Making Everything Easier!™

AlertEnterprise Special Edition

IT-OT Security Convergence

FOR DUMMIES®

A Wiley Brand

Learn to:

- Understand the benefits of security convergence
- Create a culture of convergence
- Build a convergence program

Brought to you by

AlertEnterprise!

Mike Chapple, Ph.D.

IT-OT Security Convergence

FOR DUMMIES®

A Wiley Brand

AlertEnterprise Special Edition

by Mike Chapple

FOR DUMMIES®
A Wiley Brand

IT-OT Security Convergence For Dummies®, AlertEnterprise Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-118-99954-7 (pbk); ISBN 978-1-118-99986-8 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Jennifer Bingham

Acquisitions Editor: Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Project Coordinator: Melissa Cossell

Special Help from AlertEnterprise: Ron Fabela

Table of Contents

Introduction

Critical infrastructure faces an environment consisting of increasingly sophisticated threats, requiring an equally sophisticated defense. For this reason, many critical infrastructure security professionals are turning to the concept of security convergence — combining the traditional fields of physical security, cybersecurity, and operational security.

I hope that this short book will get you started with security convergence and whet your appetite for more information about this emerging trend.

About This Book

Convergence For Dummies, AlertEnterprise Special Edition, explains the basic concepts of security convergence and shows how you can use it to enhance your organization's critical infrastructure security posture.

This book explains the new threat landscape, in which attackers target more than just IT systems. It explains how you can improve your security by taking advantage of a converged security response that integrates the traditional silos of physical security, cybersecurity, and operational security.

It also shows you some ways that you can create policy change and leverage existing technologies to get started on your convergence journey. The contents of this book were provided by and published specifically for AlertEnterprise.

Foolish Assumptions

This book is designed for critical infrastructure professionals of all backgrounds and doesn't assume familiarity with any particular discipline of critical infrastructure security. Whether you're a physical security professional, have a detailed background in cybersecurity, or focused on the security of critical infrastructure operations, this book will give you a head start on developing a converged approach.

That said, I did make a few assumptions in writing this book. Here's what I guessed:

- You have some experience in the world of critical infrastructure and are comfortable around the worlds of electric utilities, the energy industry, transportation, or similar fields.
- You have an interest in the disciplines of physical security, cybersecurity, and/or operational security specifically relating to critical infrastructure.
- You have an open mind about the convergence of those fields and recognize the value inherent in bringing them together.

If these assumptions are true, you're in the right place! This book will help you get started on developing a converged security approach that is appropriate for your organization.

Icons Used in This Book

The margins of this book sport several icons that can help guide you through the content.

TIP

When I present something that can save you time and effort, I toss in this icon to highlight it.

REMEMBER

This bit of info is worth remembering. No need to tattoo it on your forearm or anything, just keep it in mind.

WARNING!

This icon points out potential problems that you should try to avoid.

Beyond the Book

This book is designed to get you thinking about convergence and whet your appetite for a transformational change in your approach to security. Once you've read it, there are a multitude of other resources available to help you continue on your journey to converged security.

A great starting point is the AlertEnterprise website found at `www.alertenterprise.com`. It's packed with information about security convergence, including their line of solutions for the critical infrastructure industry. You'll also find case studies about how real customers have transformed their organizations by building a culture of security convergence.

Where to Go from Here

If you're looking for a broad introduction to the field of security convergence, just turn the page and start reading. Don't put this book down until you either fall asleep or can't bear to read my writing any longer! By the time you reach the final pages, you'll have a greater understanding of the field and how you can get started.

If you just want an executive-level view of the need for security convergence, Chapter 1 is the place for you. It describes how the threat landscape has changed over the past few years and how converged situational awareness and response can help you combat those threats. It also gives a few real-world examples of events that would have benefitted from a converged approach to security.

Chapter 2 provides some great background on the status quo that you'll need in order to understand how converged security approaches come together. If your background is a little light on one of the three traditional silos of security (physical security, cybersecurity, and operational security), this is the place for you. You'll leave Chapter 2 with the background you need to understand the benefits of convergence.

If you already have a strong background in security, you might skip ahead directly to Chapter 3. In that chapter, you'll learn how you can get started implementing a converged approach to security. It describes ways that you can create a culture of convergence in your organization and dives into detail on ways that you can use regulatory compliance as a lever for change.

In Chapter 4, you'll learn how existing technology provides the foundation for a converged approach to security. If you're worried that adopting converged security requires replacing your entire security infrastructure, this chapter will reassure you that convergence won't break the bank!

Finally, Chapter 5 gets down to the real fun stuff — examples of how many different critical infrastructure organizations have adopted converged approaches to security. You'll uncover use cases from electric utilities, oil and gas firms, airports, and other sensitive facilities. These will help you spark ideas about how convergence might benefit you and where you might find the low-hanging fruit in your organization.

Chapter 1

Understanding Security Convergence

In This Chapter

- Stating the case for convergence
- Exploring the new threat landscape
- Understanding the benefits of converged situational awareness and response
- Examining real-world events

For many years, information technology was a back-office function. The "IT guys" had offices buried in some forgotten corner of the building and used their wizardry to make sure that the email system and file servers functioned properly. They didn't often interact with the "real" business. System engineers kept their noses in servers while industrial engineers worried about the critical infrastructure systems that powered a business.

Over the past decade, the lines between critical infrastructure technology and information technology blurred. IT systems are now front and center, actually controlling much of the critical infrastructure. This provides powerful benefits to business, which is now able to interconnect smart devices across its operations to control business functions, physical security, environmental controls, and other assets — providing real benefit to the overall health of the organization.

With these advancements come new challenges. The risks posed by hackers, malicious code, and other computer security threats used to be limited to the IT domain. They now have the ability to reach across multiple areas of the organization, causing greater impact and disruption to critical infrastructure. The potential impact that such a disruption could have on an organization requires a higher degree of security control than ever before.

WARNING! Unfortunately, the level of protection surrounding converged technology varies greatly depending on the skills, expertise, and background of the groups responsible for installing, configuring, and maintaining them. Although some installations are highly secure, many were not designed with security in mind and jeopardize the security of the organization.

The Need for Security Convergence

Critical infrastructure operators struggle with identifying and responding to security incidents. Security problems are often initially mischaracterized as operational incidents and not recognized as information security issues. Even when an organization suspects that a security incident has taken place, it often lacks the information and tools necessary to respond appropriately. Data is spread across many different systems without any centralized monitoring or control, making incident response a difficult challenge.

The challenge is that security in critical infrastructure organizations is traditionally structured in three silos, as shown in Figure 1-1. This siloed approach simply doesn't match the reality of converged technology in the modern infrastructure operation. The threats are converged so the defense must be as well.

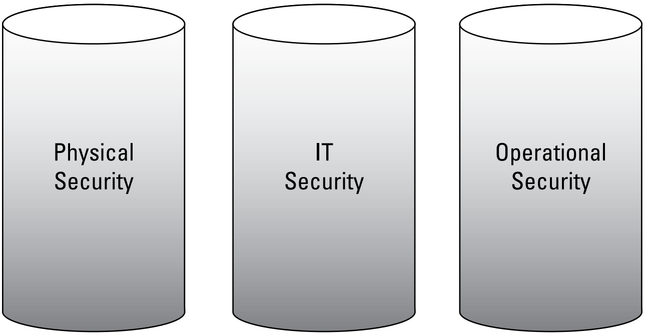


Figure 1-1: The traditional siloed approach to critical infrastructure security doesn't encourage collaboration.

