The Industrial Control System (ICS) Visibility Imperative

Navigating Cyber Chaos and Sustaining Secure Operational Performance

A White Paper by Frost & Sullivan

FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

CONTENTS

EXECUTIVE SUMMARY

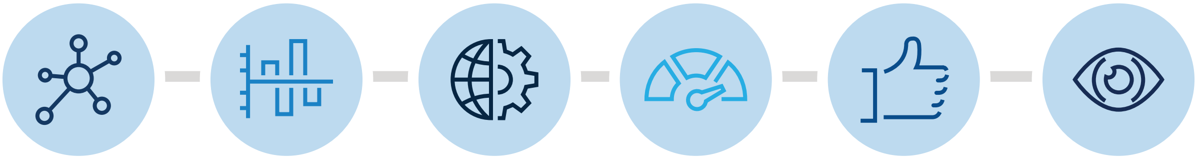
Visibility: The Key to Cybersecurity in the Digital Era

We now live in a world of technology convergences steering us to a smarter, faster, and simpler future. The convergence (OT/IT) of sensors, computing, algorithms, and cloud is driving a creative destruction and expansion of traditional operational models. No industrial market—from power generation to waste management, to food production, to pharmaceuticals—has been immune to digital transformation. Although connected devices, endpoints, and networks create a massive of amounts data, most industrial firms have limited insights and remain broadly exposed to cyber threats. Legacy industrial control system (ICS) components, which were not designed to be digitally secure, are now being connected to transformative IT technologies as firms seek to leverage data sources and optimize operational efficiencies.

With more and more devices connected to the process control network, there is a related elevation in risk for operational availability, threat visibility, and safety. Any incident that hinders an organization's ability to view, monitor, and control its industrial process is considered a cybersecurity event. Although the stakes for ICS safety, productivity, and quality are incredibly high for industrial firms, much of the industry today is reactive in its approach to managing security threats. Organizations that are imperceptive of system activities may experience significant incidents and damages from a single unaddressed cybersecurity weakness. Human errors, hardware failures, software failures, or malicious activities can occur without detection.

An organization's journey to industrial cybersecurity will be never-ending because as control system technologies continue to evolve, so will cyber threat sophistication. Ultimately, industrial firms need to establish a responsive cybersecurity posture with the ability to detect, prevent, and aptly counter undesirable cyber activities. To do so, organizations will need transversal visibility. It enables the sustaining of operational performance and efficiencies securely across vertical levels and the linear manufacturing value chain. However, the real challenge for industrial markets is the lack of expertise on how to achieve visibility.

The purpose of this paper is to unpack why ICS visibility is the cornerstone of cybersecurity and to outline six steps that organizations can take on their journey to a secure future:



STEP 01 Classify Systems

STEP 02 Define Baseline

STEP 03 Deploy Controls

STEP 04 Gauge Effectiveness

STEP 05 Authenticate Actions

STEP 06 Continuous Assessment

1 INDUSTRY EVOLUTION

Technology Transformation: OT/IT Convergence

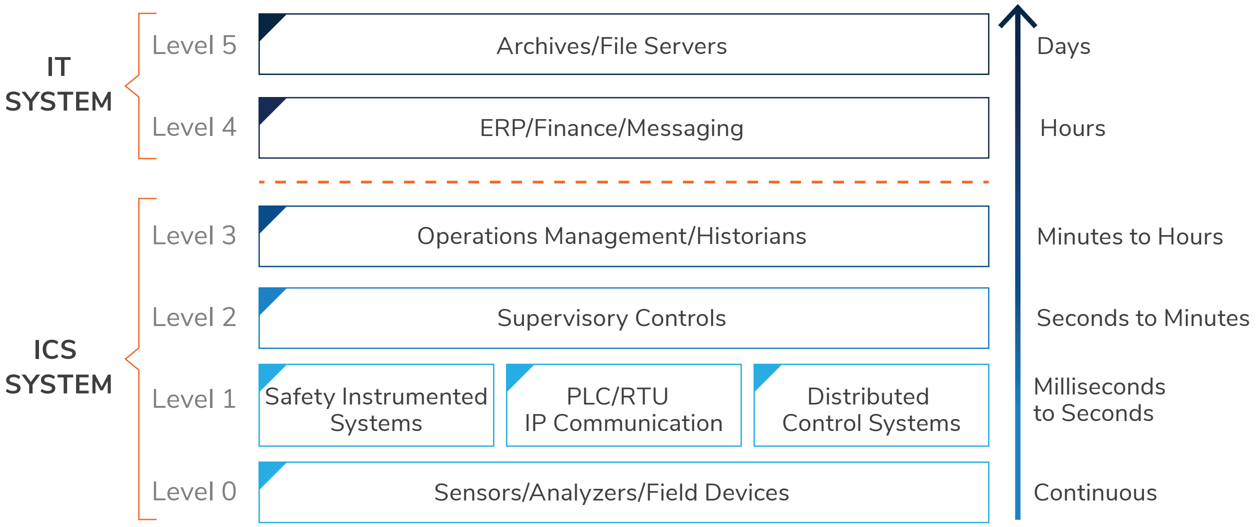
For industrial firms today, there is an increasing amount of OT and IT function overlap. More and more legacy OT assets (e.g., control systems) are being connected to IT, which creates friction between the long-established priorities of the formerly separate departments. IT has traditionally focused on securing both data flow and data integrity. OT, in contrast, centers on maintaining system availability, safe plant operations, and safe employees. Organizations seek to smooth the departmental integration and lessen the trade-off between system availability and business performance. A legacy asset refresh is the ideal inflection point for OT/IT assimilation because while such machines are essential to industrial processes, they are often outdated. A firm could replace its legacy assets, but such moves generally unacceptable as replacement costs can be astronomical. Thus, OT/IT groups must work in unison to integrate legacy control systems within the Industrial Internet of Things (IIoT) environment. Firms must also thoughtfully and securely scale in order to avoid exposure to additional safety, productivity, and quality risks.

