CYBER-SECURITY COMPLIANCE

Guide to Data Protection Regulatory Compliance with Panda Adaptive Defense

pandasecurity.com

panda

Over the last few years, new regulatory acts have been passed aimed at ensuring that companies and organizations store and process customers' **personal and sensitive** data in an appropriate and lawful manner.

1. What data protection laws and regulations might companies be affected by?
2. How does Panda Security help achieve regulatory compliance?
3. Main data protection regulations that may affect your organization
    - 3.A. General Data Protection Regulation (GDPR)
    - 3.B. Payment Card Industry Data Security Standard (PCI DSS)
    - 3.C. Health Insurance Portability and Accountability Act (HIPAA)
    - 3.D. Sarbanes-Oxley (SOX)

1. What data protection laws and regulations might companies be affected by?

Some data protection laws and regulations are specifically aimed at companies belonging to certain industry sectors. These are the main ones:

General Data Protection Regulation (GDPR).

Cross-sector regulation that applies to any organization that collects or processes personal data of European Union residents.

Payment Card Industry Data Security Standard (PCI-DSS).

Applies to e-commerce companies, banks and other retail and financial institutions that store or process cardholder data.

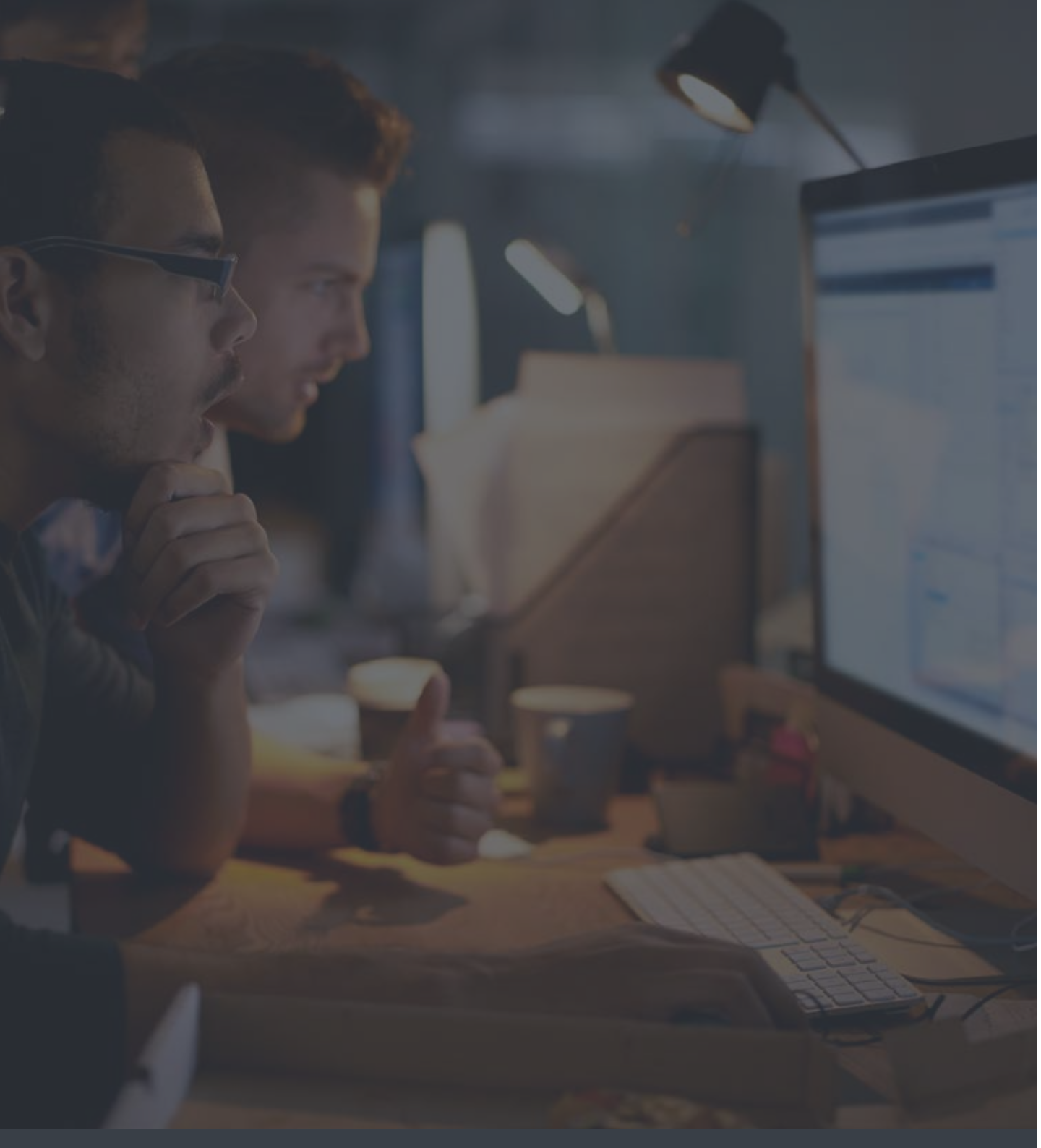
Health Insurance Portability and Accountability Act (HIPAA).

