ALERTENTERPRISE

WHITEPAPER

CYBER-PHYSICAL SECURITY CONVERGENCE:

THE DISRUPTIVE APPROACH TO TODAY'S THREAT LANDSCAPE

The digital transformation couldn't come at a better time for physical security. It ushers in an era of true convergence – where connecting cyber/IT, security and OT data across the enterprise leads to heighted situational intelligence, reduced risk and the integration of critical business processes.

Digital Disruption Transforms Traditional Metrics

Today's digital transformation means limitless opportunity for those who can harness the digitization of our physical world safely and effectively. But the transformation has forever altered the threat landscape, leaving no entity without risk. Cyber and physical threats have blended, the result of our new everything IP-connected environment. The growing internet of Things (IoT), with billions of connected devices predicted in the coming years, is further driving an exponential explosion of cyber-physical risk. Smart cities, autonomous vehicles, drones and robotics are the next inflection point. Any system compromised can have a devastating impact on security, critical operations, profitability and reputation.

Thought leaders agree that the current approach of dealing with security in departmental silos is leading to increased risk, rising costs and a climate of mistrust on the part of regulators, who remain frustrated with recurring breaches. So what are the barriers and what will it take to break them down?

According to *The State of Security Convergence in the United States, Europe and India*, an ASIS Foundation Convergence Report published in 2019, organizations are often slow to adapt to change unless forced to do so. "Reluctance to converge often centers around people issues," the report stated. Physical security, IT and OT personnel are fixed in traditional silo structures, hesitant that convergence will translate into changes that require them to diminish their roles. Yet malicious actors don't think this way and ultimately capitalize on these functions working in isolation from each other. Later in this article, we will discuss how security convergence is not designed to eliminate roles, jobs or departments, but to strengthen their ability to secure the enterprise and enhance workforce experience with automation, integration and data-insights.

> *"Explosive growth in technology and data over the next decade will obliterate barriers between cyber, physical and virtual worlds, ratcheting up the complexity and scale of cyber and privacy risk management worldwide. Digital data and devices will be increasingly embedded in critical infrastructure, consumer products, vehicles, daily life and even in humans, in a world in which the physical, cyber and virtual merge."*
>
> – U.S. National Security Telecommunications Advisory Committee