Recognizing this need, many organizations are now turning to security convergence. In converged approaches to security, the people, processes, and data from multiple technologies and organizations are brought together under one operating environment. This collaborative approach, shown in Figure 1-2, breaks down the traditional security silos and brings people together to achieve increased contextual awareness — allowing them to make more accurate security decisions.

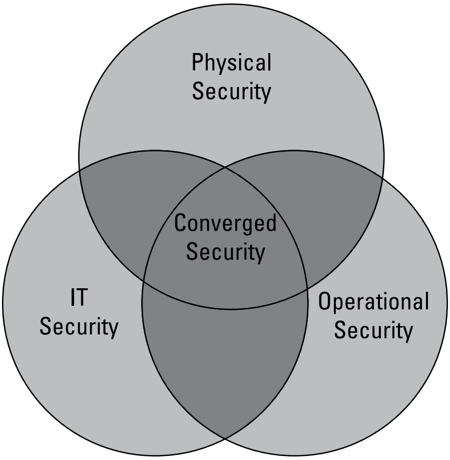


Figure 1-2: Converged approaches to security bridge the silos between physical security, operational security, and IT security.

A lack of security convergence usually becomes most evident after a major incident has occurred (or even during it). For instance, imagine a security incident where an attacker modifies the access control system that regulates physical access to the secure areas of an airport. After an intruder is detected in the facility, security responders in a nonconverged organization will have a struggle ahead of them. IT security staff may have firewall and network log data while physical security staff maintain the log trail for facility access. Responders will need to bring together different people from different organizations and coordinate their actions to assess the incident and respond appropriately. This delay may result in additional unauthorized accesses while the responders get their act together.

In a converged approach to security, this delay would be minimized, as subject matter experts on physical and IT security collaborate on a daily basis. They share common tools and can quickly bring together information from disparate systems to gain a consistent, contextual view of the security incident. Information from these disparate systems becomes much more powerful and insightful when correlated in a single place.

The New Threat Landscape

Changes to the scope and sophistication of the threats facing critical infrastructure providers make security convergence a necessity. In particular, critical infrastructure faces risks from both the insider threat and advanced persistent threats.

The insider threat

One of the most insidious threats facing organizations comes from within their own walls. There are many individuals who can access many different systems required to complete their jobs. If these individuals have undetected malicious intent, they can cause serious damage to an organization by abusing their trusted status. They're able to physically or virtually walk right past many security controls because of their position within the organization.

WARNING!

The activities of employees, temporary workers, and contractors must be monitored to ensure their physical and logical access is being used in an authorized manner. Organizations with a siloed approach to security, managing access across different departments, geographic locations, and technologies find it quite difficult to monitor insider use for anomalies.

The advanced persistent threat

External threats have changed as well. The days of the teenage hacker are over and the risk landscape is now dominated by the advanced persistent threat (APT). The characteristics of these adversaries are:

- **Technical sophistication:** APTs have access to very advanced attack techniques. On the IT side, they often employ previously undiscovered *zero-day* vulnerabilities that are quite difficult to detect.
- **Target-oriented focus:** Unlike the old-school hacker who often sought targets based on ease of attack, the APT begins a mission with a target in mind and then maintains a laserlike focus on penetrating the security controls of that organization.
- **Highly resourced:** APTs are well-funded organizations with access to very talented individuals. The skill level of the attacker may easily match or exceed the capabilities of those responsible for defending the targeted organization against attack.

Who are these APTs? They are often state-sponsored, quasi-military organizations or the forays of organized crime into cyberspace. A nation's critical infrastructure organizations — power plants, the energy industry, transportation hubs, and others — are juicy targets for the APT.

Stuxnet: APT in action

In 2010, the Iranian uranium enrichment facility located in Natanz suffered a serious setback. The centrifuges critical to the facility's operation spun out of control, causing significant damage to the facility and forcing several complete shutdowns.

Upon further investigation, security researchers discovered that the plant malfunction was due to infection of the facility's programmable logic controllers (PLCs) by malicious code. The worm, known as Stuxnet, disabled the operator's ability to control the centrifuges and then masked its own activity while it spun the centrifuges at a high rate until they were destroyed.

Although no country has officially taken credit for creating and deploying Stuxnet, there is significant circumstantial evidence that the malicious code was created by a joint U.S./Israeli action with the specific goal of shutting down the Natanz facility. That's a perfect example of an advanced persistent threat in action!

Converged Situational Awareness and Response

Converged approaches to security are able to analyze and correlate risks across the physical, operational, and technology environments. This provides security leaders with the essential intelligence they need in order to make wise decisions and effectively respond to security incidents that cross technologies. Converged security tools facilitate this process by consolidating and correlating this information in a single platform, as shown in Figure 1-3.

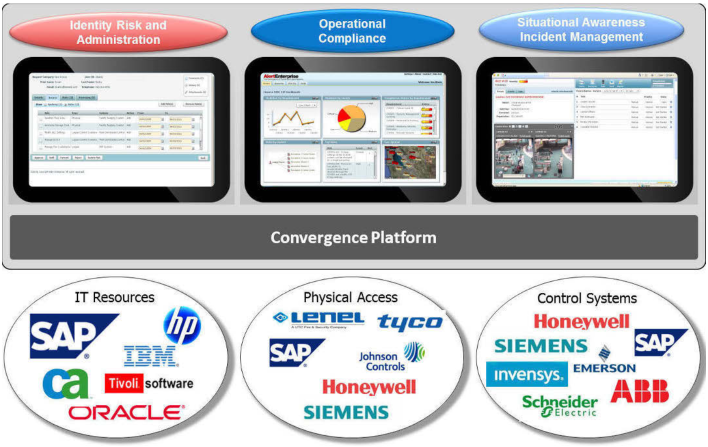


Figure 1-3: Security convergence tools provide a single platform that integrates information from a wide variety of sources.

The core benefits achieved by adopting a converged security are improving the organization's ability to:

- **Gather information:** As illustrated in Figure 1-3, security convergence platforms pull together information from a wide variety of sources. Databases, servers, physical access control systems, industrial control systems, and other sources all contribute to a single information store.
- **Facilitate decision making:** Decision makers can then draw upon that information store to immediately answer critical questions. For example, in the event of a plant

failure, decision makers can quickly recognize suspicious server activity, identify any personnel who were in the vicinity of the incident, and assess any remote network connections that were underway.

- **Enable response:** Convergence platforms go beyond information gathering and analysis. They also serve as a consolidated point of response, allowing decision makers to quickly direct response actions across a variety of systems.

With this approach, organizations are able to respond to emerging threats in an agile fashion. Decision makers immediately have the information they need to react appropriately during an incident and take action that mitigates the threat as quickly as possible.

