cavirin

SOLUTION GUIDE

Continuous Security for GDPR Compliance

The General Data Protection Regulation (GDPR), in force since May 2018, unifies data protection for all individuals while in the European Union (EU), or EU citizens even when they are traveling outside of the EU. Unlike previous approaches to privacy that focused on organizational risk, GDPR is focused on the data privacy rights of the individual.

How does this impact overall security considerations within an organization? All security strategies and tactics must ensure data protection by design and by default so that individual privacy is paramount and the risk of personal data disclosure is minimized. Under the GDPR, private data is wide-ranging, extending to both professional and private information and may include names, addresses, photos, email addresses, banking information, social network postings, medical information, and IP addresses.

For most organizations, GDPR will add a new level of complexity, and anything they can put in place to automate their compliance will be of benefit. GDPR influences how data and cybersecurity is handled both within and outside of the EU, on-premises and in the cloud. According to the 2018 GDPR Compliance Report, many organizations are still not fully compliant, due to lack of staff, lack of budget, or limited understanding of GDPR. The results are concerns that include lost market share, diminished brand perception or going out of business due to a GDPR-associated breach that could involve GDPR fines of 4% of an organization's annual revenues. In fact, multi-billion dollar lawsuits are now in play targeting Facebook and Google. And, GDPR is not isolated, with the new California Consumer Privacy Act (CCPA) modeled after many of its precepts.

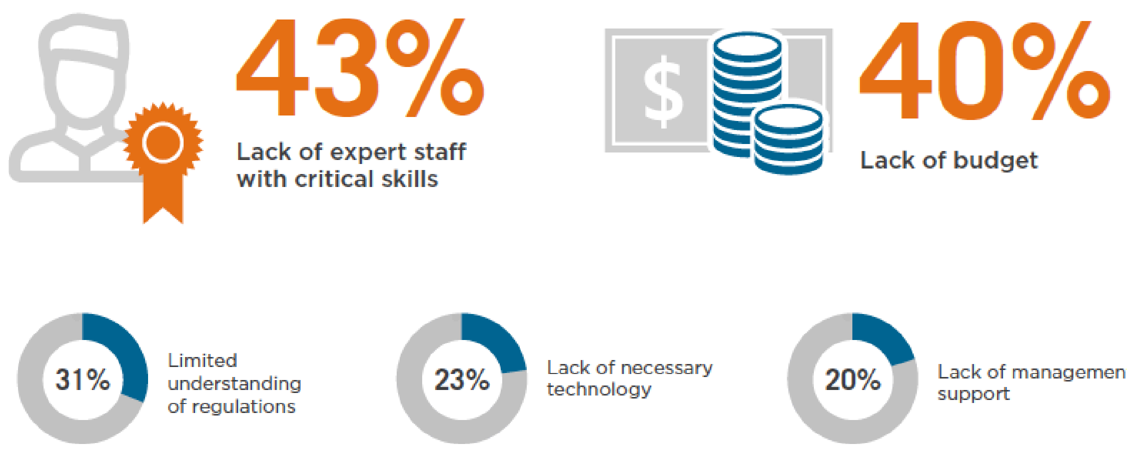
GETTING READY FOR GDPR

Getting ready for GDPR is about protecting individual's personal data from breach or loss. From an infrastructure security perspective, this translates into the following broad requirements:

- Auditing Personal Data Processing Systems: Ensuring that all user and admin activities in personal data processing systems is traceable at all times.
- Monitoring Personal Data Processing Systems to ensure they are safe from software vulnerabilities
- Personal Data Access controls: Ensure that access to systems storing or processing personal data is restricted to only users or programs that need it
- Personal Data Security controls: Monitoring configuration settings for systems storing or processing personal data to prevent breaches and disclosure
- Personal Data Transfer Security: Monitoring usage of encryption and network configuration to detect and/or prevent unauthorized transfers of personal data

