TechTarget | Custom Media
White Paper

Regulatory Compliance Is Irrelevant... Or Is It?

Compliance with global regulations like the European Union's GDPR has received a lot of ink, but there's a wealth of other reasons to invest in your enterprise's data security program. For many enterprises, such efforts need to include the mainframe. Understand the goals of a robust security strategy, and address top data security challenges by leveraging four key principles for demonstrating continuous compliance and achieving a dynamic state of data security.

ca technologies

Enterprises worldwide are scrambling to rebuild digital trust with their customers, prospects and even partners. Cyberattacks have become more sophisticated, threat vectors have expanded, and attackers are learning to collaborate and share successful tactics to penetrate existing defenses. Not surprisingly, this has pushed IT and security enterprises to devote more resources and attention to security in general and to the increasing number of regulatory compliance initiatives.

Though compliance with the European Union's Global Data Protection Regulation (GDPR) may be at the top of that list, it is far from the only priority item. High-profile regulatory initiatives such as the EU's Network and Information Security (NIS) Directive, the New York State Department of Financial Services regulation and Singapore's Cybersecurity Act also play a considerable role in many enterprises' data security strategies.

But the reality for enterprise executives—including board members—is this: **Compliance shouldn't really be the focus. In fact, compliance may be the lowest common denominator for security and IT professionals.**

Complying with the litany of security regulations is a proxy for the bigger opportunities at stake here: improving customer trust, enhancing brand reputation and avoiding expensive fines and downtime through smarter solutions.

Don't get us wrong. Ensuring compliance with regulatory initiatives such as GDPR is a big deal. The potential financial penalties alone are substantial enough to make enterprises pay attention—and take action. But remember: Passing a compliance audit is a point-in-time event. Your enterprise can be compliant one day and in violation the next.

This means that enterprises need to do more than just adhere to "checklist compliance." Instead, businesses today need to implement ongoing management, monitoring and maintenance of regulatory issues, as well as stay on top of the security space and ahead of new hacking techniques. A simple mistake, like sharing a credential, can have a devastating impact. **And on the other side, true compliance can lead to better business delivery.**

The solution: Your enterprise needs to adopt smart processes, properly train personnel and implement automated tools to ensure that all data—from intellectual property to personally identifiable information—is secure, always available and retains the highest level of integrity. If you do that, compliance will be a natural byproduct. If you don't, all bets are off.

Enterprises that depend heavily on the mainframe for their compute infrastructure especially—whether it is the core of on-premise IT or part of a complex hybrid architecture—need to understand how to truly demonstrate compliance and improve security cross-platform. After all, there is no greater concentration of sensitive and regulated data than what's living on the mainframe, making it a prime target for internal and external attackers. **Put another way, with mainframes, it is critical that the level of data security match the level of data exposure risk.**

What Do Data Security and the Mainframe Have In Common?

They should both be top of mind for enterprises trying to succeed in today's digital environment.

The mainframe has been at the heart of most enterprises' compute, storage and data infrastructure for decades. And despite the fact that much has changed over the years, many still maintain the belief that the mainframe is impenetrable. As a result, **enterprises fail to properly address security risks on the mainframe with the same urgency they do other platforms.**

The mainframe has long been regarded as an essential, run-the-business asset. However, because of its tenure, mainframe data has often been forgotten, abandoned or lost—unlike on other systems that have had shorter lifespans within the enterprise—and may not be as well understood.

In addition, mainframes are no longer isolated from other parts of an enterprise's overall digital ecosystem. Application connectivity between and among mainframes and distributed systems around the world has dramatically increased attack vectors. Also, with important developments such as BYOD, public cloud services and the Internet of Things now part of most enterprises' core business activities, **mainframes may be at risk now more than ever—making it critical that smart, adaptive and automated defenses are in place.**

In regulatory-speak, that means the mainframe needs to be at the heart of security defenses focused on identity protection and authentication. And this centrality of the mainframe in regulatory compliance and security on the whole is only going to grow as more data is exposed through unmanaged endpoints and unsecured network connections.

