tripwire by HelpSystems

SOLUTION BRIEF

Cybersecurity for Pharmaceutical Companies

Prescriptive Guidance to Preempt Attacks and Stay Compliant

Quote

"Adversaries are in it for the long haul. They continuously attempt to take data out of companies, mining for IP that can help them identify compounds to develop drugs and give them an edge in their respective countries."

— Booz Allen Hamilton

Given the significance and prevalence of their intellectual property, pharmaceutical companies are prime targets for cyber attacks—the biotech and pharmaceutical industries experienced a staggering 50 percent increase in cyberattacks from 2019 to 2020 alone[1]. The consequences of a successful breach are concerning, ranging from stolen IP, repeating clinical trials, contaminated drugs, physical damage and downtime, litigation and lost revenue.

There are many motives to attack a pharmaceutical company. Attackers may look for valuable and sensitive data like formulas and compounds. Attackers may disrupt a manufacturing process (industrial control systems such as SCADA or PLC) to compromise a drug going to market. Since this can mean the difference between life and death, security measures must become a higher priority. An example of this was when a hacker installed malware on a water company's distribution system, traversed to the SCADA system and changed the chlorine level of the drinking water to potentially harmful levels[2]. Another emerging threat is attackers using cyber espionage to gain competitive edge or to carry out political objectives.

Security and Compliance Collide

There's no doubt that IT security is top of mind with pharmaceutical companies; many must also demonstrate compliance with FDA 21 CFR Part 11. This regulation spells out controls and audit requirements for clinical trial systems that use electronic records and signatures. The intent behind the regulation is to assure the data accuracy, reliability and integrity.

In addition, the United States Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to safeguard protected health information (PHI) by mandating procedures and controls to assure the public that critical and private information is controlled from loss of confidentiality, integrity or availability. Some pharma clinical data is also scoped under HIPAA if it is patient PHI. As FDA 21 CFR Part 11 is a primary compliance concern with pharmaceutical companies, security and compliance efforts intersect here.

OT Cybersecurity Best Practices

Pharmaceutical companies need to secure the IT side of their business, but their operational technology (OT) environments are just as crucial to protect—especially considering the potential dangers to human life that could occur if elements of the manufacturing process are tampered with. In addition to concerns of safety, OT cybersecurity also helps the bottom line by enabling systems to experience maximum uptime and availability. Luckily, OT-specific cybersecurity technology can help you achieve full visibility with continuous threat detection, ensure secure remote access, and integrate with your IT operations solutions for an integrated and cohesive view.

Tripwire Helps Pharmaceutical Companies

Tripwire offers foundational controls for a solid cybersecurity strategy to preempt cyber attacks on IP-based systems. Whether it is a database of clinical trial data or drug formulas, or an industrial control system used in the manufacturing of pharmaceuticals, Tripwire offers security configuration management, vulnerability management and log management capabilities to protect critical systems. These are fundamental to security, as indicated by SANS (Fig.1) and many other industry experts who urge implementing the first six CIS Controls.

Table 2. First Six CIS Controls: High Impact, Immediate Benefits

Category	Control Title(s)	Why It's So Important
Know What You Are Protecting	CIS Control #1: Inventory and Control of Hardware Assets CIS Control #2: Inventory and Control of Software Assets	The first two Controls require rigor in knowing what endpoints must be protected and what software is running on those endpoints. Although many IT organizations have some version of a Configuration Management Database, invariably security teams find devices and software that are either not visible to or not managed by IT operations.
Continuously Monitor Vulnerability of Resources	CIS Control #3: Continuous Vulnerability Management	After the baseline is known and endpoints are configured securely, those configurations must be monitored for changes that introduce vulnerabilities or the availability of patches or upgrades needed to maintain security.
Limit and Monitor Administrative Privileges	CIS Control #4: Controlled Use of Administrative Privileges	Having addressed the basic vulnerabilities of the hardware and software resources, the vulnerabilities of user accounts must be minimized. Maintaining the least privilege to support "need to share" while maintaining "need to know" can keep malicious software from successfully executing if it does get installed.
Define Secure Configuration Baselines	CIS Control #5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	With an accurate inventory and the ability to continuously monitor assets, the next step is to establish, implement and actively manage the configuration of endpoints against configuration standards, such as the CIS benchmarks, the United States Department of Defense (DoD) Security Technical Implementation Guide (STIG) and so forth.
Continuous Monitoring/ Situational Awareness	CIS Control #6: Maintenance, Monitoring and Analysis of Audit Logs	Nothing stands still: IT installs new software, threats develop new attacks, organizations and priorities change. Situational awareness is key for security teams to focus on deploying resources in the most effective and efficient areas to meet business security needs.

