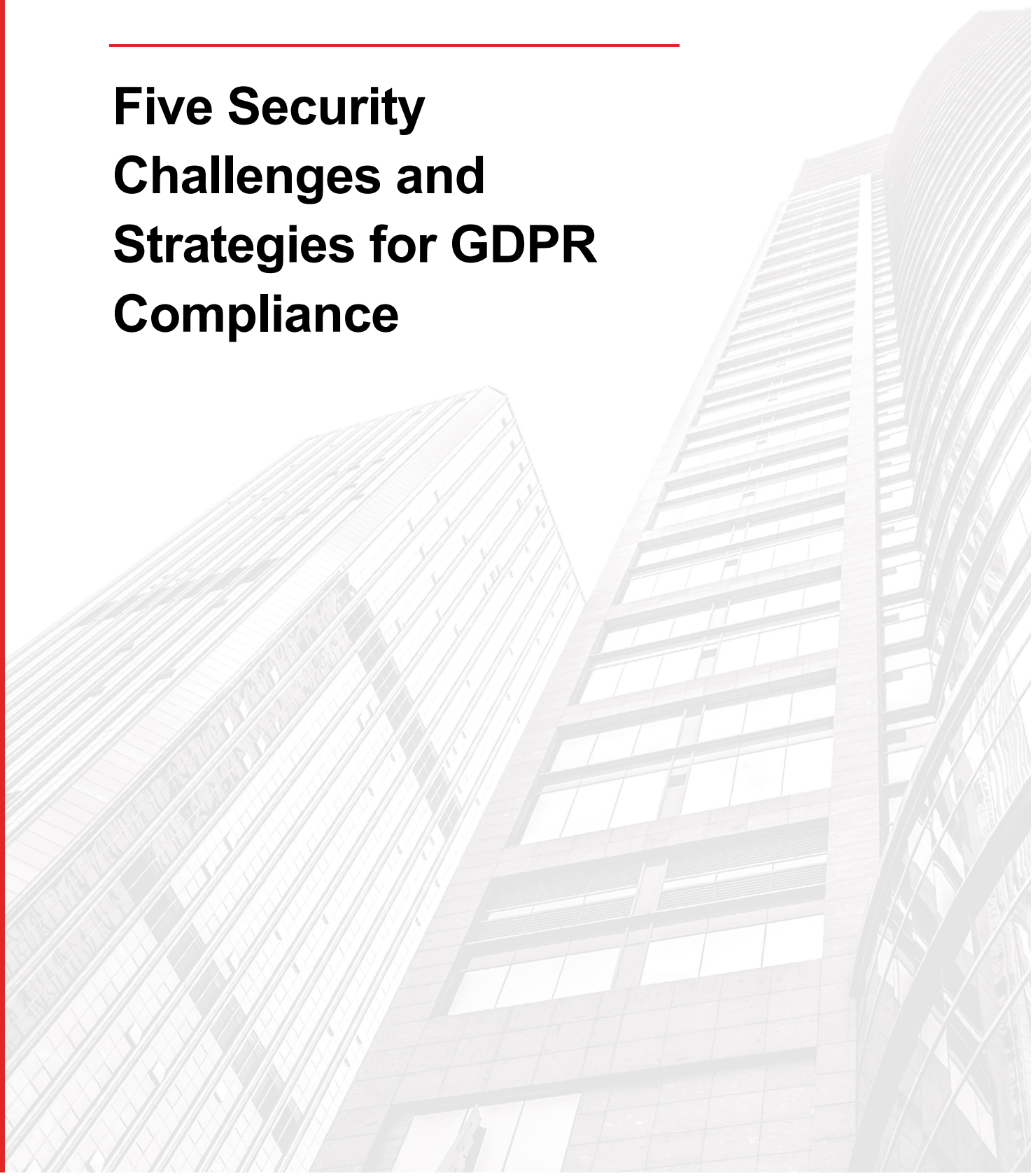
ivanti

Five Security Challenges and Strategies for GDPR Compliance



Contents

Introduction

2017 was the year of the data breach. This, coupled with increasing demands for personal data security, is leading governments to pursue stringent legislation to protect citizens' data—legislation like the new General Data Protection Regulation (GDPR). But protective legislation also places heavy burdens on enterprise IT to discover new ways of providing increased security while ensuring workers can still get their jobs done. This guide offers practical and key recommendations for IT leadership to navigate GDPR compliance and the security of personally identifiable information (PII).

The Impact of GDPR

With organizations like Equifax and Uber falling victim to cyber attacks and failing to disclose the exposure of personal data promptly, the European Union is calling for wide-sweeping reform with its new GDPR legislation. For many organizations it may require a complete overhaul of how they acquire, manage, protect, and track customer and employee information. In addition, organizations can no longer hide breaches of personal data from the public eye. The legislation standardizes and toughens laws governing personal data for any organization that serves or employs EU citizens. And the costs of noncompliance include stringent fines, penalties, and compensatory damages for infringements.[i] Administrative fines alone for noncompliance with certain GDPR provisions can be up to 20 million euros or four percent of a company's total worldwide annual revenue.