In short, your lines of defense must be drawn where the data resides—and that's on the mainframe.

Top Challenges Any Enterprise Must Overcome to Achieve Actionable Data Security

From a regulatory perspective, mandates like GDPR have received massive amounts of media coverage and generated a lot of executive discussion around privacy and compliance requirements.

That said, it's important to look at regulations from a holistic perspective, rather than viewing them as just a way to ensure personally identifiable information is protected.

Of course, GDPR violations carry the threat of substantial financial penalties—as much as 4% of annual gross revenue or 20 million euros, whichever is greater. But with a few exceptions, GDPR is not a particularly prescriptive statute. In fact, many say it is intentionally vague, leaving it up to enterprises to both interpret and comply with the regulation.

But regulatory requirements are just one angle to consider. The broader implications on enterprises' day-to-day security and systems of data protection are substantial, because **simply passing an annual regulatory audit does not mean the enterprise's most important data is safe, secure and available.**

There are many more challenges beyond compliance, including the very nature of the data itself—increasingly unstructured, often shared across applications, and collected and organized in multiple ways—that make it more difficult than ever to identify and understand the existing gaps and vulnerabilities.

Take one of the most common forms of personal identification: driver's license numbers. That multi-digit number, in and of itself, is an innocent string of digits. But combine it with other data—name, home address, bank account numbers and more—and the driver's license number becomes toxic.

Or, consider first names. Sofia, Wolfgang, David. Seems simple enough to find, right? The reality is: not so much. There is no inherent mathematical function that can be used to find names in a data set—that is, unless you leverage adaptive dictionaries customized to the language or configure and teach machine learning algorithms how to recognize a name.

In the end, the idea of giving consumers more control over their personal data is, of course, laudable. However, the execution is complex and demanding in its precision. **Whether you're talking about the regulatory demands of GDPR and other compliance mandates or protecting mission-critical data, the task is simply too large and too important to address with one-and-done legacy approaches driven primarily by manual efforts.**

IT and security professionals are going to formulate their defense strategies based, in large part, on regulatory demands, but at the end of the day, it is not enough to follow the rules established by legislators. **It is up to IT and security leaders, in close collaboration with business executives, to clear a path toward universal, continuous security.**

4 Best Practices for Superior Mainframe Security—Above and Beyond Compliance

There are many steps enterprises can and should take to ensure that their mainframe security is more than equal to the extant threat vectors and regulatory requirements.

Grow your mainframe value by focusing on these four areas:

1. **Find and identify your data, understand the risk, and manage data handling and storage.** The vast majority of data residing on the mainframe is unstructured—files, video and other non-traditional data formats—and sits "below the surface," making it harder to find and categorize. Knowing where your data is located is the first step toward assessing your risk posture, particularly when ensuring alignment of data risk with enterprise limits on business risk. How much data exposure are you willing to have? Once you have a thorough understanding of your data, it becomes easier for IT and security teams to manage how that data is handled and stored, to demonstrate compliance and establish safeguards for disaster recovery and business continuity, and to make critical business decisions based on those insights.
2. **Identify the criticality of each data point to compliance, governance and business concerns, and classify it based on sensitivity level.** Mainframes today host a wealth of data, increasing the complexity of achieving comprehensive data protection and security. Not to mention that the mainframe has been around for 50-plus years and, let's be honest, data protocols are often neglected—with undocumented data or lost, hidden or abandoned data—making it nearly impossible to organize your systems. Obviously, all this data must be evaluated to determine its priority for compliance, governance and ongoing operational security. Photos taken for a promotional campaign are certainly important to the marketing department, but they don't hold the same criticality as intellectual property documents or customers' personal data. Enterprises' approach to protecting these different types of data needs to be applied in a manner commensurate with their importance and priority.

