Scrut Automation

The Crucial Role of a Security-First Approach in **Continuous Compliance**

Scrut Automation

Contents

Introduction

Compliance frameworks and regulations do their best to keep a company's data secure in an unpredictable threat landscape. However, achieving compliance in an increasingly complex and evolving landscape of regulations and security threats can be challenging for organizations.

That said, a compliance-focused approach often tends to fail in addressing the dynamic nature of security threats and falls short of providing adequate protection against emerging risks.

A much better alternative to this is the security-first approach. It tends to not only safeguard the data of an organization better but also results in an organization achieving compliance as a byproduct of its processes.

This ebook explores why a security-first approach is a surefire way for an organization to achieve and maintain compliance while prioritizing security and discusses how to go about implementing a security-first mindset within a company.

The Role of Compliance

Compliance refers to the act of adhering to rules, regulations, standards, and guidelines enforced by governing bodies, an industry, or internal policies. It is among the top priorities of organizations across industries in the digital era.

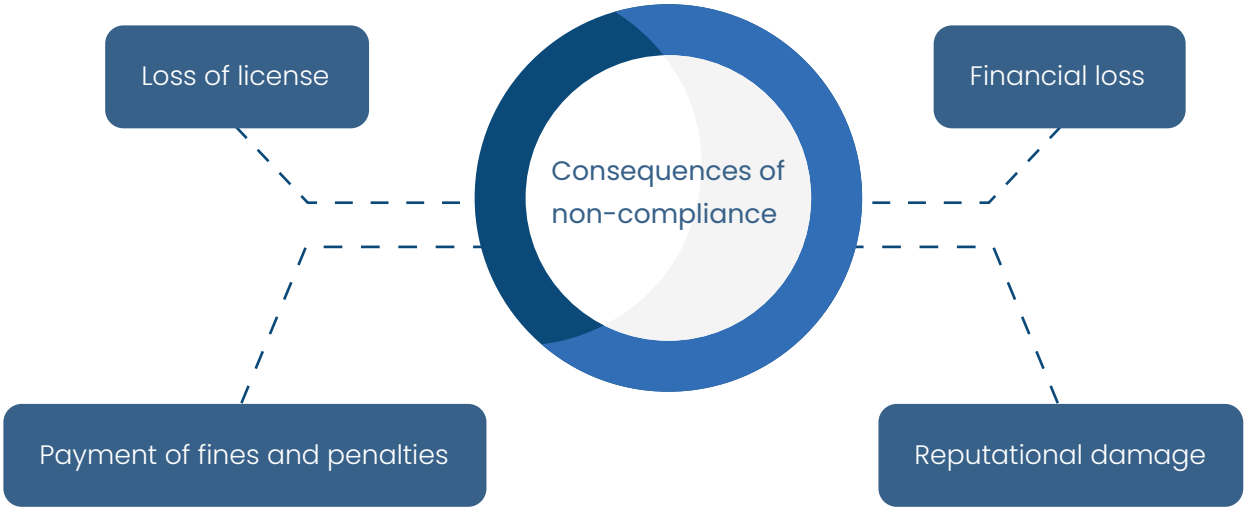
Every organization has different requirements to fulfill based on the industry it belongs to or the region it operates in. For instance, fintech companies follow PCI DSS, while organizations handling the data of EU residents adhere to GDPR

The need for compliance in the digital era

The digital era is rife with security risks, such as data breaches and cyber threats, and there is a constant need to secure sensitive data in an interconnected world. Rules and regulations are enforced by regulatory bodies in order to protect data.

The complexities associated with meeting these regulatory requirements increase as technology advances. Being compliant under such conditions requires a proactive approach to implementing robust security measures, conducting regular risk assessments, and adapting swiftly to changing compliance standards.

It is necessary to keep up with emerging compliance trends and ensure adherence to regulations to maintain the trust of customers and stakeholders in the digital age.



The evolving threat landscape

Cyber attacks are increasing in number and sophistication with each passing day, making the threat landscape hard to navigate.

> The threat landscape refers to all the potential and known threats that affect an organization or industry.

Regulatory bodies aim to help organizations protect themselves from these threats by prescribing guidelines that help safeguard their data.

Organizations, in turn, are required to boost their compliance efforts to cover new and emerging cybersecurity risks. Unfortunately, following compliance processes alone is not enough when it comes to surviving the modern threat landscape.

There is, hence, a need for a more security-focused approach in order to prevent and mitigate these threats and maintain both security and compliance.