FACTORS LEADING TO CONVERGENCE

38% Better alignment of security/ risk management strategy with corporate goals

28% Advances in technology integraton/ security operations centers

38% Greater efficiency in security and/ or business continuity operations

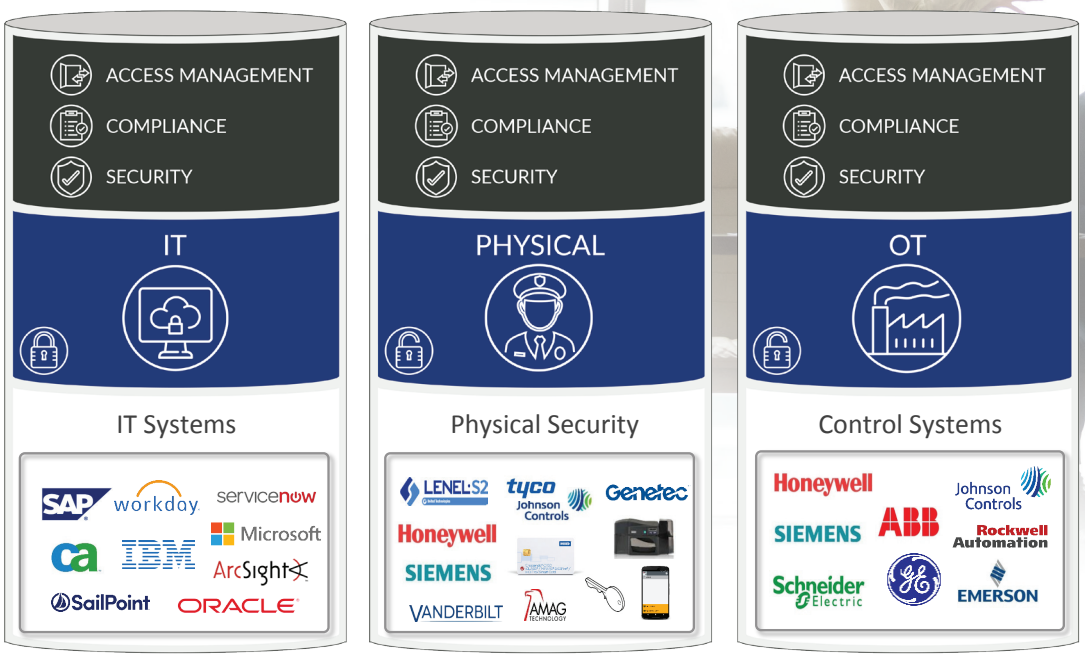
38% Clear cost savings

2019 Security Convergence Report, ASIS Foundation

Trusted and True Security Convergence

Security is long overdue for the digital transformation and the altered threat landscape requires a change to conventional thinking and a new approach. The industry continues to come face to face with the reality that millions of dollars are being spent on halfway security measures, while breaches continue unabated and threat vectors rise. Current spending on regulatory compliance and network security too often miss a structural vulnerability: security is still imprisoned in corporate silos and needs to break free.

Cyber|IT security personnel focus on virus and malware attacks, hacker penetration of network perimeters and employee access and authorization. Corporate security personnel focus on physical access to buildings, zones and remote facilities and often, environmental systems. Operators of critical assets like pipelines, power generation, chemical plants and airports focus on control systems and whether assets are functioning within established parameters. The monitoring systems for these functions are rarely integrated and even more rarely correlated for contextual understanding of an evolving security event. Everyone is isolated. It is the very definition of halfway security and corporate irresponsibility.

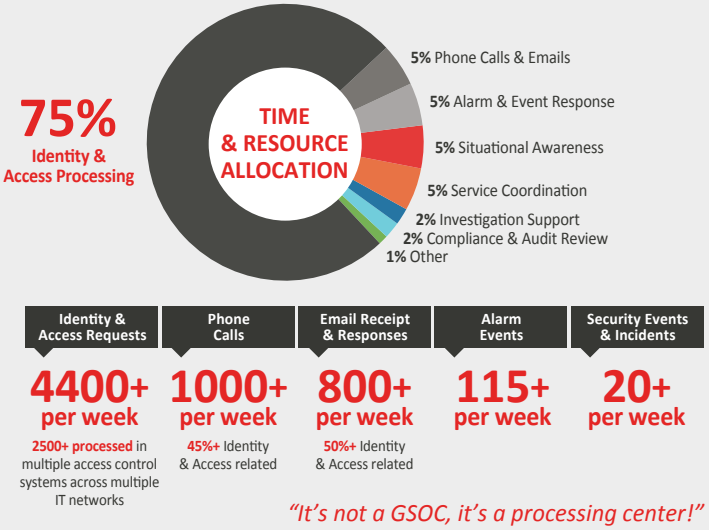


Determined attackers have a more holistic view of security. They attack the entire enterprise and understand the vulnerabilities present in security. Segregation of solutions within the enterprise means each silo is real-time blind to breaches in the others. Communication gaps between silos mean time delays, which open opportunities for attackers. The failure to integrate physical security with IT and operational technology – regardless of budget – is the moral equivalent of aiding and abetting thieves and saboteurs.

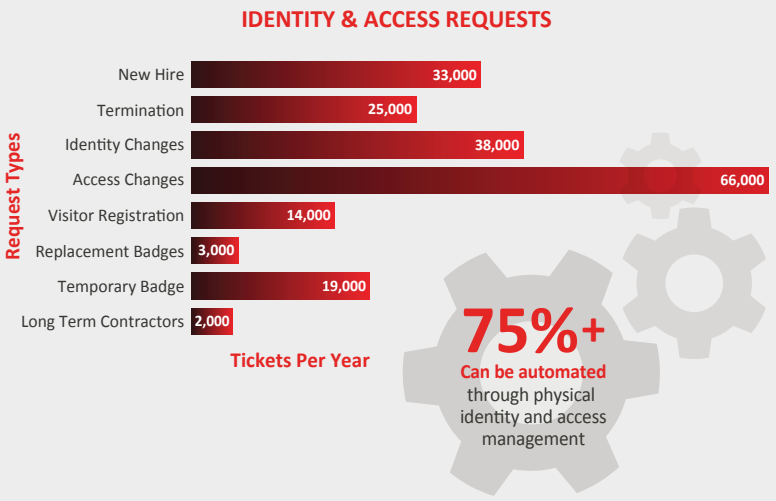
Enterprise security leaders now understand that the effects of a cyber breach, physical attack or manufacturing loss, which include business and reputational costs, far outweigh the costs of a holistic and converged system. Those who embrace the digital transformation will enable cohesiveness of systems and data, with the end result delivering proactive threat detection and prevention— a unified threat response to mitigate risk.