Convergence in the Real World

As critical infrastructure organizations move toward a converged approach to security, real-world incidents highlight the need to abandon the traditional siloed approach. Over the past few years, incidents have included a coordinated attack on a major electrical substation in California, the disclosure of national security information by several leakers, and shootings at secure military bases.

Each of these events might have been mitigated or prevented if a converged approach to security had been in place.

Metcalf substation attack

In April 2013, a team of well-coordinated individuals launched a physical assault on Pacific Gas & Electric's Metcalf substation located in South San Jose. This incident affected 17 transformers and 6 circuit breakers, causing $15.4 million in damage, according to the *San Jose Mercury News*.

Officials investigating the attack noted many marks of professionalism. The attackers severed six fiberoptic cables providing telecommunications to the substation. They fired from what were likely preplanned positions and caused an incredible amount of damage to the facility. In the words of Jon Wellinghoff, former chairman of the Federal Energy Regulatory

Commission, the attack was "very well planned and well executed by very highly trained individuals." He went on to call Metcalf "the most significant incident of domestic terrorism involving the grid."

PG&E hasn't commented on the security controls in place at their substation. If they had been using a converged approach to security, they may have noticed the attackers' advance team scouting out firing positions, detected the opening of an underground vault containing the fiberoptic cables, or correlated other signs of the attack before it began, allowing a faster response from law enforcement.

Snowden disclosures

In 2013, Edward Snowden, a former contractor for the National Security Agency (NSA) and Central Intelligence Agency (CIA) leaked massive amounts of extremely sensitive national security information to the media. This was the source of great embarrassment to the U.S. intelligence community and put the U.S. government on the defensive, forcing it to defend controversial intelligence gathering methods in the public spotlight.

Snowden's actions are a perfect example of the insider threat at work. Snowden had a tremendous number of privileges due to his job responsibilities as a senior system administrator and trusted technologist. He had physical access to computer equipment and unrestricted logical access to databases containing large amounts of information about intelligence sources and methods.

When Snowden gathered the information he later leaked to the media, he didn't use any hacking tools. He simply exploited the access he legitimately had and "borrowed" the accounts of others to help expand his access. He bypassed many of the security controls put in place to prevent this type of activity by using the highly trusted credentials assigned to a system administrator.

A converged approach to security may have identified Snowden's actions as suspicious before he was able to exfiltrate and leak large amounts of information. For example, Snowden did use the accounts of other individuals to gather information. A correlation system that combined those logical access records with information from the physical access control system may have noticed any of a number of indicators:

- If Snowden accessed the information after hours, the convergence platform may have detected the use of an individual's credentials when that individual wasn't even physically present in the facility.
- If Snowden accessed the information during normal hours, the system may have noticed simultaneous logins from different physical locations.
- A convergence platform may have noticed that Snowden was accessing and copying massive amounts of information, far exceeding both his own normal activity and the activity of others in similar roles.

Any of these indicators, had they surfaced before Snowden fled to Hong Kong, may have triggered a security investigation that might have nipped the leak in the bud, preventing actions that Secretary of State John Kerry said "damaged [the] country very significantly."

Navy Yard shootings

In September 2013, a lone gunman shot and killed 12 individuals at the headquarters of Naval Sea Systems Command located on the Washington Navy Yard in Washington, DC. The attacker, Aaron Alexis, accessed the Navy Yard using a government contractor ID and attacked employees in a building where he had worked the previous week.

Converged security systems add additional intelligence to the physical access process that may help avert tragedies such as this one, brought on by an insider accessing a facility. For example, a converged security system may have been able to reach into other systems in real time when the attacker attempted to access the Navy Yard. It may have asked questions such as:

- Does this employee have a current government contract?
- Is the employee scheduled to work today?
- Is the employee authorized access to this building?
- Has the employee recently been issued a firearms license?

Red flags raised by any of these questions might have at least prompted a more rigorous screening of Alexis. This screening would likely have identified the fact that the bag he carried over his shoulder contained a disassembled sawed-off shotgun.

Chapter 2

Exploring Security Silos

In This Chapter

- Learning how physical security systems operate in critical infrastructure environments
- Understanding the components and typical installations of cybersecurity systems
- Identifying the operational security approaches used by critical infrastructure organizations

Critical infrastructure security is often divided into three silos: physical security, IT security, and operational security. Whether these systems are managed separately or in a converged manner, each is critical to the overall security health of the organization. In this chapter, I explain the components used in each silo.

REMEMBER

I've attempted to describe "typical" installations, but there really is no typical approach to these concepts. The actual implementation of physical, IT, and operational security may vary widely from organization to organization. These differences result from variations in staff expertise, budget, implementation time, and interoperability with existing systems.

Physical Security

The objective of physical security systems is to control access to facilities: granting access to authorized individuals, denying access to unauthorized individuals, and ensuring that insiders remain within the scope of their authority. Physical access control systems (PACS) may also monitor and record the activities taking place within a facility for real-time or future use.

REMEMBER

The controls used to limit physical access to facilities grew in maturity in recent years, evolving from physical keys to magnetic strip cards and the current generation of centrally managed proximity badging systems. These systems are all managed by PACS. As PACS systems increase in functionality, they also increase in complexity and reliance upon information technology.

Key components of physical security programs

There are four major components to physical security systems: the central PACS server, operator clients, badging panels, and badge readers. Each of these components interacts to provide robust physical access controls throughout the modern enterprise.

PACS servers

The increased functionality of PACS requires an increasingly complex supporting IT environment. The modern PACS relies upon servers, network connectivity, and remote management capabilities. These supporting technologies dramatically increase the efficiency of physical access technicians, who can now monitor and reconfigure access controls through a centralized PACS server.

WARNING!

The PACS server is the heart of the physical security operation. It controls all the downstream physical security components and provides real-time reporting based upon user activity and building status. As such, the PACS server is a very attractive target for an attacker and IT staff must pay careful attention to the server's security. Security controls on the PACS server should include configuration management, security patching, and monitoring of the systems and subsystems.

Operator clients

Technicians working on an organization's physical access controls normally don't log onto the server directly. Indeed, the server is normally located within a secure data center and doesn't even have a keyboard or display attached to it. Instead, the users of a PACS system run operator client software on a separate computer and that client software interacts with the server as needed.

WARNING!

In some less mature organizations, the PACS server isn't installed in a professionally managed data center and is instead sitting under someone's desk. If this is the case, you should remediate the situation immediately. Servers require the proper environmental and security controls of a data center.

The operator client systems provide a potential pathway into the organization for an attacker. Therefore, they should be professionally managed by qualified IT support personnel and configured with appropriate security controls, such as antivirus software, firewalls, network segmentation, two-factor authentication, and other measures.

Badge readers

Badge readers and other point-of-entry controls serve as the end-user interface to the PACS. These readers contain the technology needed to read information from an individual's ID card and pass it along to the PACS server for validation. Depending upon the degree of security controls, readers may also be capable of receiving a PIN input by the user and/or reading physical characteristics of the user for use in biometric authentication.

The badges used by organizations vary and have differing degrees of security associated with them. For example, the U.S. military uses a Common Access Card (CAC). This card contains a magnetic stripe and bar code for use in older access control systems but it also contains an embedded integrated circuit, providing a higher degree of security reliability for use in compatible readers.