Fig. 1 SANS recommends the first six, high-impact CIS Controls.

Monitor to Preempt Attacks on Your Data & Systems

Tripwire® Enterprise delivers change audit and threat detection with high precision, business context, and automated remediation or guidance. Tripwire Enterprise monitors systems for unauthorized changes that could compromise system integrity. Its Policy Manager delivers proactive configuration hardening based on compliance requirements, reduces audit preparation time and cost, and provides audit-ready reporting with evidence of compliance, remediation and exception management. It also provides real-time threat detection and notification at "the speed of change." Configuration errors need corrective measures, and Tripwire Enterprise delivers the guidance needed for rapid repair. Tripwire Enterprise provides coverage for the widest breadth of system platforms and platform versions available, and readily integrates with SIEMs, IT-GRC, workflow systems, change management systems and more.

Assess and Take Action On Your Risk

Industrial Control System Visibility & Monitoring

Tripwire Industrial Visibility gathers threat data to improve the safety and availability of your OT environment. It does so by analyzing network traffic and conducting protocol deconstruction to inventory assets, create network topology, and more. It taps into OT network communication by listening through the SPAN port of routers and switches connected to the network segment, opening data packets and interpreting protocols without disrupting normal operations. Legacy OT networks can be sensitive to latency and bandwidth change, which is why Tripwire Industrial Visibility uses agentless monitoring and an integrated combination of passive and active asset discovery to leave your network undisturbed.

Log Intelligence to Proactively Protect Pharmaceutical Data and Systems

Tripwire LogCenter® integrates data from Tripwire Enterprise and Tripwire IP360, providing organizations with insight into the relationships between suspicious events, system changes, weak configurations and current vulnerabilities. Tripwire LogCenter reduces the workload and costs associated with traditional SIEMs and security analytics solutions by prefiltering data and identifying anomalies and patterns known to be threats and early indicators of breaches. This allows Tripwire LogCenter to forward only actionable, relevant data to SOC staff and third-party tools (such as threat intelligence solutions). For OT environments, Tripwire LogCenter is included with Tripwire Industrial Visibility.

Tripwire Helps Pharmaceuticals Achieve Compliance

Tripwire solutions offer highly automated foundational controls to meet the security requirements of FDA 21 CFR Part 11 and HIPAA (Section 164), reducing time spent fighting fires caused by poor network and data security practices, and enhancing the data security of ePHI or other electronic records (see examples in Fig. 2 and table next page). For additional information on HIPAA compliance, please refer to the solution brief The Tripwire HIPAA Solution: Meeting The Security Standards Set Forth In Section 164. Pharmaceutical companies can be confident with Tripwire's proven track record for compliance and popular security frameworks (e.g. CIS Controls, HIPAA, NIST, NERC, SOX, etc.)

Conclusion

Cyber threats to pharmaceutical organizations are real, and regulations are only a single step toward addressing the issue. Cybersecurity efforts must be a business initiative with people, process and technology efforts to combat the threat. Tripwire's proven track record with security and compliance solutions is an answer for pharmaceutical companies. Tripwire offers critical foundational controls to preempt and discover attacks to your data systems and manufacturing systems with the goal of ensuring confidentiality, integrity and availability for the pharmaceutical industry.

References

1 https://www.helpnetsecurity.com/2020/11/20/attacks-biotech-pharmaceutical-industry-escalate/

2 www.ibtimes.co.uk/hackers-hijacked-chemical-controls-water-treatment-plant-utility-company-was-using-1988-server-1551266

Tripwire Helps You Achieve and Maintain HIPAA Section 164

Requirement	Tripwire Response	Tripwire Enterprise	Tripwire IP360	Tripwire Log Center
§ 164.306 Security standards: General rules.				
(a) General requirements. Covered entities and business associates must do the following:				
(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	Tripwire monitors systems for any unauthorized changes, and discovers and prioritizes vulnerabilities to ensure health data is not compromised. Organizations can correlate events with changes that impact IT policies.	Provides	Provides	Supports
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.	Tripwire detects unauthorized changes, and discovers and prioritizes vulnerabilities. Organizations can correlate events with changes that impact IT policies.	Provides	Provides	Supports
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.	Tripwire detects unauthorized changes, and discovers and prioritizes vulnerabilities. Organizations can correlate events with the changes that impact IT policies.	Provides	Provides	Supports
(4) Ensure compliance with this subpart by its workforce.	Tripwire provides policies and documents to ensure certain security efforts.	Provides	Provides	Validates

Fig. 2 Examples of how Tripwire solutions support HIPAA compliance. For complete details, please refer to **Tripwire's HIPAA solution brief**.