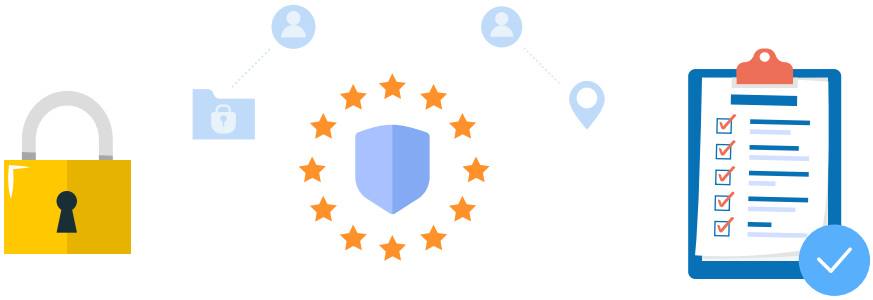
Security and Compliance

Both, compliance and security, play an important role in protecting the data of an organization. Security refers to the efforts made by an organization to protect its data from being accessed, modified, stolen, damaged, or leaked by unauthorized elements.

Compliance, on the other hand, refers to the efforts made by an organization to adhere to laws and regulations that aim to protect its data.

The two are often confused with one another since they both center around securing data and protecting the privacy of an organization.

It is important to understand the differences between them in order to appreciate why they are both important for an organization's safety.



- Constant monitoring
- Threat detection
- Security controls
- Risk management

- Regulatory requirements
- Industry standards
- Security standards
- Business optics

The differences between compliance and security

Some important differences between compliance and security are listed below to help understand their roles better.

Area of difference	Compliance	Security
Focus	Compliance focuses on adhering to required laws, standards, and guidelines for security that are imposed by an external body.	Security focuses mainly on safeguarding systems, networks, data, and assets from unauthorized access, leaks, modification, or destruction. It involves enforcing security measures, controls, and practices to prevent, resolve, and mitigate risks and vulnerabilities.
Approach	Compliance is often a reactive approach, as its basic goal is to fulfill the requirements that are laid out by governing bodies and pass audits.	Security employs a proactive approach by identifying and mitigating vulnerabilities before they can be exploited.
Scope	Compliance focuses on meeting the requirements prescribed by laws, regulations, and standards. Compliance involves activities such as collecting evidence and preparing for audits and assessments, and attaining certifications to demonstrate adherence to standards and regulations.	The gamut of security includes practices that protect information and assets from various risks and threats. It includes technical controls, physical security measures, incident response plans, security awareness training, and constant monitoring and assessment of security posture.

Area of difference	Compliance	Security
Urgency	Compliance is a constant effort since requirements have to be fulfilled consistently and evidence for the same has to be gathered to be produced at audits. However, companies are given time to prepare for these audits. This makes compliance a less pressing need.	Security is a constant effort, as security threats can strike at any time. There is always an urgent need for security.
Effect of poor implementation	When an organization is non-compliant, it runs the risk of being fined and losing its reputation. It may even result in a loss of license. Customers and stakeholders are likely to avoid doing business with a company that is non-compliant.	A company with a poor security posture is exposed to the dangers of cyber attacks, data breaches, and various security threats. These attacks have the potential to disrupt business operations, causing significant downtime and financial losses. They can result in data loss and compromise the integrity of devices and systems. A data breach not only results in the loss of sensitive information but also diminishes the trust and confidence of customers and stakeholders.

Why security is more effective when it comes to safety

The ever-evolving nature of the threat landscape renders compliance standards outdated as soon as they are established. Though these standards are updated periodically with the intention to protect companies from security risks, the time taken to develop and update them is enough for several new security threats to crop up. It can sometimes take several years for compliance standards to be updated.

This delay enables security threats to take advantage of outdated measures that were designed to combat older threats.

Security takes a more proactive approach that involves constantly devising new ways to deal with potential risks. It employs measures that take into consideration the evolving nature of cyber threats. Practices such as constant monitoring of cyber assets, regular vulnerability testing, constant security posture assessment, and implementing the best security tools make the security approach better equipped to deal with the modern-day threat landscape.

Though security and compliance are not the same, they are closely connected.

Compliance frameworks prescribe security requirements, and proper security measures are necessary for achieving compliance. Organizations have to implement effective security practices that fulfill more than compliance requirements in order to prevent and mitigate threats and protect data.

Correlation between security-first approach and continuous compliance

Pitfalls of a compliance-first approach

Since compliance frameworks aim to help make an organization secure, some companies assume that fulfilling compliance requirements alone can guarantee adequate security. But that's not the case. Here are some reasons why putting compliance first could jeopardize an organization's safety.

The organization is audit-ready, not attacker-ready

When a company follows a compliance-first approach, it tends to devote all its time and resources to passing compliance audits. Though fulfilling compliance requirements does result in a certain level of security, it in itself is not enough to make the company attacker-ready. For an organization to be adequately secure, it requires up-to-date security practices and tools, which won't be accomplished through compliance only.