Badging panels

Badging panels serve as the interface between the badge readers and the PACS server. Each panel controls a dozen or more badge readers and is typically installed in a data closet located in the same building as the badge readers. Badging panels often have caching capabilities that allow them to store authentication and authorization information for temporary use in the event the PACS server goes offline.

Typical physical security installations

PACS are commonly used to protect facilities of varying security significance. The more sensitive a facility, the more sophisticated the authentication requirements should be. For example, entering an office building may only require a simple badge swipe. Entering a nuclear power plant, on the other hand, may require supplementing a badge swipe with a PIN and fingerprint scan.

Combining multiple authentication techniques for very sensitive applications is a concept known as *multifactor authentication.* Multifactor authentication approaches draw from three categories of authentication type:

- **Something you have:** Such as a security ID badge or key fob
- **Something you know:** Such as a secret PIN or password
- **Something you are:** Such as a fingerprint scan, iris scan, voiceprint analysis, or hand geometry reading

Physical security systems are deployed in a variety of different areas, including:

- **Buildings and facilities:** Many buildings and other facilities require limited access and are secured by badge readers and/or other physical access control technologies.
- **Data centers:** The increasing reliance of organizations on information technology requires that they place significant importance on securing physical access to the data centers where those assets are maintained.
- **Critical infrastructure areas:** The most sophisticated physical access controls usually surround critical infrastructure targets, such as nuclear power plants, electrical substations, water treatment facilities, and chemical storage depots.

REMEMBER

PACS perform an important role in securing critical infrastructure facilities. The information they provide about who is accessing facilities and when they access those facilities is a crucial input to converged security analysis platforms. PACS may also rely upon other components of converged systems to make access control decisions, such as ensuring that an employee is scheduled to work before granting access to a facility.

IT security

IT security and access management systems have improved and matured over the decades in their size, capability, and interoperability with other systems. As the enterprise business grows, so do the opportunities to consolidate and monitor the security technologies needed to protect its IT operations. The organization is increasingly focused on the three components of the information security triad shown in Figure 2-1: confidentiality, integrity, and availability.

Increases in remote access capabilities, data sharing, and the use of cloud computing raise the complexity of information security requirements. As a result, enterprises adopt more sophisticated security technologies to meet these challenges. In a sense, enterprise IT security has started to build a converged security platform, consisting of single sign on technology, security incident and event management systems (SIEM), and configuration management capabilities.

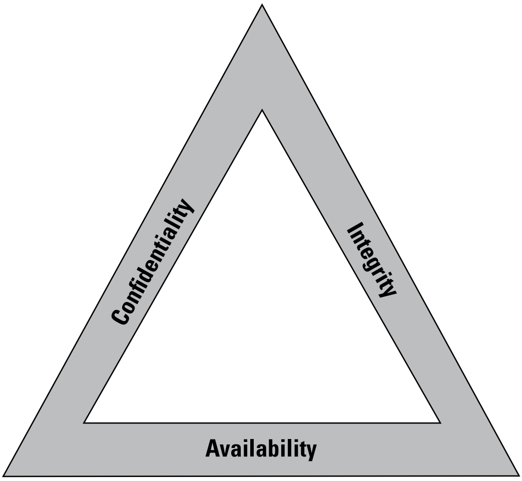


Figure 2-1: Confidentiality, integrity, and availability form the cornerstones of the IT security triad.

These capabilities are just the tip of the IT security iceberg. For example, most SIEM systems only collect and correlate data from IT systems such as server logs, firewall events, IDS logs, and other logical management systems, completely missing contextual data from other security silos such as physical security badging, operational technology, and other business systems.

Key components of IT security programs

Information security programs are complex and vary in structure from organization to organization. The specific composition of the program will depend upon the security needs of the organization and the technical infrastructure already in place. Some common components of IT security programs include:

- **Security incident and event management (SIEM)** systems consolidate logs from a variety of IT systems and correlate them for analysis. They're a form of converged security, but are typically limited to data sources within the IT security silo.
- **Identity and access management** technology ensures that individuals are properly authenticated before being granted access to IT resources and that they're authorized to access the systems they're attempting to use.
- **Vulnerability scanning** systems probe all the IT systems in the enterprise, searching out potential weaknesses that might be exploited by an adversary. Security administrators receive reports of any vulnerabilities, typically with advice on how to remediate the affected system(s).
- **Patch and configuration management** systems ensure that IT systems all run in a consistent, known state and have the most current security updates installed.
- **Antivirus technology** protects IT systems against malicious code objects, such as viruses, worms, and Trojan horses.
- **Perimeter defenses** such as firewalls and intrusion prevention systems (IPSs) form a barrier between the internal protected network and the outside world. They identify and block suspected malicious traffic before it is able to enter the enterprise network, as shown in Figure 2-2.

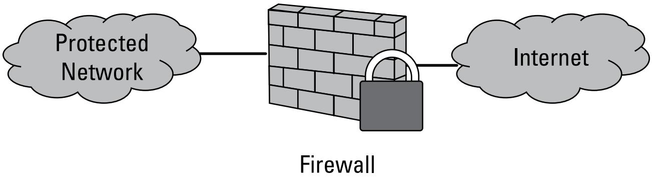


Figure 2-2: Firewalls separate private networks from public networks, such as the Internet.

These key components comprise the foundation of an IT security program. They must be operated by skilled IT staffers possessing knowledge and experience in information security issues.

Typical IT security installations

IT security programs typically contain most or all of the key components that I mention in the previous section and may also contain other components specific to the business needs of each organization. For example, organizations hosting public websites may have additional controls in place to protect against web-borne attacks. Similarly, an organization that is heavily invested in cloud computing may employ specialized cloud security products. Finally, an organization that allows employees or vendors to work remotely may allow secure access to their networks via a virtual private network (VPN).

IT security controls must be installed and maintained by qualified IT staff. They typically operate using commodity hardware and software that may be purchased off-the-shelf from IT suppliers. IT staff must then customize the configuration of those off-the-shelf products to implement the security policies of the organization. For example, a firewall must be configured to know what traffic is allowed to enter and leave the network.

IT hardware operates on a very different refresh cycle than other security systems. Whereas a physical access control system may last for a decade or longer, IT systems are typically replaced on a four- or five-year refresh cycle to avoid a disruptive equipment failure. After all, if the organization's firewall is unavailable, no network traffic may enter or leave the organization!

Operational Security

Operational security programs provide protection for the critical infrastructure systems within an organization. There are two major categories of these systems:

- **Industrial control systems** (ICS) and **distributed control systems** (DCS) are the systems that control manufacturing processes and fulfill other critical infrastructure control needs within a facility. ICS/DCS systems may be found in chemical plants, power stations, and similar facilities.
- **Supervisory control and data acquisition** (SCADA) systems control large-scale operations spanning multiple sites and include remote management capabilities. SCADA systems control entire electrical grids, energy transmission systems, and water supplies.

Operational security programs monitor and control the security of both ICS/DCS and SCADA systems.