Integration and scale issues aside, OT/IT convergence will likely result in meaningful benefits for industrial firms. Real-world cases that illustrate the transformative power of OT/IT convergence are being produced in plants and factories of various geographies and verticals. Net results vary from greater process efficiencies to increased asset reliability and powerful incident prediction. Emerging technologies are enabling streamlined workflows, and information generated by the OT layer will drive value-creation for firms whose OT embraces IT technologies.

Critical Issues: Vulnerability and Visibility

A new cybersecurity environment has formed in the wake of IIoT disruption. Across verticals, the current state of ICS infrastructure is insecure as most are not sufficiently protected against cyber threats. The core capabilities of an ICS to activate, manage, and screen industrial processes (Exhibit 1) are inept within the digital world. An ICS must now provide reliable and safe real-time operation with maximum uptime *and safeguard against cyber threats.*

EXHIBIT 1: OVERVIEW OF ICS ARCHITECTURE



Source: National Institute of Standards and Technology (NIST); Frost & Sullivan.

As organizations respond to the evolving role of ICS, they will confront two critical issues: vulnerability and visibility.

Vulnerability: First, industrial firms must address the vulnerabilities of ICS legacy assets and their insecure design. Most industrial control environments are currently obsolete because of their average age, which is an estimated 20 years. The relative shelf asset life cycle of controllers is around 15 years. Because older, legacy controls have not typically been refreshed or hardened with appropriate cybersecurity measures, its hardware and software is mismatched against current requirements. This opens the door for cyber-attacks and human error. Programming mistakes, ineffective user authentication, and sloppy password management can all adversely affect industrial processes. For example, legacy ICS networks can have a flat structure with no segmentation. User credentials may be habitually disclosed and/or hard coded, while encryption with industrial protocols may not be extensively used. Device configurations may not strictly adhere to industrial cybersecurity framework standards (e.g., NIST SP 800-82 or IEC62443). Robust user authentication protocols are also not common to the specific computers that connect to industrial Ethernet networks and control industrial equipment/processes. Such systems include programmable logic controllers (PLC), remote terminal units (RTU), and distributed control systems (DCS). The open nature of ICS devices makes it possible for parties with variable and unknown intentions to have unrestricted contact with industrial processes. Furthermore, real-time control-layer protocols, such as Modbus, Ethernet/IP, DNP3, IEC101/104, Step7, among others, were also not designed to be secure. When these protocols were first created, cybersecurity was not a concern nor did an ICS application seem relevant.

> “As organizations respond to the evolving role of ICS, they will confront two critical issues: vulnerability and visibility.

With the interconnectivity of devices, systems, and enterprises, each connected point potentially elevates the level of operational process exposure, and any additional risk must be mitigated where possible. As industrial firms shift from site-functional excellence to multi-site, enterprise-wide efficiency management, vulnerabilities may widen. For example, as apps move to the cloud, there will be a constant data exchange between the OT and IT network layers. Interactions with cloud platform services must be properly secured in order to maintain data integrity and system availability.

Visibility: After recognizing their vulnerabilities, industrial firms must tackle another unfortunate truth. They can be regularly unaware of what occurs on ICS devices, systems, and networks, even those controlling critical infrastructures. Organizations need a clear picture of their network to minimize risk for industrial processes and critical infrastructures. The visibility and security controls deemed essential today (e.g., configuration control) are not widely implemented across industrial devices, protocols, and user interfaces. Engineering activities enable the process control operations required to change set point values and drive optimization through operational dynamics. Without an understanding of such activities, organizations are lulled into mistakenly believing all is secure (e.g., cybersecurity through obscurity). Ignorance of system behaviors is one of the key reasons why industrial firms are reacting to incidents and not proactively defending against them altogether.

To begin the journey to holistic visibility, firms must be able to answer the following fundamental questions about their current cybersecurity posture:

- What assets are presently on their network?
- What firmware exists on their assets?
- How has their asset code and logic programming been executed?
- Have asset configurations been cataloged?
- Have any vulnerable assets been identified?
- Were any corrective actions performed to secure those vulnerable assets?
- What industrial protocol(s) are in place, if any?
- Does a baseline exist for standard device communication patterns?
- Has the network been diagrammed? If so, has it been continuously refreshed?

Answering these questions is necessary because cybersecurity is not a one-size-fits-all transaction. Challenges are likely to arise due to OT vendor variability. Each vendor's series of real-time industrial automation solutions are unlikely to perfectly match the needs of differing IT technologies, as every organization tends to have distinctive protocols for their hardware, software, and network.

Deeper levels of threat protection are needed for industrial control systems. Traditional defensive tactics do not provide an adequate breadth and depth of fortification to be effective today. For instance, the historically poor execution of security procedures persists even when firms face regular internal or external audits. It is also not feasible to universally apply physical protection methods, such as mechanized door locks, which may otherwise be bypassed. By enabling visibility through integrity assurance solutions, industrial firms can address their vulnerabilities and strengthen their protections against ICS cyber-attacks.

2 ICS VULNERABILITY LANDSCAPE

Navigating Cyber Chaos: Industrial Enterprises

While the world is changing rapidly, there are several ways in which the world is *not changing*: 1) companies still seek solutions to real business challenges; 2) companies remain focused on improving operational efficiency while aiming to reduce costs; and 3) enterprises must protect themselves against cyber threats. A failure to accomplish the last can dramatically impact operational efficiency, brand reputation, and cost structure.

Public awareness and scrutiny of ICS security measures has intensified in recent years for two main reasons. Principally, there are many industrial control systems that manage critical infrastructures (e.g., power generation and railway station governance). Failure or corruption of critical infrastructures could have potentially devastating side effects. Public health and safety may be risked, facilities or products could be destroyed, and considerable financial losses would likely follow. Furthermore, industrial control systems have become a hot target for cyber-attacks because of their inherently insecure design. In a 2016 report, US Department Homeland Security cited a discernible uptick in the frequency of ICS security incidents and threats. Of the 290 incidents of cyber invasions or breaches reported, 63 were in critical manufacturing and 59 in energy.