So, when must organizations be in compliance with these far-reaching regulations? The deadline is May 25, 2018. And the potential for such tremendous financial impact has more than EU financiers salivating. Corporate insurance underwriters view GDPR compliance as a source of substantial risk when calculating an organization's insurance premiums, and law firms are sure to eagerly jump on organizations that fail to comply with GDPR and expose their clients' data. The stakes are high. And time is running short.

GDPR Introduces:

- Detailed compliance processes for threat remediation, including the 72-hour rule requiring a timely report of a personal data breach to a supervisory authority upon discovery
- Significant fines for organizations found in breach of GDPR regulations
- Sweeping requirements granting EU citizens much greater control over personal data
- The need for organizations to hire "data protection officers" focused on protecting consumer data

Preparing for GDPR: Five Key Security Strategies

GDPR is clear about the need for security requirements to protect EU citizens' data, but it is less specific about what to do to secure that personal information. Although the road to compliance may be different for every organization, most can greatly minimize threats to personal data and the risk of significant fines by addressing these five security challenges:

1. Protecting personal data from threats from mobile workers
2. Managing admin rights across systems and applications
3. Mitigating the costly impact of ransomware and other malware
4. Minimizing risks of employee onboarding and offboarding
5. Tracking and reporting on personal data access

Fortunately, for each of these challenges there are powerful, quick-to-implement security strategies that you can leverage to prepare for GDPR compliance and protect personal data.

Strategy #1: Decrease security exposures from mobile workers.

By 2020 it's estimated that 72 percent of U.S. workers will be reaching for a mobile device to perform their job.[ii] However, each mobile device and access point increases the opportunity for attackers to infiltrate your network. For years, IT has developed tremendous perimeter-based static security technologies – only to see them neatly circumvented by an eager worker tapping on a smart phone while connected in a corner coffee shop.

Decreasing risk and helping ensure GDPR compliance is no easy task. To protect organizations from these new risks and help ensure GDPR compliance, new context-aware security and policy controls are a must. Context-aware controls adapt each worker's digital workspace dynamically to the level of security risk they pose at any given time, based on their working criteria:

- Are they connecting with a known or unknown device?
- Are they connecting via a trusted or untrusted network?
- Are they using unrecognized or company-sanctioned USB drives or peripherals?
- Are they attempting to access sensitive information during business hours or at an unusual time of day?

Strategy #2: Take back control of privileged user access.

Administrative privilege provides users with access that, if misused, can result in high support costs and a compromised user experience. In many cases, security is also compromised through mishandling data, installing unapproved hardware or software, the loss of data, or attack from malicious software. Every privileged user is a prime target of malicious actors, increasing vulnerability because their elevated access rights allow attackers to navigate corporate networks, systems, and applications more easily.

There are, however, many scenarios where users do require local admin rights to work effectively. Many applications, including newly released ones, allow changes to be made to hardware settings or network adapters, and all require administrative privilege to execute. This includes Web application updates, the installation of Active-X components, Adobe/Flash/Java updates, or installation of printer drivers.

For the sake of expediency and IT efficiency, some organizations grant elevated access rights to almost everyone within the enterprise simply because they lack the resources and capability to govern that access more cautiously. In most organizations, "least- privileged user" access policies are often met with uncomfortably liberal standards. In addition, when users aren't granted access to applications they need to do their job, they may introduce unauthorized workarounds, adding risk to your environment and compliance efforts.

Organizations must be able to grant admin rights to users and remove them as needed to protect the business while keeping it productive. With dynamic controls, privileged user rights can be reduced immediately when users move out of an application or indicate a job is complete. Every reduction in user privilege reduces the risk of security breaches.

Putting dynamic controls in place can have tremendous impact on managing admin rights at scale and achieving GDPR compliance.

Strategy #3: Contain ransomware and other malware attacks.

Ransomware and other malware will have zero impact on your organization—if they can't get in. And their most likely means of access are email phishing attacks and vulnerable software left unpatched. Attackers also use external drives and peripherals to transfer malicious code and gain access to personal data. When workers click on a malicious email link, visit compromised websites, or connect to unsecured USB flash drives, the device or computer they're working on can become infected. That malware will then seek to spread deeper into your environment and even steal credentials to log into third-party websites like banking and retail sites. By patching operating systems and third-party applications consistently and comprehensively, preventing unauthorized code from executing with application whitelisting, and locking down website and file access, organizations can greatly reduce their exposure to attacks.

Most organizations already have some form of whitelisting in place, but it's often not without its pain points. Discovery can be an exhaustive process. Once implemented there is a constant need to maintain and update the whitelist. Today's users must be able to do their jobs quickly and effectively, and new apps and versions are introduced daily to our environments, compounding the cost of ownership for traditional whitelisting methods. Some solutions also cause a heavy performance impact to the system, as each application accessed must be evaluated to ensure it matches the known good application and is not modified or a renamed file trying to impersonate the whitelisted file.