Key components of operational security programs

Like other security silos, operational security programs include key components that form the building blocks of a larger security strategy. The major components of an operational security program are:

- **Supervisory systems** that monitor and control other components of the operational security program. These systems typically use a client/server model similar to that employed by PACS.
- **Sensors** that provide the operational measurements needed to perform control functions. Depending upon the application, sensors may measure temperature, voltage, pressure, or other characteristics.
- **Remote terminal units (RTUs)** receive measurements from sensors, convert them to digital data, and transmit them to the supervisory system. They also receive instructions from the supervisory system and carry them out to modify the industrial process.

- **Programmable logic controllers (PLCs)** perform similar functions as RTUs but have additional control capabilities on the device. They may be programmed to perform control operations without the intervention of the supervisory system. PLCs were the devices affected by the Stuxnet worm (for more on the topic, see Chapter 1).

WARNING!

ICS/DCS and SCADA systems are extremely sensitive and must be installed and configured with security in mind. It is absolutely critical that they be isolated from public networks to the greatest extent possible and have security controls in place that strictly limit access to authorized personnel and business processes.

Typical operational security installations

Operational security installations have a much longer lifecycle than IT security systems. It is common for these systems to last decades, with a typical refresh cycle of 30 or more years. Unlike IT security systems, operational security systems make use of special-purpose equipment manufactured by ICS/SCADA vendors and must be installed by specialist SCADA engineers.

Chapter 3

Implementing Policy Changes

In This Chapter

- Learning how to create a culture of convergence in an organization
- Seeing the benefits of regulatory compliance

When you decide to commit to security convergence, you begin a journey that will take some time to complete. Before you begin trying to implement convergence tools, you need to have the solid foundation of a culture of convergence throughout your organization.

In this chapter, I discuss ways that you can create a culture of convergence. You will learn the essential elements of that culture as well as ways that you can use regulatory compliance requirements as a tool to drive the organization toward convergence.

Creating a Culture of Convergence

Executive support is the most critical step toward building a culture of convergence. If the senior leaders of the organization speak openly about their support for the convergence effort and its importance to the future of the organization, that will go a long way toward creating the needed culture change. Staff at every level throughout the organization must hear the message that silos will no longer be tolerated and that convergence is the future.

Once an organization has that executive support, the culture change can extend into many other areas of daily life. Find every opportunity you can to inject messages about the value of convergence in speeches, newsletters, emails, and informal communications. Hang posters in the hallways and coffee rooms. Take every opportunity you can to talk up convergence.

Leaders and staff at every level of the organization should have goals in their performance plans that tie to the success of specific convergence initiatives. One best practice is to have the leaders of the traditional security silos each have a common goal in their performance reviews that uses the same language. Ensure they understand that they will each receive the same rating on that goal. A shared fate is a great way to accelerate teamwork!

This culture change should then be supported by policies and procedures that promote convergence. Three specific areas where organizations can encourage a converged approach are information sharing, incident response, and two-person control.

Data and information sharing

Information sharing is often one of the trickiest changes to implement in a siloed organization. High levels of mistrust may exist and this paranoia is often exacerbated among security units who highly value confidentiality. The organization's policies and procedures should promote information sharing among silos and reward those who operate with openness and transparency.

For example, the physical security department may have exclusive access to building entry and exit records. This information would be of great value to IT security staff who may use it to correlate account activity times with an individual's presence in the building. If an individual connects to your VPN from Europe, this may not initially look suspicious to the IT security team. However, if they are able to correlate that with records indicating that the individual swiped into your New York offices 30 minutes earlier, it represents a red flag that requires immediate investigation — nobody can get from New York to Europe in half an hour!

Incident response

Incident response policies are another great area to encourage convergence among security staff. One way to accomplish this is to have a single security incident response plan that covers all types of security incidents — physical, IT, and operational. This prepares you well for more complex security incidents that cross these traditional silos.

TIP

Each security unit should be represented on the incident response team. Certainly, different types of incidents will require changes in the proportional membership of the team, but including representatives of each unit on every team will continue to build the culture of sharing. You might even be surprised a few times when people bring up information sources and ideas that provide unexpected cross-domain value!

Two-person control

The concept of two-person control is found in many security processes. It says that no individual should have the sole authority to perform any sensitive action. Critical infrastructure organizations likely already use this principle in one or more areas of their operations.

Provisioning access to critical resources is one common area where organizations use two-person control. For example, if a new employee requires access to a sensitive facility, two separate managers may be required to approve that access. This prevents a single individual from granting access under duress or as an act of malfeasance.

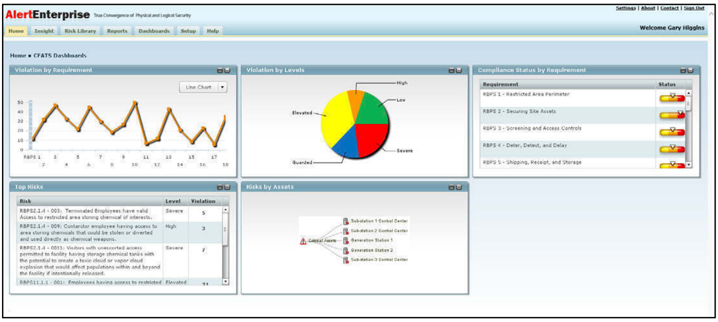
TIP

Two-person control is another opportunity to continue building the culture of convergence. Organizations may wish to modify their existing two-person control procedures to require that the two managers approving a new access request be from different security units. This provides a cross-check among the security silos and builds an understanding of each other's security functions.

Using Regulatory Compliance as a Tool

Critical infrastructure organizations are often in highly regulated fields subject to government and industry rules and standards. As such, the security teams within these organizations often operate within a culture that places high value on compliance-related activities. Tying your convergence program to your compliance program is an excellent way to position it for success within that type of culture.

For example, consider a chemical plant subject to the Chemical Facilities Anti-Terrorism Standards (CFATS). Under the standard, the facility must prepare a vulnerability assessment and then develop and implement a site security plan. Using a converged approach to security, the plant may develop a CFATS compliance dashboard similar to the one shown in Figure 3-1. This dashboard provides managers and team members with a snapshot view of CFATS compliance in real time.



Compliance Status by Requirement

Requirement	Status
RBPS 1 - Restricted Area Perimeter	
RBPS 2 - Securing Site Assets	
RBPS 3 - Screening and Access Controls	
RBPS 4 - Deter, Detect, and Delay	
RBPS 5 - Shipping, Receipt, and Storage	

Top Risks

Risk	Level	Violation
RBPS2.1.4 - 003: Terminated Employees have valid Access to restricted area storing chemical of interests.	Severe	5
RBPS2.1.4 - 009: Contarctor employee having access to area storing chemicals that could be stolen or diverted and used directly as chemical weapons.	High	3
RBPS2.1.4 - 0011: Visitors with unescorted access permitted to facility having storage chemical tanks with the potential to create a toxic cloud or vapor cloud explosion that would affect populations within and beyond the facility if intentionally released.	Severe	7
RBPS11.1.1 - 001: Employees having access to restricted	Elevated	21

Figure 3-1: Organizations subject to CFATS may benefit from a converged approach that offers a single dashboard view of their compliance status.