3. **Determine proper and appropriate access rights, and manage access to relevant data.** With so many people creating data through a wider array of both corporate-owned and personal devices, applications and services, it has become increasingly more challenging to maintain access to the data, assign authority and privileges to each user, and manage appropriate levels of access on an ongoing basis. But this is a critical aspect in ensuring security and demonstrating compliance. Roles and rights are fluid in most enterprises: People can be promoted, take on new responsibilities, and work on ad hoc or temporary projects with different groups, but be walled off from data sets outside of their scope of responsibilities. This constant change means that access management must be flexible depending on people's changing roles and rights.
4. **Monitor and record privileged access against data compliance policies.** Your systems need to have automated audit trails that easily and quickly identify who has attempted to access what data and where that data has moved. At this level of monitoring—sensitive data accessed in one source file among hundreds of data sets—manual discovery and management cannot be done reliably, quickly or in accordance with governance policies.

Digital Trust, Data Security and Revenue Are Closely Tied

With its rise in prominence in the regulatory eye, the security space is experiencing a skills shortage, and budgets are always trending low. With both IT and security budgets and staffing constantly under pressure, it becomes increasingly difficult for enterprises to go it alone when it comes to developing the right security framework and implementing the right solutions for automation, intelligence and flexibility.

On the other hand, how do you trust an external software vendor with securing your most sensitive, mission-essential data? Most enterprise decision-makers are paying attention to regulatory compliance as a driver of digital trust—and for good reason. **But digital trust isn't strictly synonymous with regulatory compliance.** It extends to customer experience, brand reputation, due diligence of third-party vendors and, by extension, revenue.

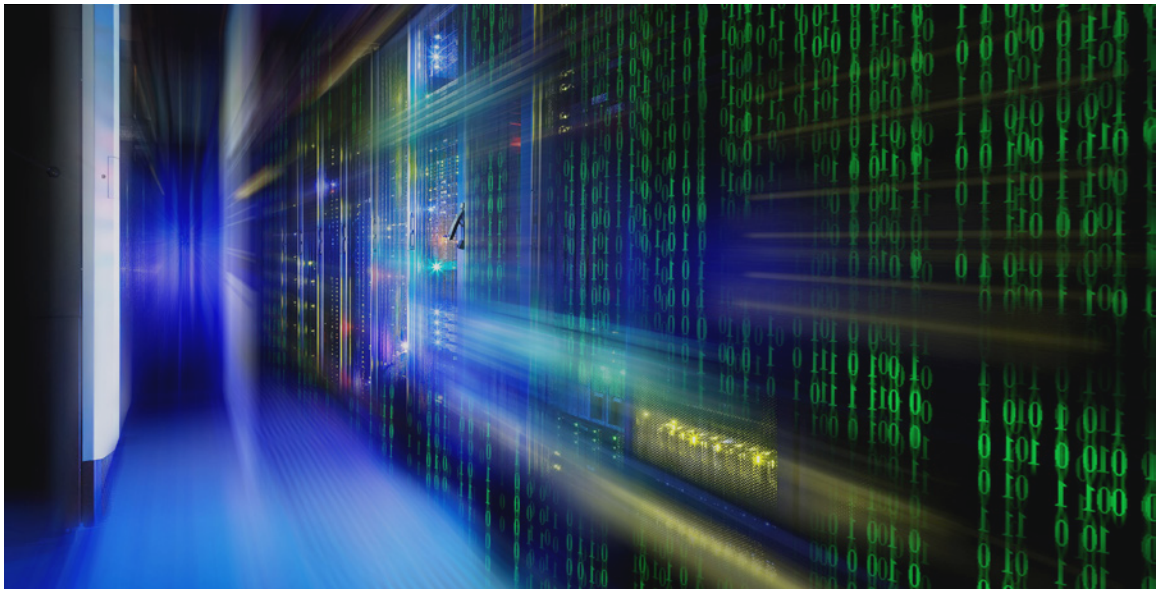
After all, the result of digital trust is success in terms of the bottom line.