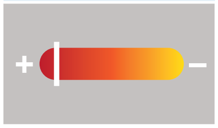
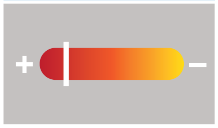
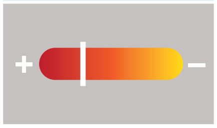
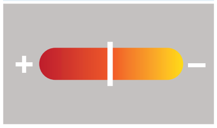
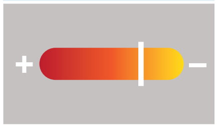
Although some of the subsequent ICS cyber risks can be mitigated, others can only be acknowledged and deterred through tactical countermeasures. Cyber posture dictates an organization's level of preparedness against potential risks and threats. A clear understanding of the continuous, never-ending journey to cybersecurity preparedness is vital for industrial firms. Systematic evaluations will help firms stay ahead of the chaos, and the end result will be a defendable level of remnant ICS security risks.

ICS Cyber Risks: Threat Types and Sources

The impact of ICS cybersecurity incidents depends on the threat type and source. For example, the stream of information could be jammed or obstructed through ICS networks to interrupt system operation. Unauthorized changes may be engineered to install new instructions, alter commands, or increase alarm thresholds. Such exploits could break or deactivate assets and/or jeopardize human life. Incorrect data could also be relayed to system operators in an attempt to complete unauthorized activity without detection or force operators to ineffectually respond to threats. ICS hardware is extraordinarily expensive and its replacement is even more costly than its repair or refreshment. If its software or configuration settings are infected with malware, equipment and operation protection systems could be destroyed.

Firms must contend with five major types of digital security threats impacting ICS systems. The three most intense threats include spear phishing, insider threats and errors, and malware management, as shown in Exhibit 2.

EXHIBIT 2: CYBERSECURITY THREAT TYPES AND INTENSITIES

THREAT TYPE	SPEAR PHISHING	INSIDER THREATS & ERRORS	MALWARE MANAGEMENT	WIRELESS FIELD DEVICES	ICS FIRMWARE
	Electronic communications scam targeting a specific individual or organization	Internal human error and/or malicious intent	Programs installed on control systems that replace existing logic	Attacks on field devices through wireless systems	OT attacks through compromised networks, Web-based malware, and improper patching
THREAT INTENSITY					

Source: Industry Estimates, DOL; Frost & Sullivan.

Limited visibility of the asset landscape hamstrings a firm's ability to counter spear phishing attacks. For instance, an unassuming email from a seemingly trustworthy source may link to an external Web site outfitted with infiltration systems. Imagine a DCS operator clicking on a spear phishing email from the operator workstation (OWS)—the threat vectors will quickly download and multiply over the network of systems. Similarly, either through error or malicious intent, insiders represent the second most intense threat. Hard coded systems and weak access procedures create avenues for current and ex-employees to access systems from outside a facility. However, some organizations in the power industry have successfully mitigated possible insider threats by recording the interaction of employees with critical systems. Recording employee behavior supports visibility and provides traceability of end-user actions.

The aforementioned threat types originate from four prevalent threat sources (Exhibit 3). Malicious third-party actors who hack systems to gain ICS access can execute any type of threat. Internal actors can also cause just as much damage through erroneous action or malignant intent.

EXHIBIT 3: CLASSIFICATION OF CYBERSECURITY THREAT SOURCES

Hostile	Unintentional	Architectural	Contextual
Hostile threat sources include individuals, groups, organizations, or nation states whose goal is to manipulate reliance on cyber resources, assets, and connectivity; these can either be internal or external.	Unintentional threats stem from mistakes or errors performed by internal staff during the fulfillment of their assigned responsibilities.	Architectural threats consist of stoppages or malfunctions of hardware, software, firmware, or controls. This can be caused by obsolescence, resource availability, or other factors that mutate standard operating conditions.	Contextual threats involve environmental elements outside the control of an organization with the ability to cause failures of critical infrastructure (e.g., natural disasters).

Source: NIST; Frost & Sullivan.

> In an interaction with Frost & Sullivan, a director of IT security & compliance at a midstream company stated, “I am most concerned about advanced, nation-state attacks. This overlaps with insider threats because an advanced attacker will use existing accounts and is effectively an insider once they compromise an existing employee account. Also, spear phishing is the primary point of entry for an advanced, nation-state attacker.” However, another midstream executive felt insider threats are of greater concern, stating, “Current or former employees have detailed knowledge of the operating and security environment. Often times, when an employee leaves the company, their network ID is turned off, but most of the time, passwords to control equipment that they might have knowledge of are not changed. This is a major problem.”

Organizations cannot afford to simply react to the new landscape as threats continue to advance. Their posture for counteracting cyber threats must become as nimble and proactive as possible. In Chapter 3, the regulations and agencies who can guide cybersecurity postural transformation are thoroughly reviewed. Structured guidelines and standards developed in response to the growing number ICS security incidents and increased public scrutiny are also included.

3 ICS CYBERSECURITY REGULATIONS AND BENCHMARKS

Key Regulatory Developments: NIST Standards & Others

Agencies exist to help organizations meet defined standards while prudently mitigating trade-offs between safety, availability, integrity, and confidentiality. The National Institute of Standards and Technology (NIST) is a key resource for industrial firms. In partnership with public and private sectors, NIST introduced specific guidelines on the deployment of ICS security controls.

NIST ICS Supplemental Guidance is an extensive reference material for organizations on the proper application of security controls and control enhancements to ICS environments. The outline guides organizations through specific security controls or control enhancements and their corresponding ICS applications.

NIST ICS Enhancements offer instructions for augmenting legacy controls, which may be essential for many industrial control systems.

NIST ICS Enhancement Supplemental Guidance offers direction on the pertinence of control enhancements and how to apply them effectively within ICS environments.

NIST ICS Risk Management Framework (Special Publication 800-53) outlines key security-control selection procedures for federal information systems. The framework matches security requirements found in Federal Information Processing Standard (FIPS) 200. It guides the selection of a primary set of baseline security controls in accordance with FIPS 199 worst-case impact analysis. The framework standardizes security control policies and balances security controls with organizational risk assessments. Seventeen areas are featured in the security rules, including incident response, access control, disaster recovery, and business continuity. Three other prominent ICS cyber regulations to consider include IEC 62443, NERC- CIP v3-6, and NEI 08-09.