Common guidelines and controls

Critical infrastructure organizations are subject to a wide variety of government and industry regulations that dictate the proper functioning of their security programs. Some of these are directed at specific security silos, but they all have common themes. Adopting a converged approach to security can distribute the compliance burden across ever security team within an organization.

NIST SP 800 Series

IT security staff members are quite familiar with the National Institute of Standards and Technology Special Publication 800 series of documents. Over one hundred documents in this series outline government standards for computer security across a wide range of topics. These include:

- Risk assessment
- Risk management
- Vulnerability management
- Incident response
- Log and records management
- Testing
- Security automation
- Physical security
- Security awareness and training
- Technical/logical security controls

Each of the NIST publications is a detailed document spelling out the specific administrative, technical, and physical controls required to comply with the standard.

NERC CIP

The North American Electric Reliability Corporation (NERC) publishes a series of Critical Infrastructure Protection (CIP) standards governing power generators and suppliers. It includes regulations describing critical infrastructure security controls for:

- Personnel security
- Physical security
- Incident response
- Security training
- Disaster recovery

- Security risk management
- Technical/logical security controls

As with the NIST publications, NERC publishes CIP standards documents providing detailed expectations for each area.

HSPD-12

Homeland Security Presidential Directive 12 (HSPD-12) provides a common standard for the identification of federal employees and contractors who require access to secure facilities that are at risk of terrorist attack. HSPD-12 requires the use of "secure and reliable forms of identification" and covers:

- Technical/logical security controls
- Personnel security and identity verification
- Interagency access risk assessment

Each of these controls is designed to limit sensitive facility access to authorized individuals.

Common themes across security controls

There are many industry-specific regulations. These regulations overlap significantly. For example, most regulations cover the following topics:

- Physical security
- Personnel security
- Technical/logical controls
- Risk assessments and other business practices

That's where convergence can help. Each security silo shouldn't track this information independently to meet its own compliance requirements. Through a converged approach to security, information can be consolidated in a central platform and then used to minimize the compliance burden across overlapping regulations.

Chapter 4

Leveraging Existing Technologies

In This Chapter

- Examining the current state of your security technology
- Identifying new technologies that support a convergence effort

To be successful in building a converged approach to security, your organization must have technology in place that supports a converged approach to security. You must have tools that are able to generate, collect, and correlate information from a wide variety of sources.

Evaluating Your Current Technology State

TIP

Most organizations already own the technology needed to support a converged environment, but they simply don't realize the potential in their existing infrastructure!

The first step on the journey toward technology convergence is conducting an inventory of all of the security systems already in place within your organization. Walk through the systems used by each one of the security silos: physical security, IT security, and operational security. As you build this inventory, make note of the purpose of each system and the types of information it collects and generates.

You're likely to discover that each silo uses many of the same or similar technologies for management and security, but that those systems aren't integrated with each other. It could be that you're actually purchasing overlapping solutions or even duplicative licenses for the same products!

REMEMBER

Building this inventory will provide you with the information you need to continue on your journey toward security convergence.

Integrating silos

The easiest way to begin integrating the silos of security is to identify areas of overlap in your security technology inventory. You can then begin to remove them by consolidating similar requirements onto a single system. Here are a few examples of places where you might find and eliminate overlaps:

- If your physical security team is using one product for tracking access to buildings and your IT security team is using another product to track physical access to data centers, combine them into a single solution and grant both teams access.
- The operational security, physical security, and IT security teams likely all have needs for a consolidated logging platform that receives records from other security systems. Can you combine everything onto a single platform that supports industry standards for logging, such as the *syslog* protocol?
- The operational security team likely has a system that monitors the status of critical infrastructure elements, including sensor readings for temperature, pressure, and humidity. Is it possible to use this same system for physical security sensors, such as open/close sensors on doors and windows?
- Each of the security silos relies upon IT systems to perform their daily security tasks. Are those systems all professionally managed? The IT security group likely has a strong configuration management system in place to protect the security of their own systems. Can you leverage that system to protect all security-related computer systems within the walls of your organization?

Combining solutions in this way has the obvious benefit of saving money across the organization but it also begins to break down the security silos. When people begin working with each other's systems, it puts them into daily contact with each other and relationships begin to develop. The paranoia initially evident in most interactions among security teams can begin to give way and develop into productive relationships among colleagues.

Filling gaps

As you build your security inventory, you may also notice that there are gaps in one or more of your silos. Perhaps you notice that your IT security and operational security teams both have systems in place for tracking awareness training but the physical security team has no such program. This is both an opportunity to fill a gap and an opportunity to continue to integrate the security silos.

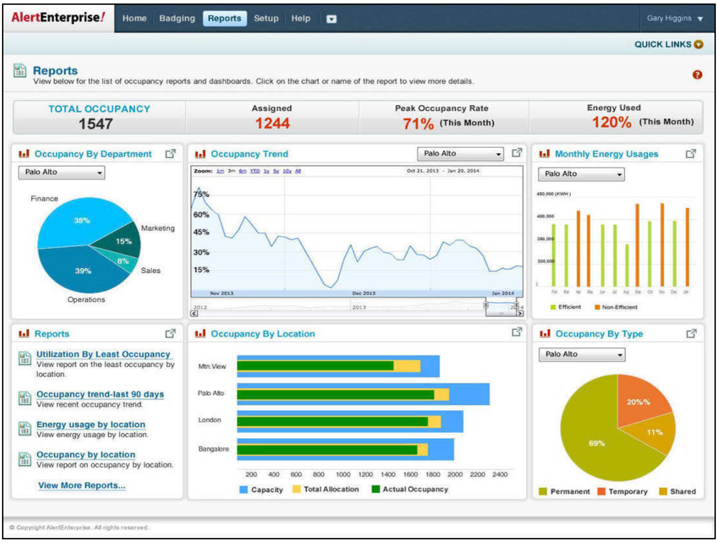
In such a case, always try to fill the gap without introducing a new system. If the physical security group can use the system already in use by either the IT security team or the operational security unit, that would be great. Even better, perhaps all three units can standardize on a single system!

You may even be able to take things a step further and integrate the business processes that drive those technologies. For example, you might be able to go beyond standardizing the three units on a converged security awareness tracking system and actually consolidate the entire security awareness training program to cover all three topics at once. Your end users will certainly be happy to only have one security training program!

Implementing New Technologies to Support Convergence

Convergence becomes even easier when facilitated by security convergence technology. Convergence solutions assist organizations in pulling together information from a variety of sources and they facilitate the decision-making process for security managers.

Convergence solutions connect to and leverage databases, systems, and applications already in use in the enterprise. They can reach across physical security systems, IT security, and management solutions and operational control system environments. Convergence solutions use a platform approach, connecting to and gathering data from all three of the security silos and displaying on a single console, sometimes referred to as a *single pane of glass,* as seen in Figure 4-1.



Reports
View below for the list of occupancy reports and dashboards. Click on the chart or name of the report to view more details.

TOTAL OCCUPANCY 1547 | Assigned 1244 | Peak Occupancy Rate 71% (This Month) | Energy Used 120% (This Month)

Reports

Utilization By Least Occupancy
View report on the least occupancy by location.