Quote

"Tripwire's fundamental controls provide continuous monitoring and control to anticipate and preempt an attack on our intellectual property. On top on that Tripwire offers audit-ready reports to demonstrate compliance."

— CISO,
Large Pharmaceutical

How Tripwire Can Help with the Most Important Requirements of FDA 21 CFR Part 11

Requirement		Tripwire
System Validation — 11.10(a)	"Procedures should be in place for Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records."	Supports: Tripwire Enterprise ensures that systems are configured securely and monitors file systems to mitigate the risk of unauthorized access and cybersecurity breaches which can impact the accuracy, reliability and availability of systems.
Accurate and Complete Copies — 11.10(b) and 11.10(c)	(b) "Procedures should be in place to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records."	Validate: Tripwire Enterprise could possibly validate if copies of documents are exact.
Accurate and Ready Retrieval — 11.10(c)	(c) "Records must be protected to enable their accurate and ready retrieval throughout the records retention period".	Validates: Tripwire Enterprise can confirm that systems settings are such that logs are appropriately protected, backed up and possibly what settings are that support retention. Supports: Tripwire Enterprise generates alerts for unauthorized changes (thus, protecting the records). Tripwire LogCenter's log management and archiving capabilities retain logs for the required periods.
Limited Access — 11.10(d)	"Procedures should be in place to limit system access to authorized users."	Supports: Tripwire Enterprise generates alerts for unauthorized changes. Tripwire Enterprise can also make sure a system is configured to restrict access to authorized users. Tripwire LogCenter rules can capture successful and unsuccessful logins for all monitored hosts.
User-Independent Computer Generated Time-Stamped Audit Trails — 11.10(e)	"Procedures should be available to use secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying".	Provides: Tripwire LogCenter provides log collection, retention and reporting. Tripwire Enterprise identifies files used for evidence of compliance, and monitors them for change and retention. Tripwire Enterprise can also make sure a system is configured with the appropriate controls to protect logs implemented.
Operational System Checks — 11.10(f)	"Procedures should be available to use operational system checks to enforce permitted sequencing of steps and events, as appropriate".	Supports: In a distinct use case, if a system is using something that feeds the step data—such as a batch file that you might find in control systems—Tripwire Enterprise can make sure that all changes to that file are reported.
Use of Authority Checks — 11.10(g)	"Procedures should be available to use authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand".	Supports: Tripwire can scan logs for account management activity and configuration settings to ensure authentication is enforced, alerting as appropriate. Tripwire Enterprise also alerts to unauthorized changes. Tripwire Enterprise can make sure proper controls are implemented and enforce them.
Use of Device Checks — 11.10(h)	"Procedures should be available to use device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction".	Supports: Tripwire Enterprise can discover the authorized device configuration and advise if it is compliant.
Individual Accountability — 11.10(j)	"Procedures should be available to establish, and adhere to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification".	Supports: Tripwire can scan logs for account management activity and configuration settings to ensure authentication is enforced, alerting as appropriate.

Controls Over System Documentation — 11.10(k)	Procedures should be in place for appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Supports: Tripwire can scan logs for account management activity and configuration settings for changes to account privilege, alerting as appropriate. Tripwire Enterprise can make sure that controls exist, are turned on and can alert when changes take place.
Use of Digital Signatures for Open Systems — 11.30	"Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified for closed systems, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality".	Supports: Tripwire's Change Auditing feature can be custom configured to assess if an application or operating system is configured for secure data transmission, storage or event logging—itself logging when these settings are changed or suppressed. Tripwire Enterprise can make sure that the systems used are properly configured and hardened and can alert on any changes to their configuration
Electronic signature components and controls — 11.200	"(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password."	Supports: Tripwire can verify configuration settings for passwords and other security settings to meet and maintain compliance requirements.
Controls for identification codes/passwords — 11.300	"Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). (c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. (d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. (e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner."	Supports: Tripwire can verify configuration settings for passwords and other security settings to meet and maintain compliance requirements.

Source of Important Requirements from Lab Compliance, Dr Huber
www.labcompliance.com/tutorial/part11/default.aspx?sm=d_c#requirements

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

SBCPC2b 2102