A U.S federal law affecting organizations that store and transmit personal health information in electronic form.

Sarbanes-Oxley (SOX)

This regulation affects companies listed on the New York Stock Exchange and their subsidiaries.

In some specific cases also affects to private organizations.



The possibility of suffering an **internal or external attack** that compromises the personal and sensitive data of customers and organizations, and the obligation to maintain **records of all accesses** and operations on said data, are forcing companies to implement strong data **security measures** to avoid or minimize the following consequences:

- **Hefty fines** and penalties for regulatory breach.
- **Costs** deriving from the forensic analysis and research performed in the event of data exfiltration.
- **Loss of confidence** from customers, contractors, employees and other stakeholders, as a result of security breaches or personal data exfiltration.
- Damage to **reputation/goodwill** resulting in **operational risks.**

2. How does Panda Security help achieve regulatory compliance?

These regulations are designed to ensure the confidentiality, integrity and security of the personal and corporate data that is the subject of each of them. And to meet that objective, all regulations focus on three main areas:

- **Security** of the personal and corporate data created, received, stored or transmitted.
- **Data privacy**, with a special focus on the protocols used to access, transmit and share personal data.
- **Notification of data breaches** to regulatory authorities, regardless of when the breach took place. This forces companies to keep log files for retrieval if required.

Panda Security's advanced Endpoint Detection and Response solution Panda Adaptive Defense, and Panda Adaptive Defense 360 which also includes Endpoint Protection capabilities, along with their additional modules Advanced Reporting Tool, Data Control and SIEMFeeder, help organizations achieve regulatory compliance through the continuous monitoring of the actions performed on the files at rest and in transit found on the protected workstations and servers. Specifically:

Panda Adaptive Defense and Panda Adaptive Defense 360

Panda Adaptive Defense and **Panda Adaptive Defense 360** are **advanced security solutions** that protect employees' and contractors' workstations, servers and laptops against any type of threat: from known, advanced and zero-day malware to ransomware, fileless (memory-based) and malwareless attacks.

Panda Security's solutions leverage a unique security approach based on the **continuous monitoring of all applications and processes** running on the network, making sure that only those applications trusted by Panda Security are allowed to run.

This **advanced security model** ensures maximum efficiency in all phases of the adaptive security strategy that all organizations should implement: from **Prevention and Detection**, to **continuous Response** to threats and incidents, and **Remediation**. Providing these features to organizations in the most seamless and convenient way is only possible thanks to our solutions' managed services: 100% Attestation Service and Threat Hunting Investigation Service (THIS).

For more information about **Panda's Adaptive Defense Platform** and its managed services, please visit: https://www.pandasecurity.com/intelligence-platform/

Panda Data Control[1]

Panda Data Control is an additional module for **Panda Adaptive Defense** and **Panda Adaptive Defense 360**. It offers **monitoring and control** tools to find the **unstructured personal data files** stored on an organization's workstations and servers. Additionally, it provides real-time monitoring of every action taken on such files, reducing the risk of **loss and exfiltration** inside and outside of the corporate network.

Panda Data Control allows organizations to view the personal data found both in real time and retrospectively, via dashboards and preconfigured reports that can be tailored to their needs. With **Panda Data Control**, organizations can simplify audits, as well as policy management and data governance.

Advanced Reporting Tool (ART)

Advanced Reporting Tool (ART) is an **additional module** for Panda Security's advanced security solutions. It stores and correlates, unattendedly, information regarding the events occurring on a company's workstations and servers, along with their context and enriched data generated by the Panda Adaptive Defense Platform.