For a Fortune 100 diversified, multi-national healthcare enterprise with 20,000+ employees/ contractors, security across its 500+ corporate remote locations was anything but integrated or cohesive. In fact, without a coordinated approach, some 75% of its time and resource allocation was spent processing non-automated access and identity requests each week – and only 5% on actual situational awareness, risk management and threat assessment. Implementing a unified approach that converged and automated physical security with IT and OT, the user was able to substantially minimize risk while increasing compliance and reducing operational costs.

GSOC BEFORE AUTOMATION | BY THE NUMBERS



"It's not a GSOC, it's a processing center!"



The Intelligent Enterprise Needs Intelligent Security

Tectonic Shift to Collaboration of Data: Departments like Corporate Security and Plant Operations at one time had little or no need to collaborate with IT. The well-seeded approach of dealing with security in departmental silos no longer holds value in a digitized society. Formerly a cost center only, physical security now has the attention of C-Suite and IT executives, as predictive risk analytics and insider threat monitoring of physical-logical systems are closing gaps, linking formerly security only data to daily tasks, resulting in lower total cost of ownership, heightened operational efficiency and a solid return on investment from integrated solutions.

Business leaders are clear-eyed about new risks tied to emerging technologies, according to PwC's 2018 *Global State of Information Security*® Survey (GSISS). GSISS respondents recognize that a successful cyberattack on OT could have major consequences, including the disruption of operations, compromise of sensitive data and damage to product quality.

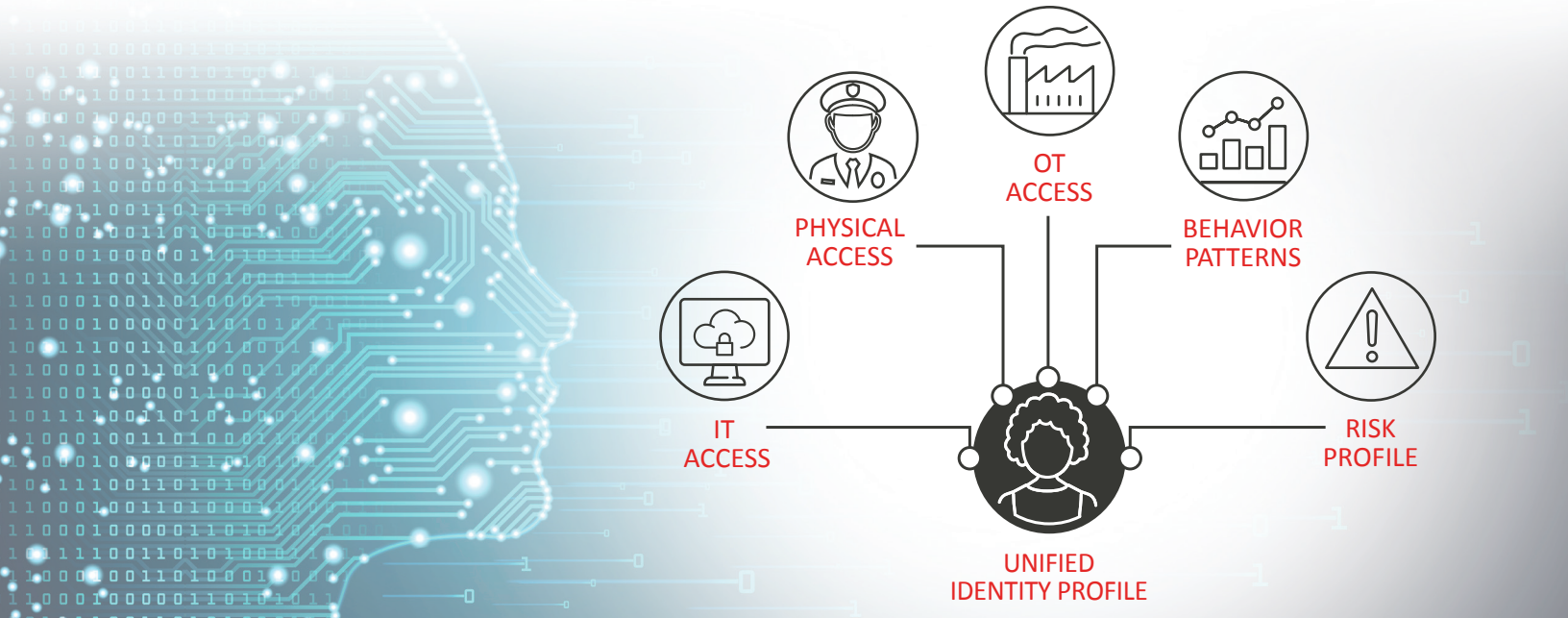
Facing these new and emerging threats requires intelligent platforms that can effectively converge applications and leverage big data, machine learning and predictive analytics to seamlessly aggregate and analyze data across OT, IT and physical security.