Occupancy trend-last 90 days
View recent occupancy trend.

Energy usage by location
View energy usage by location.

Occupancy by location
View report on occupancy by location.

View More Reports...

© Copyright AlertEnterprise. All rights reserved.

Figure 4-1: The single-pane-of-glass approach provided by convergence platforms allows an easy look at security information across the enterprise.

As you consider the solutions available on the market, you should compare them to the specific security requirements of your organization. Does the system support those requirements? Does the vendor have experience working in your industry and under your specific compliance regimens? Here are five things you should look for in a convergence product:

- The system should have the ability to connect with multiple security systems and components. It may use an application programming interface (API) or software development kit (SDK) to directly integrate with the target system. It may also use the OPC Data Access specification to exchange information or rely upon the use of an HTTP-based web portal.

- The system should be able to consume raw data in multiple file formats, including Excel data files (XLS) and comma-separated values (CSV). Network architecture, organizational controls, or regulatory controls may require that systems be physically separate from your network, requiring the ability to manually upload and import data files from isolated systems to the convergence platform.

- The system should allow rules-based policy enforcement. Once all of this converged data is in a centralized location, the system must be able to use, correlate, and present the data in a way useful to the organization. Rules-based workflows provide the capability for organizations to enforce policies. For example, a physical badge-in could be required before a workstation login. A rule would be configured to alert a security operator immediately if any policy discrepancies arise.

- The system should provide immediate remediation steps. When the convergence platform is used for monitoring and incident response, the use of scripted deficiency/violation response steps ensures the consistent and efficient remediation of security issues. Advanced convergence systems support the automation of those steps to ensure timely action. For example, the user may be immediately notified by email of a policy violation, allowing immediate corrective action.

- The system should act as a force multiplier for your existing capabilities. You don't want to take a *rip and replace* approach, discarding the significant investments of money and energy in your existing security infrastructure. Asking each silo to replace all of its existing technology can be challenging, if not impossible. Convergence solutions allow your business to leverage existing technologies without painful and costly changes.

These five points will give you an excellent start on your security convergence journey. Use them as a reference guide when you are evaluating different products and help get your convergence program off to an outstanding start!

Chapter 5

Seven Use Cases for Security Convergence

In This Chapter

- Examining use case for security convergence

Converged approaches to security benefit organizations of all sizes in a wide variety of fields. Convergence is particularly useful to those charged with protecting elements of the world's critical infrastructure. In this chapter, I provide seven use cases demonstrating the value that convergence brings to critical infrastructure organizations. I take you through some stepped-out scenarios of how these use cases would play out.

Physical and Logical Control Provisioning for a Sensitive Facility

A sensitive critical infrastructure facility decided to adopt a converged approach to security. In this case, both organizational policies and regulatory standards required the use of a separation-of-duties approach to access provisioning. Specifically, no single employee may have access to both critical IT systems and the physical critical infrastructure components that they control. This separation of duties is a critical part of ensuring both the operational reliability and the overall security of the facility.

In addition, the organization implements strict controls before granting an individual access to either IT or physical access. One of these controls requires background checks for all employees before they're granted any sensitive access. The Human Resources department performs criminal record and credit checks upon request and stores the results in a centralized personnel database.

In this example, the organization manufactures and stores inventory within the sensitive facility. Managers must request access for employees who need either physical access to the warehouse or logical access to the inventory control system. The separation-of-duties principle is enforced in this case because an employee with access to both systems could steal inventory from the warehouse and then alter the inventory control system to hide the theft.

Here is the process flow for access requests using a converged security solution:

1. **The access control officer receives a request for access.** The request originates from a manager requesting access for a new employee.
2. **The convergence solution performs a conflict check.** The convergence solution identifies any requests that would result in granting an employee access to both the warehouse facility and the inventory control system, violating the separation of duties principle. The system also verifies that the background check database contains valid entries for the employee.
3. **Asset owners are notified of potential conflicts.** When a conflict is detected, the convergence solution notifies the warehouse and inventory system asset owners.
4. **Asset owners approve or reject conflicting requests.** The asset owners evaluate the request in the context of both operational needs and the separation of duties requirement. The employee may be granted access as an exception only with the approval of both asset owners.

5. **If approved, access is provisioned.** If the asset owners approve the request, access is granted, but mitigation steps such as increased monitoring may be put in place on the account.

In this case, a converged approach to security allows the organization to perform automated conflict identification that reaches across HR, IT security, and physical security systems.

Physical Access and Video Surveillance for an Airport

Airports have numerous access zones in which there are hundreds or even thousands of employee badge swipes for physical access each day. Many of these sensitive areas have camera surveillance system installed. In this use case, a converged security solution monitors and highlights areas when physical access events occur, allowing response personnel to effectively manage and record incidents.

For example, here is the workflow that occurs when a door alarm is triggered in the airport:

1. **A door alarm triggers.** When a sensitive door is opened, the physical security system triggers an alarm event and passes it to the convergence system. The security watch officer notices the alarm.
2. **Video cameras are automatically focused on the door.** The converged security system automatically enlarges and highlights relevant camera views.
3. **The watch officer reviews relevant information from all security systems.** The converged security solution pulls all relevant information, including all recent badge-in events at the door, all recent accesses to any system or facility by the employee, and other information.
4. **The watch officer assesses the event.** The officer uses all available information to make a judgment about the event. For example, the video might reveal that the last employee to enter the secure area propped the door open.

5. **The watch officer takes remediation actions.** For example, the watch officer might dispatch a security guard to secure the door and notify the employee's supervisor of the security violation.

In this case, the convergence solution provides the airport watch officers with detailed information from a variety of systems, improving the efficiency and effectiveness of the response.

Access Control and Provisioning for an Airport

Airports have many different categories of secure areas and many different employee roles with varied access needs. In this use case, the convergence system processes an access request for an employee. Here is the workflow:

1. **The access control officer receives a request.** The supervisor of a new employee submits the request via the provisioning system.
2. **The convergence solution performs a conflict check.** The convergence solution identifies any requests that would result in security policy violations by cross-referencing HR and other systems. For example, the request for a janitorial staff member should not include access to the tarmac.
3. **The system sends violation notifications to the employee's supervisor.** If the request would violate security policy, it is returned to the supervisor for review and modification.
4. **The supervisor resubmits a modified request.** The supervisor corrects the policy violation and submits a modified request for review.

The convergence solution benefits the airport in this use case by allowing the access provisioning system to cross-reference other systems to identify potential policy violations.

Security Monitoring for an Electric Utility

Power plants responsible for generating electricity and transmission substations must protect their infrastructure components with both physical and logical controls. For example, SCADA systems contained within those facilities may have remote administration limited to a trusted control location.

In this use case, a converged security solution monitors SCADA remote access attempts. When an attempt occurs, the solution verifies that an employee making the request is physically present in the control facility. Deviations from this policy may indicate that either an employee is violating the policy or an intruder is using stolen access credentials.