This reporting and visualization module is **100% cloud-based**, which eliminates the need for additional investments in storage, maintenance and processing infrastructures. Also, the collected data is stored for a period of one year, enabling companies to access information regarding past accesses or breaches retrospectively if required by the relevant authorities.

The SIEMFeeder module

The **SIEMFeeder module** allows organizations with an existing SIEM solution to feed it in real time with event data collected from their network and enriched by Panda Adaptive Defense's platform. Then, it's the responsibility of the head of IT security to set the log retention policies required to ensure compliance with applicable data protection regulations.

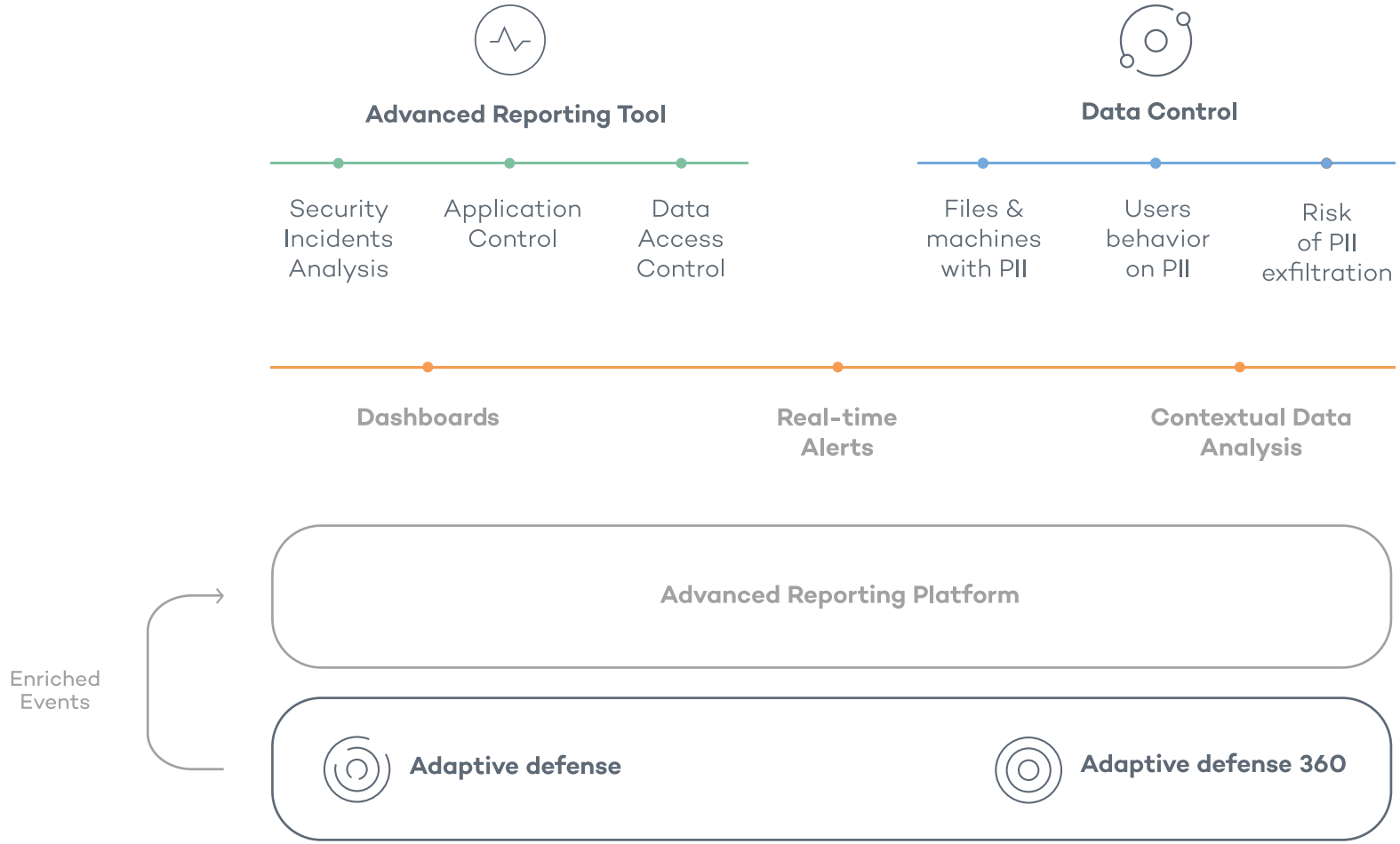
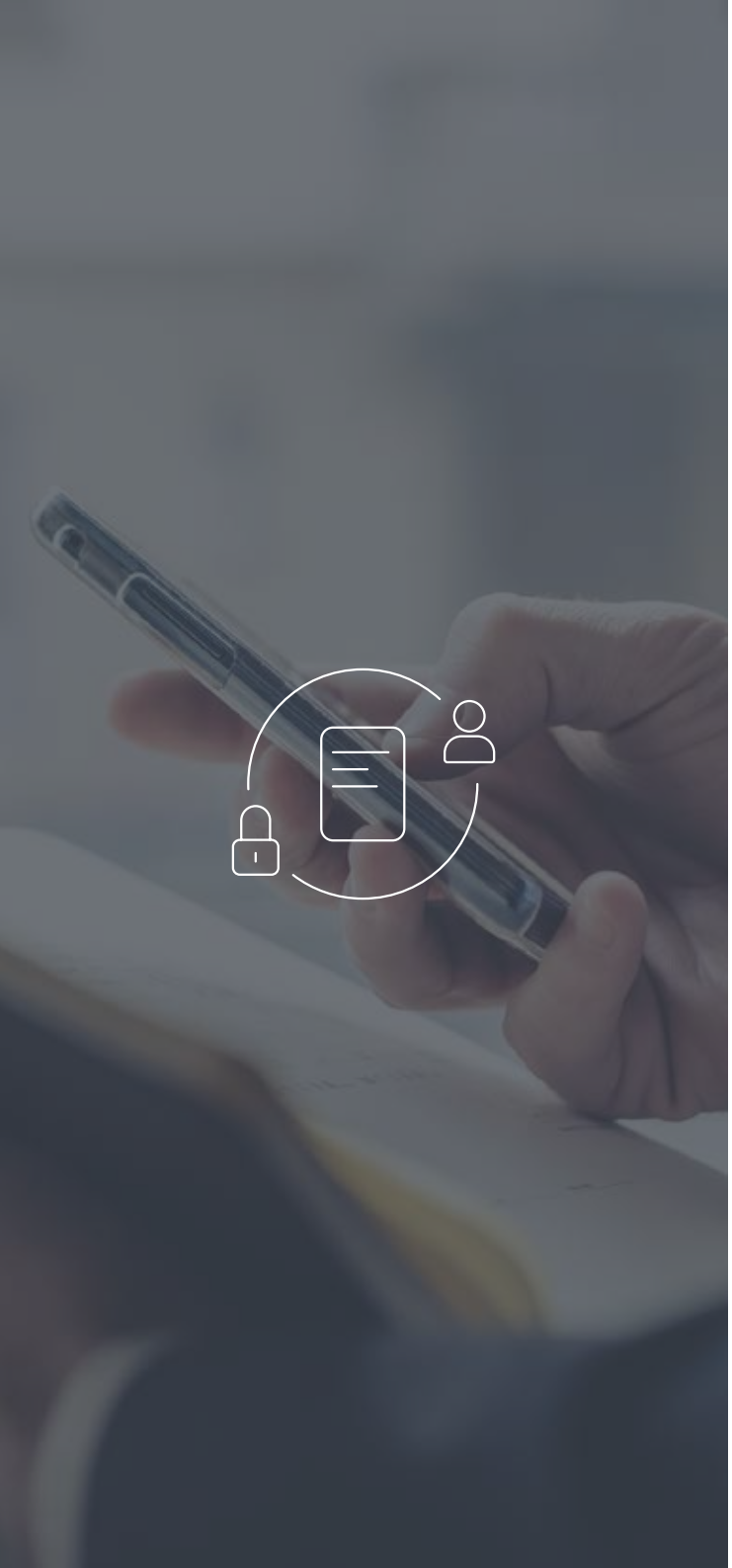


Figure 1. The **Panda Security Adaptive Defense Platform** protects organizations from cyber-threats, monitoring all application and process activity on workstations and servers. This comprehensive visibility allows **Advanced Reporting Tool** and **Panda Data Control** to provide value-added information in areas such as security, IT optimization, productivity control, as well as regulatory compliance.