IEC 62443 was created by the International Electrotechnical Commission (IEC). It sets the standard process criteria for the secure activation of products used in industrial automation and control systems. It maps a secure development life cycle (SDL) for the creating and sustaining of secure products. The standard defines parameters for secure design, implementation, coding, verification, validation, deficiency management, patch management, and product end-of-life. IEC 62443 also pertains to emerging or existing processes for advancing, conserving, and withdrawing hardware. However, the standard applies to the firm producing the products and not to the operator or end user.

NERC-CIP v3-6 was developed by The North American Electric Reliability Corporation. Its critical infrastructure protection plan (NERC-CIP) sets the security criteria for electric infrastructure and corresponding operational assets in North America. The purpose of the plan is to establish accountability for guarding against compromises preceding the mismanagement or volatility of the bulk electric system (BES). It contains 9 standards and 45 requirements that define the safety and defense critical cyber assets. Personnel and training, security management controls, and disaster recovery planning are also outlined.

NEI 08-09 was created by The Nuclear Energy Institute (NEI) as a cybersecurity plan for nuclear power reactors. Its purpose is to guide firms through the implementation of requirements in the Code of Regulations 10 CFR 73.54 ("Protection of digital computer and communication systems and networks at nuclear sites"). The plan provides information on how organizations can address peripheral access control, inspections, event responsibility, event reaction management, and system integrity.

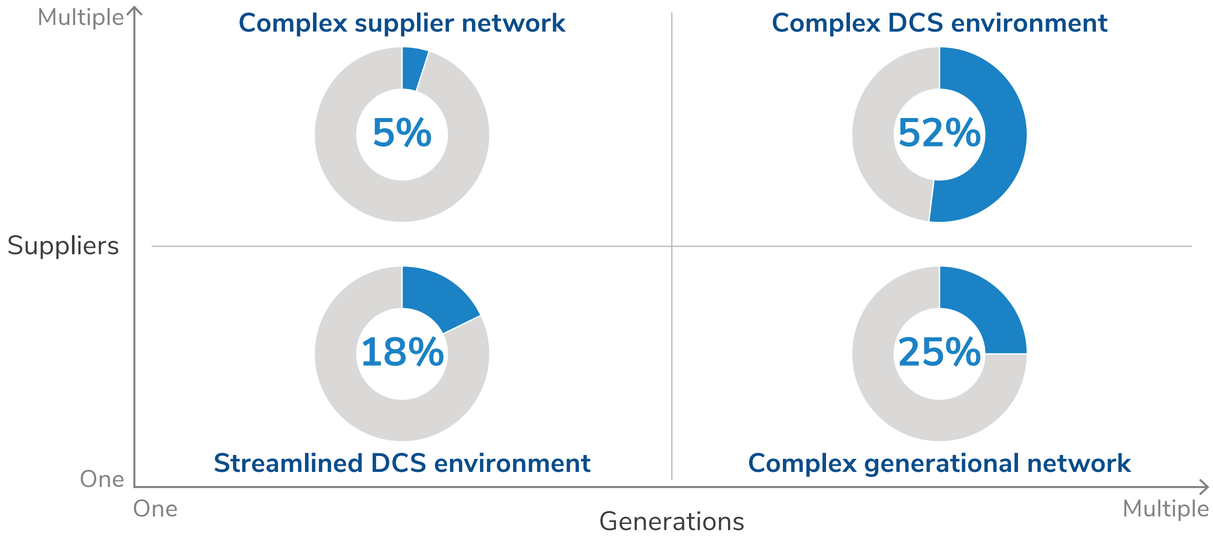
Diversity in Standards & Geographies

Regardless of manufacturing category and geography, cybersecurity challenges are present. The current state of cybersecurity in an industry depends on how heavily it is regulated. Utilities, for instance, have much more advanced systems in place because they are forced to comply with government mandates on cybersecurity control. However, even in the case of utilities, only a small portion meets regulation requirements. For example, the preponderance of transmission substations or generation facilities is not meeting regulatory thresholds under NERC-CIP requirements. Such requisites include the number of lines inflowing and outflowing or the maximum megawatt production. While the power industry is the most government-regulated industry, cybersecurity governance in other industries is driven by corporate initiatives. Cybersecurity awareness is increasing throughout industrial verticals such as automotive, aerospace and defense, electronics, and semiconductors.

The worldwide adoption also varies, with Europe leading the way followed by North America and Asia-Pacific. Strong data security and governance policies that are specific to regions create hurdles to remote system monitoring and performance management.