The Unavoidable Human Side of Security

At the center of converged security is people, identity and trust. For example, do you know who is handling your critical infrastructure operations? It may seem like a simple question, but in real-life this is a question that needs to be asked or a control that needs to be tested with every event and credentialing or identity transaction every minute of every day.

Consider the worker who is able to log into Utility or Energy enterprise operational systems despite having followed someone into the building without swiping his own access card. This may be an innocent occurrence when seen as an isolated event. However, when correlated with HR data, staff schedules and system transactions, it may reveal something much more sinister. Was he scheduled to be on duty? Was he supposed to be on vacation? Was he on disciplinary probation? Was he altering system configurations? Disabling alerts? Was he attempting to access systems he was not authorized to engage? Logging into operational systems without first using badge access should trigger automated checks to answer these questions and alert security to investigate a physical breach – innocent or not.

With a converged security technology platform and a single unified view of cyber, physical and operational parameters, the Security Operations Center (SOC) can now deliver a unified and proactive threat response to a wide range of incidents – with real-time data connection across HR, physical security and other critical enterprise applications.



Insider Threat Protection 2.0

AI-powered Workforce and Workspace Intelligence is the next journey on the road to security convergence. It offers powerful identity and business benefits, including:

- *A clear, converged connection of AI-powered Security, Operational and Experience data for enhanced insider threat protection.*
- *The ability to leverage security, HR and operational data to deliver essential space utilization and optimization insights and to enterprise facility and corporate real estate.*

According to the ASIS Foundation Convergence Report, almost 80% of non-converged organizations acknowledge that convergence would strengthen their overall security function.

The security industry has an incredible opportunity to lead the digital transformation – starting now.

Convergence Today. Convergence Tomorrow.

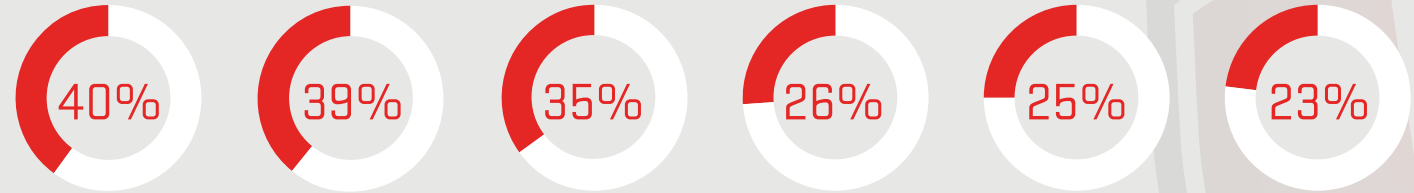
The technology to accomplish real-time, cross-enterprise security convergence is an operation in mission critical environments today. It is not designed to eliminate roles, jobs or departments, but to strengthen their ability to secure the enterprise and enhance workforce experience with automation, integration and data-insights. AlertEnterprise delivers a holistic security convergence platform that can integrate, analyze and correlate data across thousands of systems and applications to expose risks and deliver more informed and actionable situational intelligence in real-time. This eliminates both the vulnerabilities and inefficiencies of managing security and risk in silos. It enables fast and informed responses to IT, physical and operational threats, thereby reducing cost and liability while increasing safety and reliability.