Here is the workflow used by the convergence solution to enforce this security policy:

1. **The convergence solution detects an access attempt.** When someone attempts to remotely manage a SCADA device, it triggers an alert that is monitored by the convergence solution.
2. **The convergence solution accesses the physical security database.** The database query determines whether the employee accessing the SCADA system is physically present in the control facility.
3. **Any policy conflicts are identified by the convergence solution.** If the convergence solution detects an access attempt without a corresponding physical facility entry, it triggers a security policy conflict event.
4. **Operators receive a security conflict alert.** The convergence solution notifies the watch officer of the alert, along with relevant details.
5. **Automated and manual remediation occurs.** The convergence solution blocks the access attempt automatically and the operator may follow up with other remediation actions, such as contacting the employee.

REMEMBER

In this case, the convergence solution is able to cross the security silos and use information from multiple systems to improve the facility security.

Visitor/Contractor Access Control for an Electric Utility

Electric utilities often require background checks for visitors and contractors who require access to critical facilities. Typically, this is a resource-intensive process requiring that an administrator access multiple systems to verify and grant the proper access.

In this use case, a convergence solution connects both logical and physical access control systems with a third-party background check service to automate access provisioning.

Here is the workflow:

1. **The convergence solution receives a request for access.** An employee requests access for a visitor/contractor to a critical facility. The convergence solution receives this request either directly or from an HR system.
2. **A background check requirement is identified.** The solution detects that a background check is required, preventing access until the check is completed and reviewed by a supervisor.
3. **The background check is requested and reviewed.** The convergence solution connects to the background check system and automatically requests a check. When the check is complete, it retrieves the results.
4. **The supervisor receives the background check results.** The convergence solution notifies a supervisor of the request and the background check results. The supervisor reviews and approves the request.
5. **Access is provisioned.** If the supervisor approves the request, the convergence solution reaches into both logical and physical control systems and provisions the access.

REMEMBER

In this use case, the convergence solution increases the speed of provisioning by automatically completing many required steps. It also improves the effectiveness of security controls by enforcing the background check requirement.

Incident Response and Emergency Management for an Electric Utility

With physical threats to the U.S. electrical grid on the increase, organizations are deploying more physical security systems at critical facilities. These systems are typically focused on a single type of event. For example, a ballistics system may be used to detect gunshots.

Other systems may contain a wealth of contextual data that could greatly improve the response and management of incidents. In this use case, a convergence solution is connected to a gunshot detection system, a control system, and a physical badging system to provide a clear picture to the incident manager.

Here is the workflow:

1. **The ballistics system triggers a gunshot event.** The convergence solution receives a gunshot event notification.
2. **The convergence solution checks the physical security system.** The physical badging system provides information about any employees in the area.
3. **The convergence solution identifies and notifies any at-risk employees.** Any employees physically present in the area receive an SMS notification of the emergency, warning them to take cover.
4. **The operational security system identifies power loss.** The convergence solution receives a notification from the operational security system that power flow has been disrupted at the location of the event.
5. **The control system operator is provided with information.** The convergence system automatically notifies the control systems operator that the power flow disruption may be a result of the gunshot event and that there is a safety risk for any responders.

REMEMBER

In this use case, the convergence solution correlates physical and operational information, thus reducing the security threat.

Controlling and Monitoring Privileged Access to Protect Against the Insider Threat

Many organizations face an insider threat when it comes to logical or physical access to data and systems. Many times, these insiders use legitimate privileges in unauthorized ways. For example, an insider might use another employee's password to access a critical system.

In this use case, a convergence system mitigates the insider threat by correlating logical access attempts with physical presence. Here is the workflow:

1. **The convergence system processes physical badge-read events.** The solution receives a notification from a physical security system that Joe Smith entered a facility located in the United States.
2. **The convergence system processes a logical access attempt.** The solution receives a notification from an IT security system that Joe Smith has logged into a workstation located in Germany.
3. **The staff is notified of a potential hazard.** Detecting a potential break-in, employees in both facilities are notified of a security threat.
4. **The convergence system alerts an incident handler.** The solution provides the handler with details on each event, along with relevant video surveillance data.
5. **The incident handler directs a response.** The handler reviews the video recording and determines that the physical access in the United States is actually Joe Smith. The handler then uses the convergence system to disable the logical account.

REMEMBER

In this use case, the incident handler benefits from the use of the convergence system to correlate information from multiple sources, improving response time and effectiveness.

AlertEnterprise: The Security Convergence Solution Leader

AlertEnterprise, based in Silicon Valley, uniquely delivers Information Technology and Operational Technology (IT-OT) Convergence for Corporate and Critical Infrastructure protection. AlertEnterprise eliminates silos and uncovers blended threats across IT Security, Physical Access Controls, and Industrial Control Systems for true prevention of insider threat, fraud, theft, sabotage, and acts of terrorism. AlertEnterprise delivers Enterprise IAM, industry-specific Operational Compliance Management, as well as Situational Awareness with continuous monitoring and incident management for effective response to critical threats and protection of critical infrastructure for various sectors including pharmaceutical/healthcare, utilities, oil and gas, airports, federal agencies, and many other industries. With the AlertEnterprise incident management capability, an organization is provided with complete situational intelligence so that seemingly innocent events when correlated across IT, physical and operational domains, can be simultaneously uncovered and resolved. With AlertEnterprise, organizations can leverage their existing IT systems and physical access control systems while managing security, risk, and compliance for business applications, enhancing security and reducing risk from complex processes like onboarding and offboarding. See more at **www.alertenterprise.com**

AlertEnterprise Awards

AlertEnterprise solutions are well recognized as leaders in the security convergence solution space. AlertEnterprise has won awards ranging from the ASIS14 Accolades Security's Best Winner, SAP Pinnacle Awards, and many more!

Security Products Magazine
2012
New Product of the Year
ASIS 14 accolades
Security's Best Winner
Security Products' GOVIES
2013 Government Security Awards
SAP Pinnacle Awards 2013 Winner
2011 Winner
GSN: Government Security News
Homeland Security Awards
GRC Technology Innovator 2012
© 2012, Corporate Integrity, LLC

Adopt a converged approach to security

Taking a converged approach to security allows critical infrastructure organizations to better position themselves to combat emerging security threats. Converged approaches to security bridge the traditional silos of physical security, IT security, and operational security to create a consolidated situational awareness and response effort.

- ***Understand security convergence* — learn the role that convergence plays in consolidating information to improve situational awareness and response efforts**
- ***Explore security silos* — know the key components and typical deployments of physical security, IT security, and operational security**
- ***Implement policy changes* — understand how policy and compliance initiatives can help create a culture of convergence in your organization**
- ***Leverage existing technologies* — learn how you can use existing security technologies as components of your converged security infrastructure**

Open the book and find:

- **Examples of real events that would have benefitted from a converged approach to security**
- **Description of the threats facing critical infrastructure organizations**
- **Common themes between different regulatory environments that would benefit from convergence**
- **Case studies describing practical applications of converged security approaches**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

Mike Chapple, Ph.D. is Senior Director for IT Service Delivery at the University of Notre Dame. He is the author of 20 books, including the *CISSP Study Guide*. Follow him on Twitter @mchapple.

FOR DUMMIES®
A Wiley Brand

ISBN 978-1-118-99954-7
Book not for resale

WILEY END USER LICENSE AGREEMENT