Cybercriminals can exploit vulnerabilities

Compliance requirements are not a secret, so attackers know exactly what security measures an organization that puts compliance first carries out. This makes it easy for them to know where its vulnerabilities lie. Attacking such companies is a walk in the park for cybercriminals.

The security team is underutilized

An organization that puts compliance first tends to underutilize its security team. Team members are made to focus their energies on carrying out mundane compliance tasks instead of carrying out activities that effectively prevent and mitigate security threats.

Inefficient security practices are carried out

Since compliance standards are obsolete the moment they are prescribed thanks to the ever-evolving nature of security threats, there is no compliance framework that can guarantee total security. Compliance frameworks do prescribe useful security measures, but they are not intuitive enough to combat new and innovative security threats.

The Benefits of a Security-First Approach

When a company follows a security-first approach, it weaves security into every process that it carries out at every level. It constantly seeks ways to innovate security measures to one-up cyber-criminals and employs an effective set of practices that help prevent, monitor, and tackle security threats. The benefits of this approach are listed below.

Proactively identifies and mitigates threats

A company that follows a security-first approach focuses primarily on proactively identifying and mitigating potential threats before they can cause damage. Implementing robust security measures helps organizations to detect and resolve vulnerabilities, prevent attacks, and mitigate the impact of security incidents.

Strengthens security posture

A security-first approach implements multiple measures that aim at covering all bases of cybersecurity. Practices such as network security, endpoint protection, access controls, encryption, and employee awareness training make it a comprehensive approach to protecting data. It predicts the course of security threats and takes precautionary measures to mitigate their impact.

Tackles emerging threats

Organizations that follow a security-first approach constantly update their security measures in order to tackle emerging security threats. Since security threats keep increasing in number and sophistication, a good security program will adapt its security measures to deal with them effectively. Prioritizing security helps organizations to respond better to emerging threats and protect against evolving risks.

Creates security awareness

An alarming number of security breaches are caused unwittingly by the employees of an organization. A company that puts security first ensures that its employees are made aware of security risks by conducting security awareness training. This helps employees to avoid clicking on suspicious links and compromising sensitive data. A security-first approach promotes careful behavior across an organization.

Increases customer trust

When an organization prioritizes security, it prevents the likelihood of security breaches and safeguards sensitive data. This increases the trust of customers, partners, and stakeholders. A security-first approach protects the reputation of a company and keeps its customers satisfied.

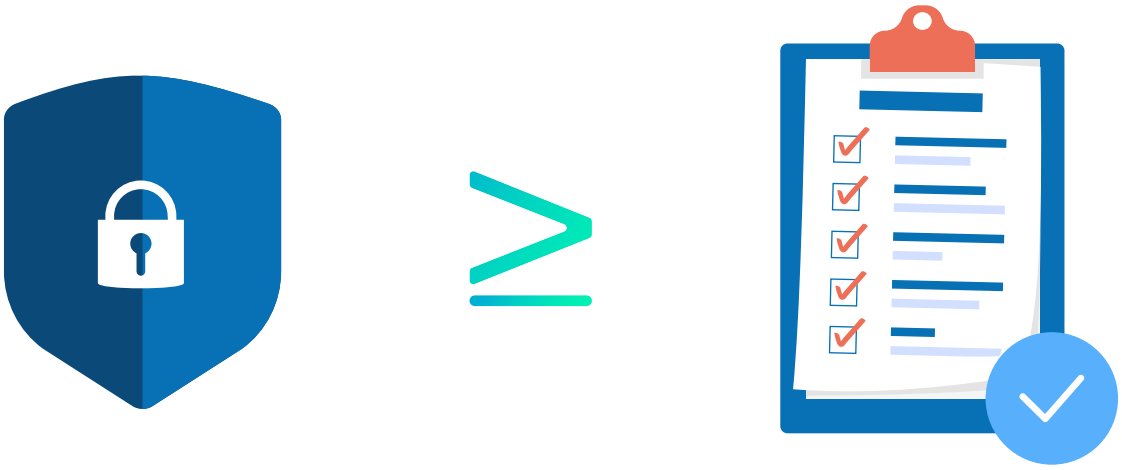
Prevents financial loss

Security breaches not only leak sensitive information but also result in financial loss. Organizations are fined large amounts of money, and they may also be forced to shut down for a few days in order to recover. which can be brutal for any firm. Investing in comprehensive security measures can, therefore, lead to long-term cost savings.

How a security-first approach results in compliance

The goal of a compliance framework is to ensure that an organization is secure in order to prevent data breaches. It prescribes actionable steps to help companies prevent security incidents. However, compliance efforts only fulfill the bare minimum of security requirements, and many organizations take them up just to pass audits. Hence, when an organization follows a compliance-first approach, it lacks adequate security.