The AlertEnterprise technology platform integrates seamlessly with enterprise applications including HR systems to conduct risk analysis on an ongoing basis and automate the onboarding and offboarding process. Insider threats and hostile intrusions are managed by integrating across multiple card access systems, video surveillance systems and sensor networks. This enables monitoring of employee, contractor and visitor access to critical assets across the value chain.

Real-world incidents demand a world class response. AlertEnterprise also provides geo-spatial monitoring for contextually informed alerting and response to cross enterprise threats and serious acts of sabotage, terrorism, fraud and theft. Even seemingly innocent activities can be correlated with system, network, application and database access events to detect real threats and risks. Powerful alerting and automated remedial action guidance complete the system.

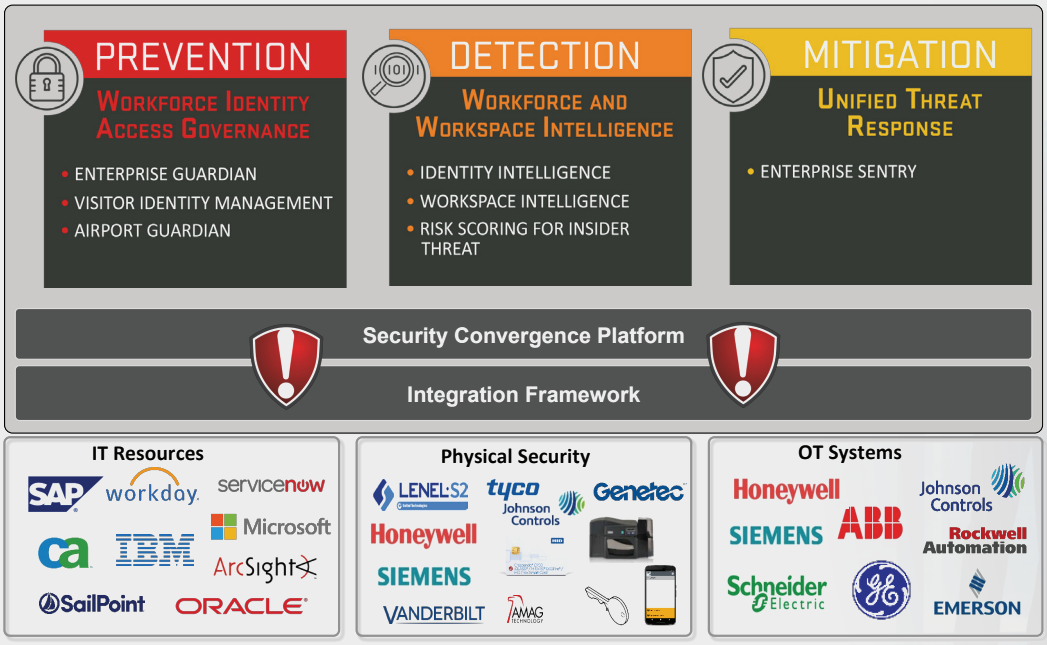
TOP 6 BENEFITS OF CONVERGENCE

As reported by organizations that have converged



2019 Security Convergence Report, ASIS Foundation
**Total does not equal 100% because respondents could select multiple answers.*

The AlertEnterprise Convergence Platform bridges the gap across IT, Physical and OT security.



Blended threats occur in the white spaces between silos of automation represented by IT, Physical and OT security. AlertEnterprise is the only platform that can uncover blended cyber-physical threats across the entire enterprise landscape.

WHERE TO START

The next steps start from within and require a deep dive into your organization and its strengths and weaknesses, developing a top-down plan based on eliminating silos, integrating identity with cyber and drawing in operational technology and automation. Once your stakeholders understand the implications of isolated plans and processes and the importance of a converged approach, you can begin to implement the right technologies to begin the journey to greater situational awareness.

The digital transformation and its impact on physical security are clear. It takes a new approach, focusing on bringing people, processes, data and technology together safely and securely. The future is here, and with AlertEnterprise organizations are now empowered to do more with less, create engaging employee experiences, increase compliance and reduce risk – all from a single, trusted digital identity platform. For more information, contact AlertEnterprise today at 510.440.0840 or info@alertenterprise.com.

ALERTENTERPRISE