4 Data Security Best Practices for Maintaining Compliance with Data Security Laws
Executive Summary

Maintaining compliance with the many regulations mandating the security of private data is likely top-of-mind in most boardrooms these days. Given the well-publicized and record-setting pace of regulatory compliance violations in recent years, that is a very appropriate mindset. Every organization should embrace their responsibility to protect the data privacy of users and customers. And every organization should be cognizant of the threat that accompanies the failure to fulfill this responsibility.

Protecting users, applications and private data is the fundamental focus in maintaining compliance with data security regulations. This paper discusses four best-practice approaches that any organization can adopt for achieving and maintaining compliance with the ever-increasing, ever-more-powerful government privacy laws and data security regulations.

There’s plenty of evidence to indicate that many organizations are falling short in their regulatory compliance efforts. Financial institutions have been fined hundreds of billions of dollars for security compliance failures.¹ Healthcare organizations were fined more for HIPAA compliance violations in 2018 than in any previous year.² And the recently enacted General Data Protection Regulation (GDPR) generated tens of thousands of security compliance failures in less than a year’s time.³

Why do so many organizations struggle so mightily — and fail so consistently — to meet and maintain compliance standards? Quite simply, these organizations have gaps in their data security standards that continue to go undiscovered and unaddressed.

Though the specific security gap failures can vary from company to company, any enterprise can find and eliminate security gaps by implementing the following four processes detailed in this paper:

1. Enhancing the enforcement of security compliance policies by holistically addressing risks to users, applications and data
2. Using discovery tools to understand external threats and sensitive data classes subject to compliance mandates
3. Strengthening user protection by applying identity and data-centric controls to users and data
4. Hardening application security and enabling privacy by design

Enhancing the Enforcement of Security Compliance Policies

The organization-wide enforcement of security policies is best accomplished with a holistic approach to addressing risks to users, applications and data. A holistic approach to security should involve mastering the basics of security monitoring, breach detection, and incident escalation and response. Organizations can then build on these basics by leveraging advanced data science, analytics and shared intelligence. These advanced methodologies can be useful in finding and eliminating the security gaps that can pose threats to maintaining compliance standards.

Occurrences of cybercrime are always escalating. The annual creation of new applications is accelerating year over year. Given these factors, along with the massive expansion of the quantities of data generated and stored, only a holistic approach can provide an adequate cybersecurity defense against potential threat vectors.

Using Discovery Tools for Revealing Compliance Threats

Complying with government mandates for the protection of data requires understanding which data is most sensitive and where the threats are most likely to manifest. Tools that can be used in discovering and classifying the risk to your organization’s data can be invaluable in countering those compliance threats. Tools can also be used to automate the identification and securing of the personal information (of customers or users) that is most likely to be targeted by cybercriminals.

Security discovery and monitoring tools can also help to reveal application vulnerabilities and can monitor for occurrences of unauthorized access and changes to data. But not all security vulnerabilities stem from instances of unauthorized access. Security lapses and compliance violations frequently occur when privileged users perform unauthorized actions that compromise applications or data. Tools can help to guard against threats from both unauthorized and authorized users.

Applying Data-Centric Controls

Data security is about protecting data throughout its entire lifecycle without exposing the data to high-risk, high-threat environments. From the point of initial capture of data through all movement within an enterprise environment, a data-centric approach works to assure the security of data — and the users of that data — at every step by embedding protection within the data itself.

A data-centric approach to security is becoming increasingly essential. The exponential increase in the sheer volume of data, along with the disparate data types in use within most enterprises, makes a data-centric approach the best approach to bolstering data security.
A data-centric approach to security can include:

- **Format-Preserving Encryption**: A new approach to encrypting structured data that integrates datatype-agnostic encryption into legacy business application frameworks without altering the data format.

- **Page-Integrated Encryption**: Encryption of sensitive user data and increases the security of e-commerce platforms.

- **Stateless Key Management**: Secure, adaptable and extensible enterprise key management.

- **Stateless Tokenization**: Advanced data security without token databases, dramatically improving speed, scalability, security and manageability over conventional, first-generation, and PCI DDS tokenization solutions.

The privacy and compliance benefits that may result from a data-centric security approach can include:

- Simplified audit and protection capabilities within a single governance framework
- Enhanced compliance with specific governmental regulations and legislation such as HIPAA and GDPR
- The protection of data streamed from IoT devices and sensors
- The implementation of end-to-end data protection for both iOS and Android applications
- The safeguarding of credit card data and payment transactions

Deploying a data-centric approach to security can protect users and data across enterprise, cloud, mobile and big data environments. A data-centric approach can provide the kind of protection that modern enterprises require in achieving and maintaining security compliance standards.

### Privacy by Design and Hardening Applications

Many of the government regulations, such as GDPR, that are driving compliance requirements embrace the privacy of personal data as a fundamental human right. And, in turn, organizations that fail to protect the privacy of personal data will fail to maintain compliance with these regulations.

The need to maintain compliance with laws such as GDPR is driving the widespread adoption of a software development concept generally labelled as ‘privacy by design.’ According to Deloitte, “Privacy by design holds that organizations need to consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that
involve processing personal data.” Deloitte also notes that “The GDPR requires organizations to consider privacy at the earliest stage.”

Implementing privacy by design into the development process can be assured by adhering to the following best-practice architectural considerations:

- Architect data processing systems so that they only process the minimum amount of personal data necessary to achieve their design objectives
- To the extent possible, limit the data types and volumes of personal data that is collected and processed
- Limit the number of times personal data is processed, the number of people that handle the data, and the length of time the data is retained and stored

An additional approach to strengthening security compliance is to integrate application security into the DevOps process. According to Gartner: “The goal should be to deliver more secure code at the speed of business, rather than to patch or replace code reactively based on manual reviews or in response to breaches. In this way you can avoid wasteful rework, which contributes to the business falling behind competitors.”

Compliance Requirements Won’t Get Any Easier

As noted above, many companies around the world are struggling to maintain regulatory compliance. And many companies are stumbling in their attempts to achieve and maintain compliance. With billions of dollars in fines levied in recent years, it’s apparent that many companies have made little progress in their struggle for compliance.

The bad news is that the struggle is only going to become more difficult.

Though GDPR is the newest law mandating standards in the handling of private data, more laws are likely to soon follow. One example is the California Consumer Privacy Act (CCPA), scheduled for implementation in 2020. These new laws may represent somewhat of a moving target for companies trying to get compliant. As reported in an Information Week article, “The act isn’t set in stone because it could be amended as the result of midterm elections. Alternatively, it could be preempted by a federal equivalent.”

How can organizations even hope to remain compliant with the onslaught of new and yet-to-be-enacted government regulations?

---

5 https://techbeacon.com/devops/5-ways-align-security-your-devops-strategy

---
A comprehensive approach, based on implementing all the data security best-practice recommendations discussed in this paper, will provide a firm foundation for complying with both current and future laws regarding data security. This approach will best position any enterprise for complying with the many laws that have been, and will be, enacted by local, national and multinational governments.

Contact us today to learn more about how Micro Focus products can assist your organization in implementing the above four best practice recommendations for achieving and maintaining data security compliance.

Micro Focus offers decades of industry-leading information archiving experience, and currently manages the world’s largest secure private cloud. Selected by Forrester and Radicati as an archiving leader, Micro Focus offers information archiving services to both regulated and unregulated businesses.