On the other hand, when an organization follows a security-first approach it establishes a strong foundation of security practices that go above and beyond regulatory requirements and industry standards. Such organizations end up being compliant automatically as a result of their robust security posture.



Here are some reasons why a security-first approach leads to compliance.

Efficient risk management

Compliance standards expect organizations to protect their data. This requires effective risk management. A security-first approach assesses and manages risks continuously. It identifies potential vulnerabilities and threats and implements security measures to mitigate their impact. A security-first approach's proactive risk management enables organizations to meet compliance requirements involving risk assessment with ease.

Use of security controls

A security-first approach implements effective security controls. These controls protect systems, networks, and data from unauthorized access, data breaches, and other security incidents. Compliance frameworks and regulations require the implementation of specific security controls. A security-first organization will not only have these security controls in place but also implement other effective controls that combat more sophisticated security threats.

Continuous monitoring and incident response

An organization that follows a security-first approach continuously monitors its systems, networks, and data. It also uses tools and technologies to detect and respond to security incidents promptly. This results in the organization automatically adhering to compliance requirements that require continuous monitoring and timely incident reporting.

Up-to-date systems

Keeping software, applications, and systems up to date with the latest security patches and updates is an important part of a security-first approach. This helps in dealing with any vulnerabilities in the system and protecting it against emerging threats. Some compliance frameworks call for patch management, so a security-first organization will fulfill this requirement.

Security Awareness

Compliance frameworks prescribe security awareness training as an important security measure. Security-first organizations conduct regular training programs to raise the security awareness of their employees. This not only results in the organization adhering to the compliance requirement, but it also prevents any untoward incident caused by an employee's negligence.

Regular audits and assessments

Security-first organizations regularly conduct internal audits and assessments to evaluate their security posture. Any vulnerabilities are addressed, and steps are taken to further improve cybersecurity. These regular assessments help an organization pass compliance audits without any hassle and ensure continuous compliance with regulations by being consistently secure.

Strategies for Implementing a Security-First Mindset

How to carry out a security-first approach

For an organization to follow a security-first approach, it has to embed security measures into all its operations and decisions. When security is made a priority, it not only fulfills compliance requirements, but it also enables the success of other business objectives. Here are some ways in which an organization can implement a security-first mindset.

Develop a comprehensive security strategy

A security strategy outlines all the steps an organization has to take to protect its digital assets from security threats. From identifying and resolving vulnerabilities in its system to implementing controls and measures to prevent, detect, and respond to cyberattacks, a good security strategy makes sure to cover all bases.

Document security policies and procedures

Having security processes and policies in writing provides clarity to employees across an organization and helps in reinforcing a security-first mindset. It also prevents confusion regarding security practices. The documents should explain in simple terms how security threats can be prevented and provide actionable steps that are to be followed in case of a security incident.

Implement effective security controls

A security-first organization should have in place technical controls, physical controls, and administrative controls in order to maintain security. Technical controls include practices that protect data from unauthorized users such as data encryption, while administrative controls include security practices that influence the behavior of employees such as security awareness training programs, and physical controls include things that deny entry to unauthorized personnel like identity cards and fingerprint scanners

Use automation tools

Using automation tools eases the burden on the security team and frees up their time to innovate better security solutions.

Quick incident response and round-the-clock monitoring make automation a handy tool to combat security threats. The use of automation tools is a vital part of any security-first organization today.

Conduct regular security assessments and audits

Security-first organizations regularly assess their security posture through internal audits and assessments. Any vulnerabilities in the system are addressed and security practices are updated regularly to keep pace with ever-evolving security threats. This practice of regularly assessing their security posture makes security-first organizations resilient to cyber threats.

Conclusion

A security-first approach naturally results in compliance, as the goal of both processes is to protect digital assets. When organizations prioritize security they align with compliance standards by ensuring the safety of sensitive data.

A compliance framework is like a basic guide to security. Any security-first organization would cover most compliance standards in its security program. Practices such as risk management, implementation of security controls, incident response, or security awareness training, which are recommended by regulatory bodies, are carried out by security-first organizations consistently, fulfilling both security and compliance requirements.

Security-first organizations are defined by their constant monitoring of assets, internal assessments, and threat detection, which helps them navigate both evolving threats as well as emerging compliance standards.

To conclude, when an organization invests in security it saves money in the long run by preventing security incidents and non-compliance. Security-first organizations ensure that they do their best when it comes to maintaining both security and compliance. One of the most effective ways they do this is by using automation tools such as Scrut.

Scrut automates all the tedious parts of the compliance process such as the gathering of evidence and mapping of controls, and it speeds up audits. It also helps organizations monitor their assets around the clock and detect vulnerabilities.

Schedule a demo today if you would like to streamline and simplify compliance and security processes in your organization.