3.A General Data Protection Regulation (GDPR)

What is it?

The GDPR is the European Union's data protection regulatory framework. Its objective is to give citizens back control over their personal data, imposing strict rules on its location, accessibility and processing. The GDPR will enter into force in May 2018.

Who does it affect?

The GDPR applies to all companies across all industries and regions, including those based outside the EU, which collect and store personal information about European citizens.

How can it affect my business?

Failure to comply with the GDPR may result in a fine of up to €20 million or 4 percent of an organization's global annual turnover. Not to mention the reputational damage that comes from a serious breach of personal information.

How does Panda Security help achieve regulatory compliance?

Below is a description of the GDPR articles that Panda Adaptive Defense and its modules help companies comply with.

Security of processing Article 32

Panda Adaptive Defense and **Panda Adaptive Defense 360**, protect organizations against any type of threat: from known, advanced and zero-day malware to ransomware, fileless (memory-based) and malwareless attacks. They use a security approach based on constantly monitoring application activity to make sure that only those applications trusted by Panda Security are allowed to run. This prevents the loss or theft of data across the network.

Additionally, Panda Data Control provides real-time discovery and monitoring of the personal and sensitive data files held on workstations and servers. This allows organizations to identify unauthorized access to personal data by employees and contractors.

Notification of a personal data breach to the supervisory authority. Article 33

Should a security breach or unknown process be detected on a company's workstations or servers, **Panda Adaptive Defense** and **Panda Adaptive Defense 360** will immediately notify the security administrator via email, detailing all activities carried out by the threat.

Additionally, in the event that a threat manages to run on the corporate network, Panda Adaptive Defense's dashboard will display the attack lifecycle, indicating whether data files were accessed and the actions taken on them (exfiltration, copy, etc.). This information can be easily exported to files, accessed on **Advanced Reporting Tool**, and integrated into the company's SIEM thanks to Panda Security's **SIEMFeeder** module.

Not only this, Panda Data Control's customizable, preconfigured reports will show the applications, operations and files related to any exfiltration incident affecting personal data: national identification numbers, phone numbers, addresses, first names, last names, etc. This information is critical when it comes to notifying a data breach.

Data protection impact assessment. Article 35

Panda Data Control enables organizations to discover the volume, type and use of the personal information residing on their network, so that they can assess the impact and risk of processing such data.

Tasks of the data protection officer (DPO). Article 39

Panda Data Control provides customizable, preconfigured dashboards and reports that meet the needs of DPOs, assisting them to carry out their duties and assess the impact of data protection efforts.

3.B Payment Card Industry Data Security Standard (PCI DSS)

What is it?

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards. It was set up to help businesses process card payments securely, reduce card fraud, and protect cardholder data.

Who does it affect?

The PCI DSS affects all users, banks and financial institutions that store, process or transmit cardholder data, generally in the retail sector (e-commerce platforms and merchants).

How can it affect my business?

Failure to comply with the PCI DSS may result in a fine of up to $500,00 per violation. Fines can be accumulated.

How does Panda Security help achieve regulatory compliance?

Panda Security helps organizations follow the best practices below in order to comply with the PCI DSS requirements:

Implement and keep your corporate systems and network secure

Panda Adaptive Defense and **Panda Adaptive Defense 360**, are advanced security solutions that protect organizations against any type of threat: from known, advanced and zero-day malware to ransomware, fileless (memory-based) and malwareless attacks.

Panda Adaptive Defense 360, includes a personal firewall, IPS/IDS, anti-spam protection, URL filtering and categorization, device control, plus other preventive security features aimed at controlling productivity and reducing the attack surface.