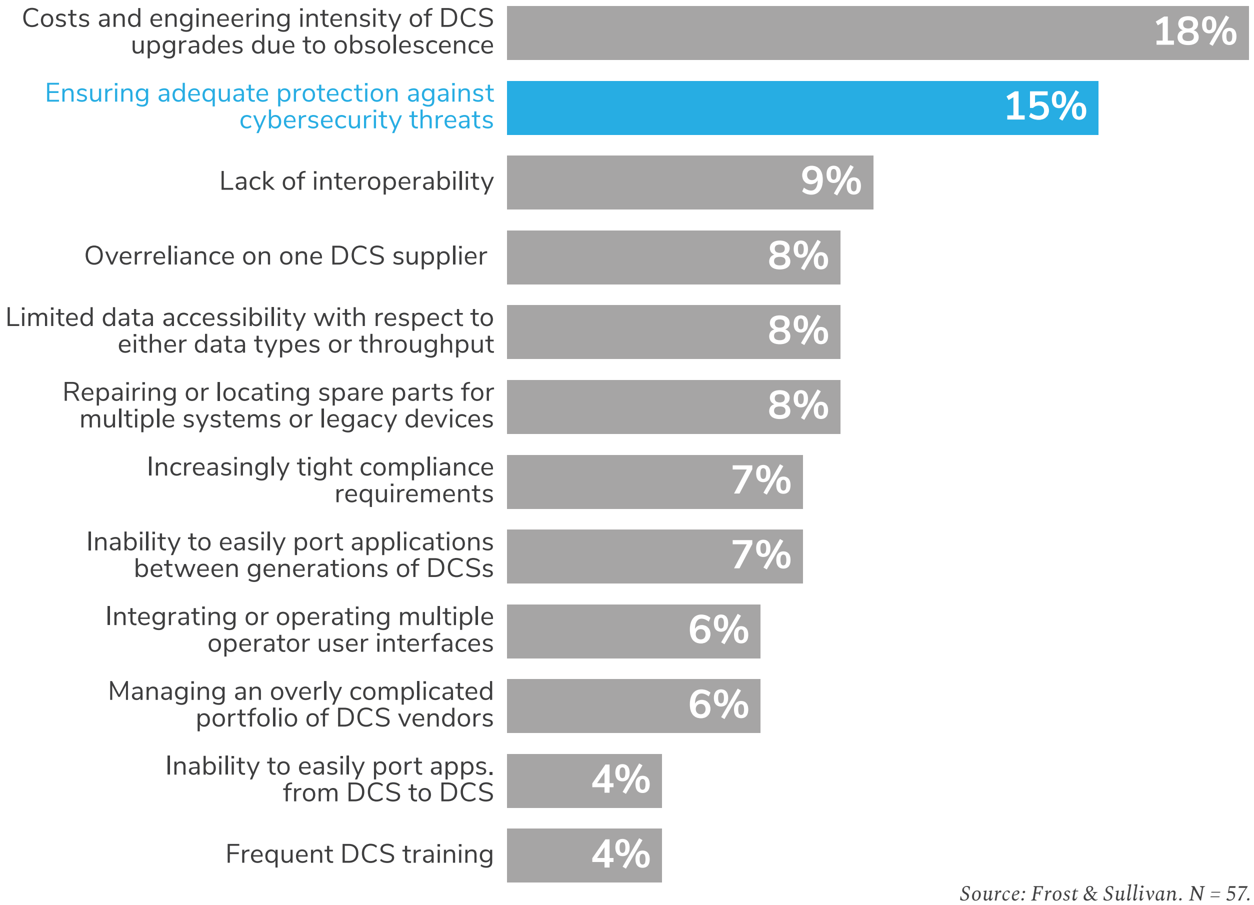
Recent Frost & Sullivan surveys of global industrial facilities indicate two key findings. First, over half the industrial firms surveyed have complex distributed control system (DCS) environments (Exhibit 4). Second, a key pressure point for industrial firms is sustaining adequate protection against cybersecurity threats (Exhibit 5). ICS complexity stems from the diversity of system make, vintage, and age as well as proprietary controls and access protocols. Achieving fleet-wide system visibility is a very cumbersome process for organizations that work with several disjointed DCS OEMs.

EXHIBIT 4: DCS ENVIRONMENT CHARACTERISTICS, GLOBAL, 2016–2018



Source: Frost & Sullivan. N = 57.

EXHIBIT 5: DCS PRESSURE POINTS



Source: Frost & Sullivan. N = 57.

Manufacturing Industries: Process, Discrete, & Hybrid

Manufacturing represents many verticals, products, and processes. There is a sizeable diversity among its functions and operations. However, the industry can be boiled down to two general categories: process-based manufacturing and discrete-based manufacturing:

Process-based manufacturing industries usually use continuous or batch processes:

- Continuous manufacturing processes run uninterrupted and transitions occur to make different versions of a product. Petroleum production in a refinery or the movement of fuel or steam in a power plant are examples of continuous manufacturing processes.
- Batch manufacturing processes have separate administration steps that are dependent upon material quantity. Each batch process has its own distinct start and end step. Steady state operations occur concisely during intermediate steps. Food manufacturing is a representative example of the batch manufacturing process.

Discrete-based manufacturing industries create end products by executing a series of steps on a particular item. For example, electronic parts fabrication for a semiconductor qualifies as discrete-based manufacturing. Exhibit 6 showcases vertical examples of discrete-based manufacturing and their corresponding ICS network.

EXHIBIT 6: DISCRETE-BASED MANUFACTURING AND ICS

Automotive

Automotive manufacturers design and produce a range of vehicles in many variations and in either one or multiple locations.

A key to delivering flexible manufacturing capabilities is reducing downtime and maximizing output.

Aerospace & Defense

Aerospace and defense (A&D) firms are adopting many new technologies, including robotics/autonomous systems, artificial intelligence, additive manufacturing, and sensors.

However, the approach to A&D's digital innovation strategy needs to be disciplined. Highly credible and trusted partners will be relied upon to develop low-risk solutions that mitigate the inherent complexity of new technology adoption.

Electronics

The need to control costs is a major priority for electronics manufacturers.

New technological innovations enter the market, and this creates new revenue opportunities. On the other hand, electronic manufacturers frequently partner with technology solutions providers to leverage capabilities outside of the scope of the company.

Semiconductors

Semiconductors are used expansively in electronic devices, such as smartphones, flat-screen monitors and LED TVs, civil aerospace, and military systems.

Industry growth is driven by the expanding needs of long battery life, AI capabilities, and biometrics for cloud computing, internet-connected devices (IoT), and machine learning.

Source: Frost & Sullivan.

Despite operational differences, process-based and discrete-based industries both incorporate sensors, actuators, and networks into their production. Other facilities, which deploy a range of both discrete and process-based assembly, are classified as hybrid manufacturing. However, it is important to note type of process does not protect an industrial firm from cyber threats – whether internal or external.

While Chapter 3 mapped the cybersecurity threat landscape, Chapters 4 and 5 will explain how organizations can implement visibility solutions—the cornerstone of ICS cybersecurity—and address their vulnerabilities.

4 VALUE OF VISIBILITY

Strategic Importance & Objectives

Imagine one window illustrating complete visibility of all systems (vendor, make, model, and firmware), industrial protocols, vulnerabilities, communication patterns, configurations, and system/device logs. Achieving such a capability requires ICS systems and networks to visualize security threats and respond in near real time. Today, 80% of time is spent collecting data and 20% is spent analyzing it.

A value inversion must happen, wherein solutions such as machine learning algorithms will augment human intelligence and enable exception-based monitoring.

To begin a prudent cybersecurity investment strategy, organizations must first structure their journey towards a secure future. Comprehensive security objectives for ICS include visibility, prevention, and continuous monitoring (Exhibit 7). Once holistic visibility is achieved, suitable protective controls can be implemented. Continuous monitoring can then be established to ensure effective safeguards and countermeasures.