And partnering with a proven, dependable mainframe security provider, one with decades of hands-on experience and state-of-the-art tools, is part of that. Enterprises must trust that vendor solutions work, and work accurately all the time, for truly enhanced data security that leads to greater digital trust.

CA Technologies, for example, has been a leader in mainframe software for decades. It has built a reputation for reliable and flexible enterprise security tools, including its ability to handle expanding and transforming workloads, stay on the leading edge of a wide range of compliance mandates and understand how to protect mainframe data in the data center, on the network's edge or in the cloud.

And building the level of digital trust essential in today's IT-driven business climate requires modern tools that reflect the criticality of mainframe data and the complex ways in which that data is stored, managed and accessed—tools for data discovery, trusted access management, mainframe security management and more:

- Privileged access management solutions such as **CA Trusted Access Manager for Z**—built for IBM z/OS environments—leverage the wide and deep knowledge of experienced mainframe IT and security professionals to assess and manage access rights to critical data. CA Trusted Access Manager for Z eliminates the need for shared privilege credentials, aligns with existing security workflows, operates 100% on the mainframe and delivers forensics on all privileged user activity.



- **CA Data Content Discovery** is based on a find-classify-protect model with the goal of eliminating the risk of exfiltrating sensitive data. The solution automates the scanning of critical data right on the platform, classifies the data based on regulatory and business concerns, and simplifies risk mitigation so you can make better business decisions. It also integrates with other CA mainframe security solutions, such as CA Compliance Event Manager, to form a comprehensive framework for security and data protection.
- **CA Compliance Event Manager** is a mainframe-specific solution to obviate the impact of data breaches and insider threats. By using real-time alerting and sophisticated reporting tools, CA Compliance Event Manager delivers immediate insights about the depth and breadth of data exposure on the mainframe, supports end-to-end auditing and forensics, and delivers deeper, richer insights to protect mission-critical data, reduce risk and provide for efficient data protection processes.

In the end, technology solutions are only as good as the vendor's expertise, commitment to tight collaboration and ability to innovate around demonstrated security and data protection best practices. **Ultimately, digital trust extends to every enterprise's due diligence of software life-cycle partners.**

Think BIGGER Than Compliance

The global regulatory environment is rife with activity. Legislators and regulators nowadays have to answer to the body politics' growing concern for data privacy and security. Therefore, it is highly likely that more mandates of similar impact and magnitude to GDPR are coming. The time to start planning is *now*. **Your scope should be wide enough to include forward-thinking data security—a competitive advantage.** The goal is, after all, to gain and maintain customer loyalty and stay ahead of the competition.

These compliance mandates are a fact of life for digital enterprises and, as such, a significant drain on their technical, personnel and financial resources. Far-reaching mandates, such as GDPR, get a lot of attention, but we all know press coverage is

not always wide enough in its scope—local regulations are critical too. Be sure to adjust the aperture of your data security strategy to include all relevant mandates, security goals and current standards and best practices.

Compliance, though, is not the only risk factor enterprises need to take into account. Customer concerns, the fact that your data is no longer "living in a safe neighborhood" and the staggering growth in data must be considered as well.

Data security, as a result, has become a corner-office and board-level initiative. It impacts every business process and every technology center, and that includes the mainframe. Enterprises that continue to rely on the mainframe as a core component of their overall digital strategy can fortify their security by modernizing their approaches with flexible, automated tools and a real-world perspective on both compliance and the benefits of stronger data protection.

In the end, regulatory compliance is certainly not irrelevant, but it should not be the sole focus of your security efforts nor the main impetus. Smart data protection policies, processes and practices go beyond the realm of compliance to create a more efficient and secure enterprise, from the mainframe to the cloud.

To learn more about smart, proven approaches to mainframe security and data protection, click here.