Protect cardholder data

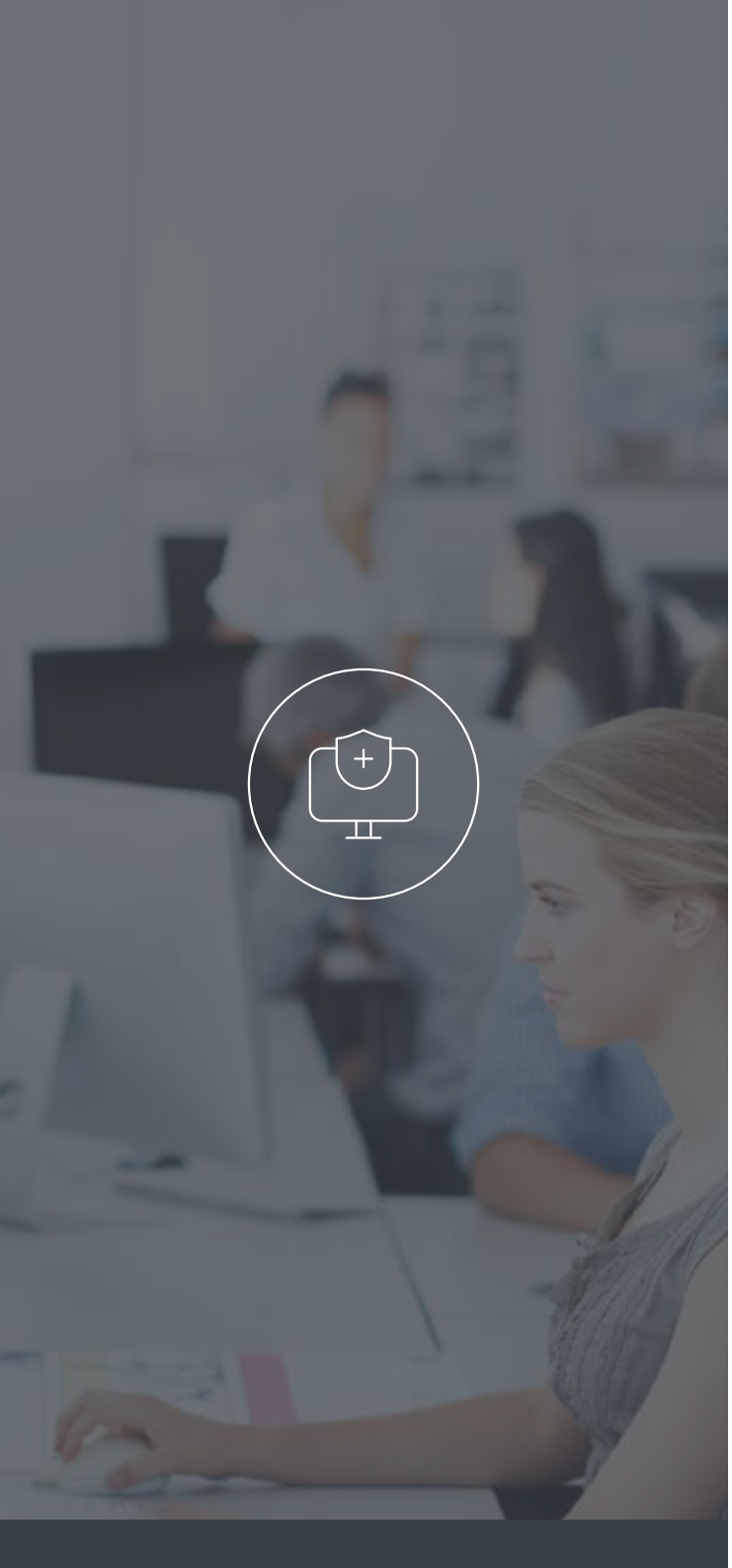
Panda Data Control finds the payment card and bank account data held in unstructured files on your workstations and servers, monitoring the actions taken on them at all times. This information is key to define and implement measures to control access to the personal data subject to the PCI DSS: cardholder, credit card and bank account information.

Implement a vulnerability management program

The fact that Panda Adaptive Defense and Panda Adaptive Defense 360 are continually monitoring the network allows the optional module **Advanced Reporting Tool** to generate reports about the vulnerable applications installed and run on all workstations and servers. This information helps IT and security teams perform their vulnerability management tasks effectively.

Implement strong access control measures

Panda Data Control monitors all access attempts and operations performed on files with payment card and bank account data. This information is presented via dashboards and preconfigured reports that can be tailored to each organization's needs.



3.C Health Insurance Portability and Accountability Act (HIPAA)

What is it?

The Health Insurance Portability and Accountability Act is a U.S. federal law that governs the privacy and security of the Protected Health Information, including electronic PHI (ePHI) stored, accessed or shared by companies in the healthcare or related industries, such as insurance companies processing medical records.

Companies operating outside the United States don't have to comply with the HIPAA rules. However, the European Union laws are very similar to the HIPAA Security and Privacy regulations, regulations, so these can be considered as standard guidelines of general application.