EXHIBIT 7: COMPREHENSIVE SECURITY OBJECTIVES FOR ICS

Visibility

A clear picture of the control network

- Catalog assets for both hardware/software
- View industrial communication
- Map network topology
- List configuration changes
- Pinpoint vulnerabilities

Prevention

A plan for the installation protective controls

- Segment networks effectively
- Define zones and conduits
- Harden systems and devices
- Centralize remote access
- Deploy compensating controls

Continuous Monitoring

An understanding of proper operational function

- Outline device configuration
- Set operational baselines
- Enable logging
- Identify new vulnerabilities
- Identify rogue assets/protocols
- Protect against preventative control circumvention

Source: Tripwire; Frost & Sullivan.

Security Objective 1: Visibility. Firms create visibility by bridging the cybersecurity gap between IT and OT environments and establishing a clear picture of what is occurring on all of its devices—both legacy and modern. Knowing what is on the control network is the first step of cybersecurity. Otherwise, it is next to impossible for an industrial organization to secure the unknown.

Security Objective 2: Prevention. Organizations confront breach scenarios from several sources, such as discontented employees, corporate espionage, and potential state-sponsored or organized criminal attacks on critical infrastructure. To help prevent attacks after holistic visibility is achieved, the most sensitive and valuable assets associated with industrial safety/productivity must be outfitted with protective controls.

Security Objective 3: Continuous Monitoring. It is imperative for firms to know the state of normal, unobstructed network function and device configuration. This enables the detection of when and where unauthorized or unintended system alterations or activities occur. Continuous monitoring enables a secure baseline and the ability to recognize unexpected behavior.

Operational Benefits

Major operational benefits can be realized by securing industrial automation systems and sustaining their safety, reliability, and availability. Security risk management accountability and visibility policies require monitoring ICS networks in order to detect threats and prevent incidents. Industrial firms must safeguard the interests of its operations, staff, shareholders, customers, and related stakeholders. ICS visibility is a cornerstone of informed cybersecurity decisions on protective actions, and it produces the following operational benefits (Exhibit 8):

EXHIBIT 8: OPERATIONAL BENEFITS OF VISIBILITY

Greater control system safety, reliability, and availability	Stronger performance against regulatory targets and requirements	Lesser legal liabilities
Fewer community concerns or apprehensions	Weightier insurance coverage and cost	Better employee morale, loyalty, and retention
Finer goodwill for the corporate brand and reputation	Higher investor investor confidence	Stronger investor and banking relations

Source: NIST; Frost & Sullivan.

“Low-hanging Fruit” Actions

An organization’s categorization, scope, volume, and performance constraints determine its relevant management controls and often define its security controls. Industrial firms can achieve rapid benefits by acting straightaway to reduce security risks through assessing, pinpointing, and executing subsequent “low-hanging fruit” actions, such as:

- Segmenting networks
- Securing remote access points
- Hardening devices to an industrial cybersecurity framework requirements (e.g., NIST SP 800-82, IEC62443)

- Limiting Internet connectivity
- Removing email and USB connectivity from control stations or consoles

To combat amplified cybersecurity stakes, industrial firms can implement strategically sound integrity assurance solutions and achieve visibility. "Low-hanging fruit" actions will support the process and generate organizational momentum. If firms do not act to prevent incidents and protect assets, employees, and stakeholders, then considerable and irreversible losses may occur.

5 EVALUATION RECOMMENDATIONS

Supplier Selection Criteria: Key Solutions

According to NIST and other regulatory agencies, there is no singular "savior" security product or technology that can provide sufficient ICS environment protection on its own. Industrial firms need to deploy a balanced yet powerful combination of security technologies and a properly configured set of security controls. For instance, if one mechanism fails, the entire system must not also follow suit.

There are major operation considerations to weigh during the selection and implementation of ICS security controls. Organizations must judge which security controls meet their needs, what implementation timeline to pursue, and determine if their selected controls are enabling effective visibility. For each instance, the following questions should be addressed:

1. **Security Control Possibilities.** What security controls will competently lessen risk to a satisfactory level while simultaneously supporting key organizational functions? How quickly can the current state of the ICS environment be assessed against targeted security controls?
2. **Implementation Timeline.** What is the targeted timeline for security control implementation, and is it practical against industry benchmarks? Have implementation priorities been set? If so, in what order will systems impacted?
3. **Effective Visibility.** Have the given security controls been properly implemented? Are they operating as expected? Is someone trying to subvert the security controls? Can optimal configuration be confirmed regularly?

> Industrial firms need to deploy a balanced yet powerful combination of security technologies and a properly configured set of security controls.

Ideal Security: Integrity Assurance Supplier Solutions Portfolio

As industrial processes adapt, cyber threats surface, technology landscapes evolve, and new regulations develop, integrity assurance solutions are needed more than ever. Their purpose is to help organizations build fortified foundations for security, compliance, and operational excellence.

The ideal supplier solution portfolio enables industrial firms to achieve visibility across ICS networks, reduce their attack surfaces, and increase awareness of suspicious changes (Exhibit 9).

These outcomes are the pillars of system integrity and data integrity. The average firm's integrity assurance needs are twofold. Initially, they need to sustain a high level of visibility into the underlying infrastructure and supporting industrial processes. Next, they need to ensure there are no detrimental effects to safety, integrity, availability, confidentiality, productivity, and quality.

EXHIBIT 9: THE IDEAL ICS VISIBILITY SOLUTION CAPABILITIES

Asset Roster and ICS Protocol Itemization	Precise Administration	Threat Recognition	Security Aptitude Evaluation
✓ Map networks with precision ✓ Thoroughly reconcile all assets on control network via deep packet review on major industrial protocols	✓ Systematize all security controls ✓ Spot any changes to controller configurations, mode changes, and firmware updates by administering change management policies	✓ Deter attackers through early threat detection ✓ Spot anomalies and identify malicious activity by recognizing variations from normal behavior and corresponding behaviors	✓ Ardently address vulnerabilities ✓ Define the state of cyber performance and follow best practices to root out configuration weaknesses and possible vulnerabilities

Source: Tripwire; Frost & Sullivan.

