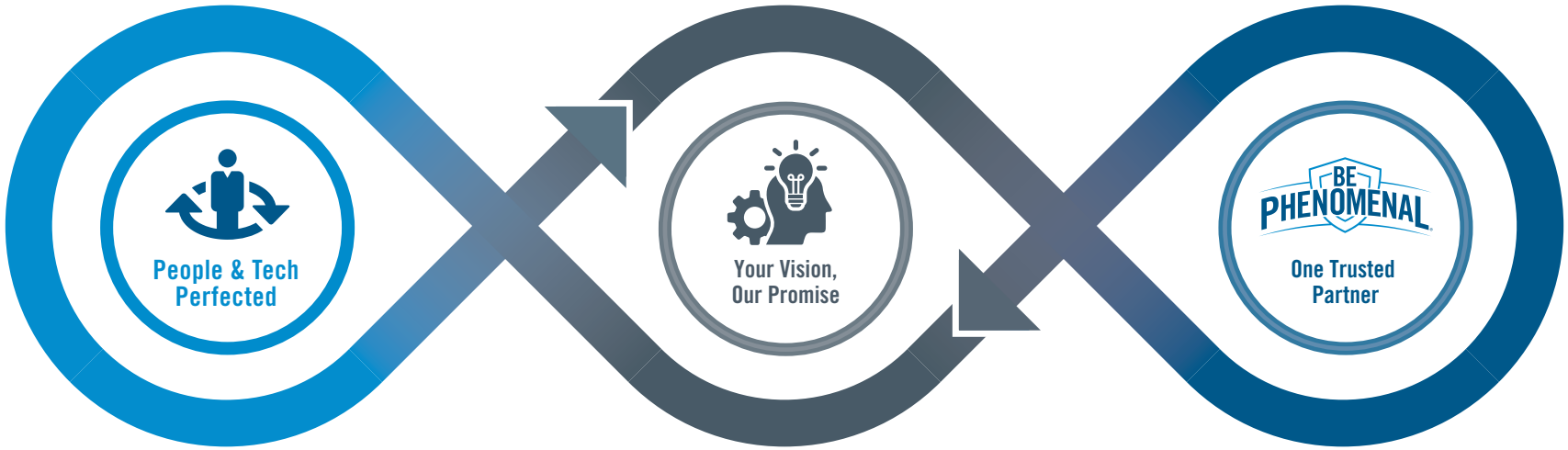
The combined weighted score will indicate your organization's readiness.

#8: The Right Partner to Power Your Security Ecosystem

Building a strong security ecosystem requires more than tools and talent. It takes a partner with the experience and scale to connect people, technology, and expertise into one cohesive solution. As threats evolve and operational demands increase, choosing the right security partner becomes critical to long-term protection, continuity, and performance.

Allied Universal takes a business-first approach to security. We start by understanding each client's core operations, risk priorities, and long-term objectives. From there, we design security programs that align with those goals while driving process improvements and measurable results. Our deep expertise across guarding, technology, and integration allows us to recommend the best-fit solutions for any environment.

We do not just deliver services; we build business outcomes. Whether it is reducing complexity, improving coordination, or scaling across multiple sites, we help clients elevate security in ways that support the broader business. Because we offer both guarding and technology, organizations are able to experience a streamlined, frictionless approach through a single, fully aligned partner.



What Sets Allied Universal Apart

- A global network of 800,000+ trained security professionals and technology experts
- Full lifecycle support from risk assessment and planning to implementation and optimization
- Scalable programs customized to each client's risk profile and operational maturity
- Trusted experience securing critical infrastructure, including government, defense, and energy sectors
- Integrated guarding and security technology solutions that deliver measurable return on investment

With global reach and a proven history, Allied Universal brings the scale and adaptability needed to support evolving security needs. Whether you are modernizing an individual location or reimagining enterprise-wide protection, we deliver security strategies that are built to last and structured around your business.

Conclusion

Today's security environment requires more than just reacting to threats; it demands foresight, coordination, and adaptability. Organizations that integrate people, technology, and expertise into a unified ecosystem are better positioned to manage risk, help protect critical assets, and support business continuity.

The most effective security programs are built on alignment — not only between systems, but across strategy, operations, and partnerships. From assessment and engineering to monitoring and ongoing maintenance, security should function as a connected, evolving solution that grows with your organization.

We do not just deliver services, we support your entire security lifecycle with solutions tailored to your goals. Whether you are safeguarding a single facility or managing complex, multi-site operations, our team is ready to help you build a smarter, stronger security program.

Take The Next Step

- Start a customized security consultation request with Allied Universal
- Schedule a visit to our Customer Experience Center (CEC) to see modern security operations in action.
- Request a Risk360® review to identify and prioritize vulnerabilities
- Explore a HELIAUS® demo to see how AI-driven insights can enhance security performance

Learn more about Allied Universal Integrated Technology Services
https://www.aus.com/security-services/integrated-technology-services

ALLIED UNIVERSAL®
There for you.

Supporting Your Organization with Integrated Security Technology

Learn more about Allied Universal by visiting our website - aus.com - and exploring additional resources, tools, and insights.

- Guarding
- Integrated Technology
- Risk and Vulnerability Consulting
- Canine Security
- Executive Protection and Intelligence
- Active Law Enforcement
- Weapons and Explosive Screening
- Event Security
- Investigations
- Disaster and Emergency Response
- Electronic Monitoring
- Cash Solutions
- Workforce Solutions
- Janitorial Services

There's Security in our Solutions®