Who does it affect?

This regulation applies to healthcare providers, as well as any organization that stores or processes electronic protected health information, such as health insurance companies.

How can it affect my business?

Failure to comply with this regulation may result in fines of up to $1.5 million per year, loss of professional license, and even imprisonment.

How does Panda Security help achieve regulatory compliance?

Panda Security helps organizations follow the best practices below in order to comply with the HIPAA requirements:

Adaptive Defense and Adaptive Defense 360

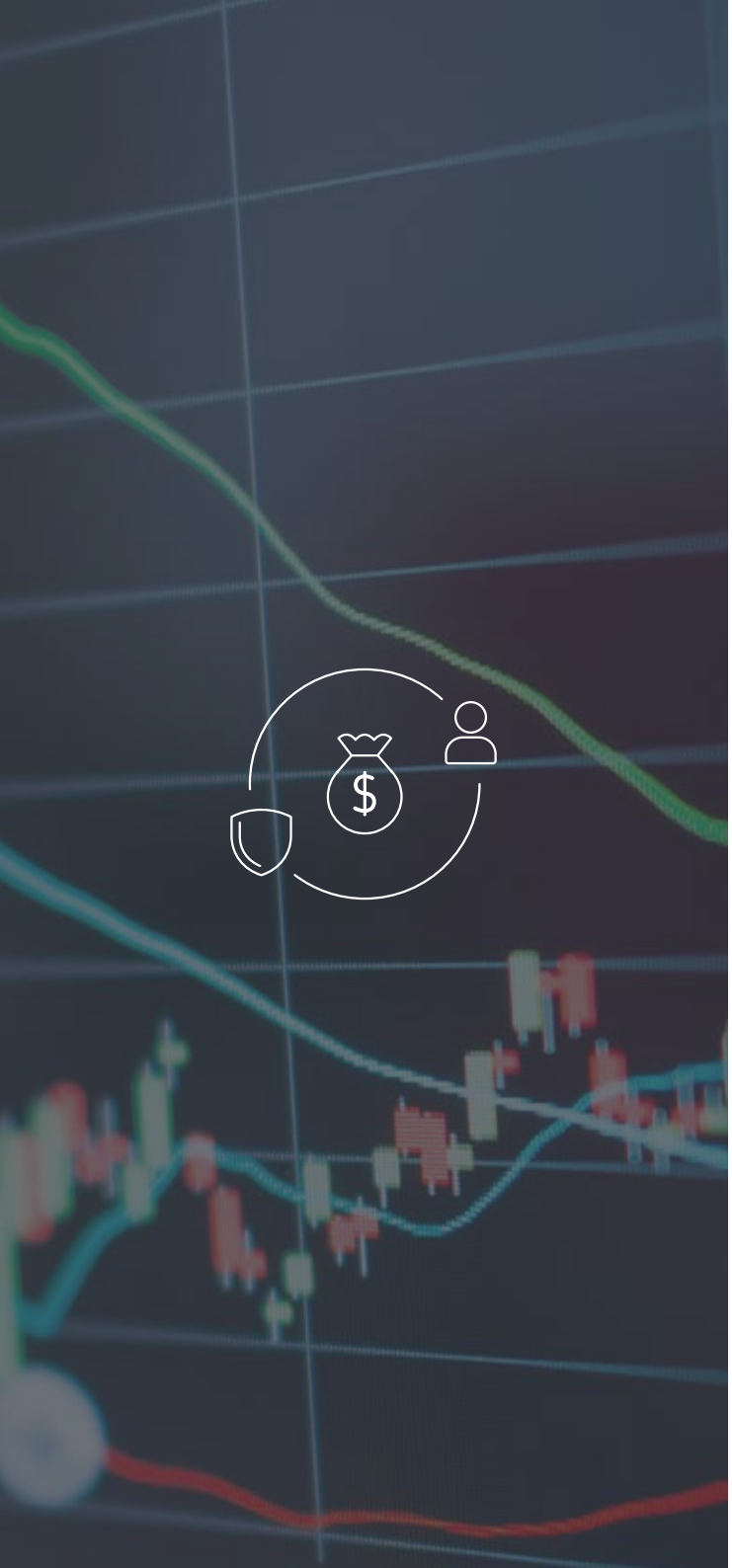
- Ensure the **confidentiality**, **integrity, and availability** of all electronic protected health information created, received, stored, or transmitted across the protected workstations and servers, safeguarding it against any known or unknown threat. Section 164.306
- Help **implement procedures to regularly review records** of information system activity, such as audit logs, access reports, and security incident tracking reports. Section 164.308
- Help implement procedures for guarding against, detecting, and reporting **malicious software**. Sections 164.308 (a) (5) (ii) (B)
- Prevent and mitigate security incidents with known and unknown malicious software, drastically reducing them to almost zero. Should malicious software manage to run, the behavior monitoring capabilities of both solutions will identify and block it, minimizing its effects. Sections 164.308(a) (6)(ii)
- Help implement **continuous monitoring mechanisms** of all applications and processes run on the organization's servers, workstations, and laptops, in order to document potential **security incidents** and their results. These mechanisms are typical Endpoint Detection & Response (EDR) security solutions. Section 164.312 (b)
- Provide **detailed information**, via the console and email notifications, regarding the actions taken by attackers during security incidents. This allows organizations to **fulfill the HIPAA requiremen**t to notify personal data breaches to the relevant authority, including who, when and how accessed the data subject to the regulation. 45 CFR 164.404 (b)