Visibility Solution Adoption

Tripwire is a best-in-class ICS visibility solution provider, and two key abilities set it apart from its peers. First, Tripwire can provide complete coverage for all levels of the Purdue Model from level 0 (field devices, I/O) to level 4 and 5 (enterprise IT). Second, Tripwire can collect data through a variety of methods (Exhibit 10). Its non-intrusive data collection methods include active, passive, and hybrid techniques. Their strategic combination of data acquisition methods maximizes uptime because both agentless and agent-based passive data collection keeps legacy systems up and running during data acquisition. Unlike traditional vulnerability management and security configuration management (SCM) products, Tripwire employs no-touch sensing that can be used when legacy systems would otherwise crash if polled or queried directly.

Tripwire also has a strategic partnership with Claroty, a leader in cybersecurity for industrial control networks. Together, the pair created Tripwire Industrial Visibility (TIV), an integrated top floor to shop floor cybersecurity solution. TIV delivers unchallenged visibility, monitoring, and threat reconciliation throughout OT environment. TIV dissects the network traffic between all isolated assets and visualizes it for operators to take proactive action on anomalies. The strength of the solution centers on its ability to simulate attacks, which will help customers understand security loopholes, what-if scenarios, and the potential impact on the organization.

TIV is a highly effective solution for industrial cybersecurity strategy because it not only provides visibility to all assets, but it also facilitates protective countermeasure implementation. TIV generates organizational value by 1) verifying the reliability and integrity of the industrial process and 2) seamlessly integrating the control and administration of both IT and OT networks.

EXHIBIT 10: STRATEGIC COMBINATION OF TRIPWIRE DATA COLLECTION METHODS

Active

Collecting data by actively interfacing with a device

- Using polling (e.g., native ICS protocol and SNMP)
- Leveraging command line interfaces
- Via web user interfaces
- Running software agents

Passive

Collecting data passively by analyzing and dissecting a copy of network traffic

- Configuring switch port analyzers (SPAN)
- Through the use of mirror ports
- Through the use of network taps

Hybrid

Collecting data by interacting with applications where data is available or accessible

- Utilizing Rockwell FT Asset Centre
- Integrating with MDT Autosave
- Leveraging Kepware

Source: Tripwire; Frost & Sullivan.

In adopting visibility solutions, industrial firms lay the foundation for protecting the security and integrity of its infrastructure. The following foundational controls are recommended for ensuring ICS security (Exhibit 11).

EXHIBIT 11: TABLE OF KEY ICS SECURITY SOLUTIONS TO ADOPT

SOLUTION AREA	DESCRIPTION	BEST-IN-CLASS EXAMPLE
Threat Detection	Industrial firms should monitor for changes in configurations and/or security policies as indicators of threat activity.	**Tripwire Enterprise** Tripwire Enterprise detects configuration changes, providing intelligence on how changes affect security posture and compliance.
Vulnerability Management	To assess vulnerabilities, firms need a clear picture of its network assets, users, and devices.	**Tripwire IP360** Tripwire IP 360 accurately determines risks, which enables agile responses to potentially unprotected assets.
Enterprise Visibility	Visibility needs are not limited to a single access point. Integrity assurance solutions must also be viable when scaled across an enterprise.	**Tripwire Industrial Visibility** Tripwire Industrial Visibility analyzes network traffic and performs deep packet inspections to detect possible threats to the safety and availability of OT environments.
Log Collection	By collecting logs, firms can better understand all events of interest.	**Tripwire Log Center** Tripwire Log Center tailors log collection and filtering rules using a simple and user-friendly drag and drop interface.

Source: Tripwire; Frost & Sullivan.

6 STRATEGIC CONCLUSION

Key Takeaways: Visibility is the Future

Traditional IT boundaries are evaporating as corporate and operational systems become more thoroughly integrated. Organizations will continue to leverage emerging technologies in order to capitalize on key innovations. However, in the quest for operational excellence, companies must also be cognizant of how security risks may be intensified by digitalization. Industrial firms are currently under-reacting to new cyber risks, which are happening more frequently and with greater sophistication. ICS security controls must adapt to match their mutated role within the cyber environment. Strategic investments in cyber posture transformation should be considered by company executives, business leaders, and IT management teams. Such initiatives will facilitate organizational growth and innovation.

Industrial firms with integrated ICS systems can move to strengthen their ICS cybersecurity posture and reduce risks by evaluating the following:

Consider what makes the organization vulnerable. Because industrial control systems are insecure by design, their vulnerabilities carry a high risk for the organization, its assets, its people, and its stakeholders. The cyber threats of today are real and dynamic; the number of cyber incidents targeting ICS critical infrastructures is on the rise. Ignorance and inaction on cybersecurity needs may result in far reaching physical, economic, and societal consequences.

Consider the current state of security. A security and operational baseline will enable comprehensive visibility and help customers take proactive steps to address compliance issues or harden system weaknesses. To become cyber secure, industrial firms must have an inventory of ICS assets, including firmware, hardware, software, devices, and equipment. This inventory defines the current the state of security and the level of organizational preparedness against cyber-attacks.

Consider how to protect assets and detect threats. Although preventive controls harden key ICS assets, detection capabilities and responsiveness are equally important. Even if actors, malicious or otherwise, manage to access the ICS environment, situational awareness has the ability to drastically lessen damage from intrusions.