Consider whitelisting solutions that remove a lot of the overhead to maximize the value they bring to the table. In addition, adding granular, hash-level controls that employ signatures to open files or execute applications will go a long way toward helping prevent users from launching an attack accidentally when clicking on a link or email attachment. Organizations can also put controls in place to dynamically block users from accessing specific websites or files, prevent users from saving malicious files to local drives or disks, and lock down external devices so only protected or encrypted files can be opened or saved. And beyond preventing unauthorized / unwanted applications from executing, it's also important to ensure endpoints aren't compromised by trusted applications modified while running in memory. Proactive controls help organizations ensure personal data is protected and demonstrate compliance with GDPR security requirements.

Strategy #4: Implement secure onboarding and offboarding.

Many organizations still rely on manual processes to onboard and offboard workers, which often lead to inaccuracies and delays of days or weeks. A recent Ponemon Institute study found that more than 24 percent of people leaving an organization still had access to their corporate data even weeks later.[iii] T processes can provision workers automatically with role-based access to the apps and services they need to do their jobs. And the same technology can be used to de-provision workers immediately the moment they leave the company, or move or change roles. Automating provisioning and de-provisioning enforcement policies streamlines security without the worry that something was missed and also simplifies preparing for an IT audit. Provisioning and de-provisioning processes should be tightly integrated into existing human resource apps, project management systems, or other enterprise identity stores, so access changes can be triggered automatically when a worker's identity status is changed in those systems. With this more holistic approach to identity lifecycle management, organizations can significantly improve productivity and security while supporting GDPR compliance requirements.

Strategy #5: Improve visibility into and reporting on personal data

To help prove GDPR compliance, organizations need greater visibility into the data flowing through their IT environments. Who accessed what data must be tracked, and they should be able prove that proper controls were implemented to secure personal data. And to discover and remediate threats before they become the headline for the latest security breach, IT administrators must be able to consolidate and cut through the mass of information being tracked, extracting the critical insights that matter in real time.

Organizations should also be able to produce reports easily about deployed workspace details, including changes, usage, devices, apps, and configurations. Log tracking and reporting allow organizations to demonstrate proof of GDPR compliance and quickly prepare the information required for reporting breaches to supervisory authorities and individuals. With visibility into your mountains of data, not only can you prove compliance more efficiently, but you can share data insights with the right personnel to accelerate your business and introduce new revenue streams.

How Ivanti can support your GDPR strategy

We help the world's most trusted organizations manage and secure their IT environments with technology solutions that bridge security, service management, and IT operations to automate and secure the digital workplace.

Assess

Organizations should prepare for GDPR by first assessing their level of risk of non-compliance. They need transparency and access to client, server, and user-provisioning data to make this assessment. Ivanti can help you access your level of risk quickly with customized dashboards and reporting tools. You can view threats to the security of personal information in real time and gather insights into which workflows should be established to help achieve compliance.

Automate

Next, organizations should enforce policies to ensure consistent management of personal data and privacy. With more than 50 percent of ex-employees retaining access to employer applications, for example, and 20 percent of data breaches stemming from failure to de-provision access rights,[iv] organizations need the ability to act fast to protect personal data.

Ivanti can help you transform error-prone, manual processes and policies into automated workflows based on user roles within your organization. Now you can provision and de-provision employees quickly across your IT environment.

Protect

Ivanti's solutions discover and provide insight into areas of weakness in your IT environment as well as take action and protect sensitive PII information from attacks. With Ivanti solutions you can:

- Discover the hardware and software in your environment. You can't protect or defend against the unknown.
- Retrieve and track data, report, and analyse.
- Patch the applications you can patch, and control access to those you can't.
- Implement application controls to help prevent ransomware and protect PII data.
- Control removable device use and enforce encryption on removable devices and hard drives.
- Limit admin rights without affecting productivity or consuming your IT team's valuable time.
- Grant users get the right levels of access based on their identity, giving them the ability to stay productive while the business remains secure.

Respond and Comply

Lastly, Ivanti can help you prove that necessary policies are being enforced, consolidating data across your entire IT ecosystem to deliver real-time contextual reporting and expedite auditor requests. With pre-built connectors to more than 50 industry-leading third-party IT solutions, Ivanti makes it easy to get started. Now you can automate workflows to identify requested data in minutes, not hours, and gain actionable insight into your systems and endpoints to maintain GDPR compliance.

Contact Ivanti Today

With the deadline quickly approaching and security risks looming, you can't afford to put off implementing your GDPR compliance strategy. It takes time to get the right processes, policies, and technology in place. If you'd like to learn more about how Ivanti can customize a solution for you, please contact sales@ivanti.com.

www.ivanti.com/GDPR

1-888-253-6201

contact@ivanti.com

[i] http://eur-lex.europa.eu/eli/reg/2016/679/oj, Articles 83 & 84

[ii] http://www.channelfutures.com/mobile-computing/idc-mobile-workers-us-exceed-105-million-2020

[iii] http://media.techtarget.com/Syndication/NATIONALS/Data_Loss_Risks_During_Downsizing_Feb_23_2009.pdf

[iv] https://www.onelogin.com/press-center/press-releases/new-research-from-onelogin-finds-over-50-of-ex-employees-still-have-access-to-corporate-applications