Advanced Reporting Tool and SIEMFeeder

- Help **manage vulnerabilities**, informing of the vulnerable applications installed and run across the organization. Section 164.308(a)(1)(ii)(B)
- Help identify and report anomalies by **keeping logs of all login attempts** to the protected workstations and servers. These log files are kept for up to one year. 45 CFR 164.308 (a) (6) (ii)

Panda Data Control

- Identifies **security incidents** involving protected data, indicating the affected file, its location, etc. This allows organizations to **identify attacks on files** with electronic protected health information and report security incidents as required by law. Section 164.404(b).
- Allows organizations to **identify access to electronic protected health information** by unauthorized employees and contractors, as well as to report irregularities as required by law. Section 164.404(b).



3.D Sarbanes-Oxley (SOX)

What is it?

A U.S. federal law that provides that debts arising from securities fraud are not dischargeable in bankruptcy, thus enhancing investor protection. This Act requires that affected organizations implement and monitor stringent internal controls to prevent disclosure of confidential data and accounting fraud.

The SOX was passed in 2002 as a response to the Enron scandal. Enron Creditors Recovery Corporation was one of the world's major electricity, natural gas, communications and pulp and paper companies before it bankrupted in 2001 due to irregular accounting procedures and fraud, affecting the lives of thousands of employees and shareholders.

Who does it affect?

The SOX Act affects all companies listed on the New York Stock Exchange (NYSE), and their subsidiaries. There are also a number of provisions of the Act that also apply to privately held companies, for example the willful destruction of evidence to impede a Federal investigation.

How can it affect my business?

Failure to comply with this regulation may result in fines of $5 million and 20 years in prison.

How does Panda Security help achieve regulatory compliance?

Below is a description of the SOX sections that Panda Adaptive Defense and its modules help companies comply with.

Section 404 - Management assessment of internal controls

Panda Adaptive Defense and **Panda Adaptive Defense 360** allow identification of the workstations and servers which are unprotected or have operational problems that may lead to protection failures. This enables organizations to establish internal controls to periodically review network status and mitigate risks.

Section 409 - Disclosure of changes in financial condition or operations

From a security point of view, **Panda Adaptive Defense 360, Advanced Reporting Tool** and **Panda Data Control,** report in real time on the security incidents whose execution is blocked. Additionally, should an attacker manage to take action such as introducing a persistent threat, accessing files, or executing lateral movements, they will provide detailed information on the attack, allowing organizations to fulfill the requirement to notify the relevant authority of who, when and how accessed protected data.

Section 802: Criminal penalties for altering documents

Panda Data Control monitors all create, edit, open, delete, rename, copy and paste operations performed on personal data files, enabling organizations to identify file alterations as well as who, when and how executed them.

1. **Panda Data Control** is available in the following countries: Spain, Germany, UK, France, Sweden, Italy, Portugal and Netherlands.

2. There are 18 specific types of electronic protected health information, including patient names, addresses, social security numbers, email addresses, fingerprints and photographic images. Any past or present medical record is subject to the same degree of protection.

More information at:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

Adaptive Defense 360

Limitless Visibility, Absolute Control

panda