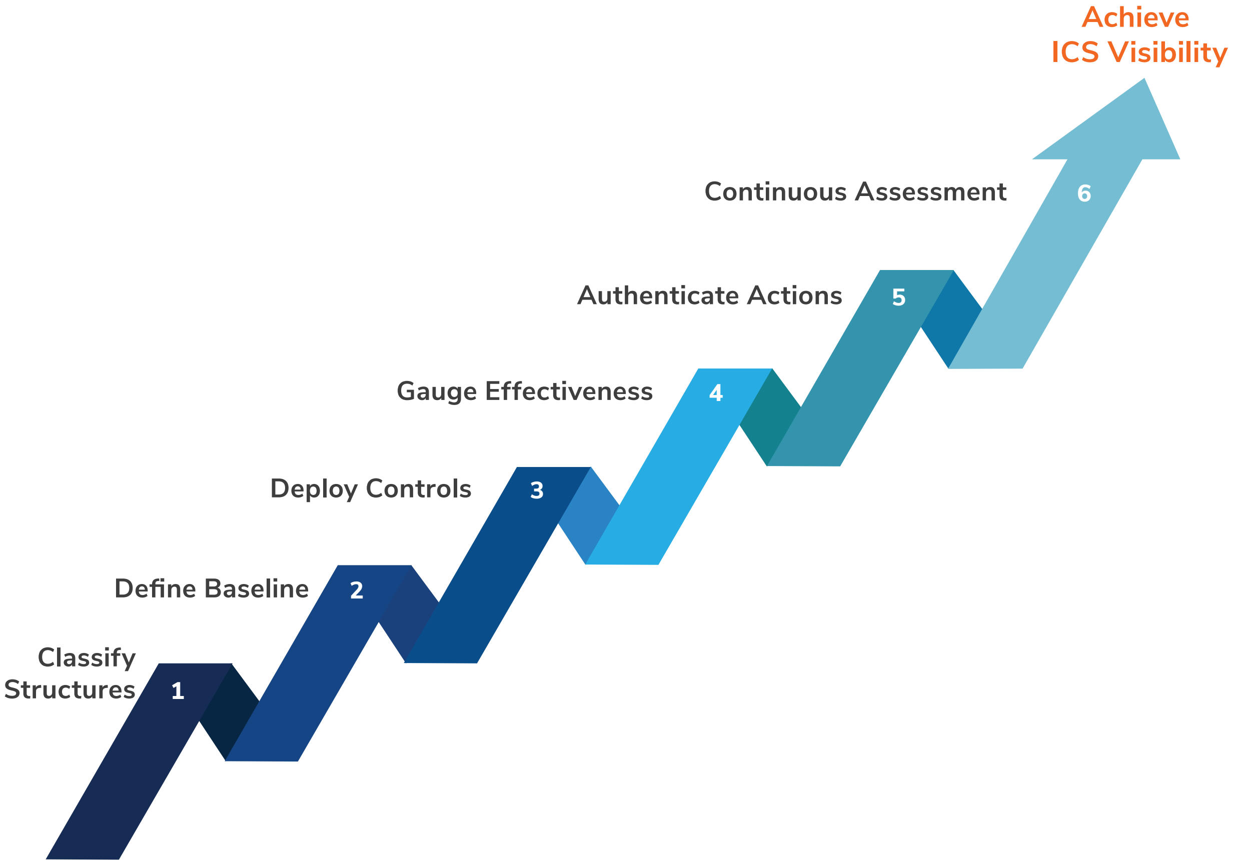
Consider proactive cybersecurity measures. A proactive cybersecurity stance does not occur overnight, it requires organizational investment and strategic planning. The challenge of enabling proactive cybersecurity measures occurs on two fronts—technology and bureaucracy. Leadership must recognize the strategic value of visibility in order to realize its organizational and operational benefits.

Secure Future Roadmap

Visibility is the strategic imperative for industrial firms today because it is not possible to secure an ICS environment without fully understanding its assets and behaviors. Organizations can opt to work with a solution provider whose differentiated solutions match current and future ICS challenges. As systems become more open, integrated, and connected, IIoT communication protocols will likely become key requirements for the next generation of ICS systems.

Based on the NIST Risk Management Framework, Frost & Sullivan recommends the following six steps for firms on their journey to achieving holistic ICS visibility (Exhibit 12).

EXHIBIT 12: SIX STEPS REQUIRED TO ACHIEVE ICS VISIBILITY



Source: Frost & Sullivan.

- **Step 1: Classify Structures.** Information and subsequent assets of an ICS must be classified by the level of organizational impact if potentially damaged. The Federal Information Security Management Act (FISMA) defined the three most important cybersecurity objectives as 1) confidentiality, 2) integrity, and 3) system availability. Within ICS environments, availability is considered the top concern.
- **Step 2: Define Baseline.** The security control selection process begins with baseline controls. Appropriate selection is ascertained by the security category and corresponding impact level to the ICS environment (Step 1).
- **Step 3: Deploy Controls.** Frost & Sullivan recommends the following security controls: 1) network segmentation and 2) device configuration hardening to an industrial standard, such as NIST SP 800-82 or IEC62443. Security controls can then be installed in new information systems (per requirements) or legacy information systems (per embedded security controls). Controls to refresh security are expected to be incorporated into the systems during Step 3.

- **Step 4: Gauge Effectiveness.** The effectiveness of security controls in the information system must be gauged. While NIST guidelines determine proper security control assessments for protected implementation and operation, system performance should be judged on an ongoing basis in order to achieve the desired outcomes and security requirements.
- **Step 5: Authenticate Actions.** Ultimately, management decides whether or not to approve the operation of an ICS. Risks are then unequivocally accepted with operations, assets, or individuals.
- **Step 6: Continuous Assessment.** The organization must continuously assess whether or not potential changes have been made to the ICS. Monitoring activities creates the situational agility needed for cyber preparedness.

ICS visibility solution providers, such as Tripwire, exist to help organizations navigate cybersecurity challenges. Selecting the right solution provider to guide your firm to a secure ICS future is the linchpin in future-proofing tactical investments.

MAKE THE STRATEGIC CHOICE TO EXPERIENCE VISIBILITY AND SUSTAIN SECURE OPERATIONAL PERFORMANCE!

Speak with a Tripwire representative:
https://www.tripwire.com/contact/

FROST & SULLIVAN

NEXT STEPS >

- **Schedule a meeting with our global team** to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.

- Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.

- Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

SILICON VALLEY | 3211 Scott Blvd, Santa Clara, CA 95054
Tel +1 650.475.4500 | Fax +1 650.475.1571

SAN ANTONIO | 7550 West Interstate 10, Suite 400, San Antonio, Texas 78229-5616
Tel +1 210.348.1000 | Fax +1 210.348.1003

LONDON | Floor 3 - Building 5, Chiswick Business Park, 566 Chiswick High Road, London W4 5YF
TEL +44 (0)20 8996 8500 | FAX +44 (0)20 8994 1389

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?