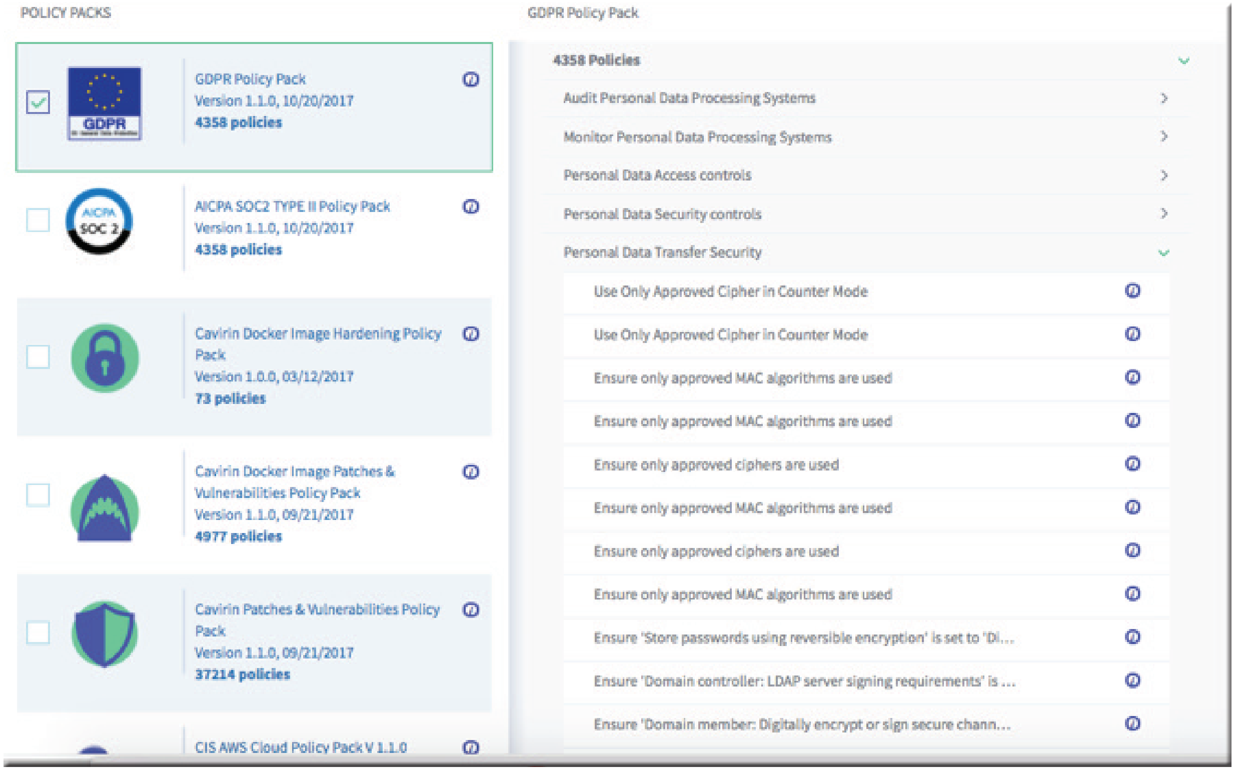
These requirements apply to all systems that store or process personal data, regardless of whether they are on-premises or in public clouds. The same requirements apply to any organization handling EU resident/citizen data, including cloud service providers.

What challenges are your company facing in becoming compliant with GDPR regulations?



SOLUTION

Cavirin, leveraging deep expertise in industry best security practices and regulatory controls, has developed a GDPR Policy Pack consisting of nearly 4,400 infrastructure security controls tailored to the requirements for protecting and monitoring access to personal data, spanning various Operating Systems and their networking configurations. As an example, 400 policies pertain to protecting and monitoring Windows 10 machines. Organizations can assess their on-premises and public cloud infrastructure against this Policy Pack and gauge their GDPR readiness at a glance. More important, Cavirin helps organizations reach a “golden posture” with respect to GDPR compliance through targeted security remediation plans. Besides GDPR, organizations can also leverage 20 other policy packs spanning 80,000+ policies to protect and continuously monitor their infrastructure.



POLICY PACKS

☑ GDPR Policy Pack
Version 1.1.0, 10/20/2017
4358 policies

□ AICPA SOC2 TYPE II Policy Pack
Version 1.1.0, 10/20/2017
4358 policies

□ Cavirin Docker Image Hardening Policy Pack
Version 1.0.0, 03/12/2017
73 policies

□ Cavirin Docker Image Patches & Vulnerabilities Policy Pack
Version 1.1.0, 09/21/2017
4977 policies

□ Cavirin Patches & Vulnerabilities Policy Pack
Version 1.1.0, 09/21/2017
37214 policies

CIS AWS Cloud Policy Pack V 1.1.0

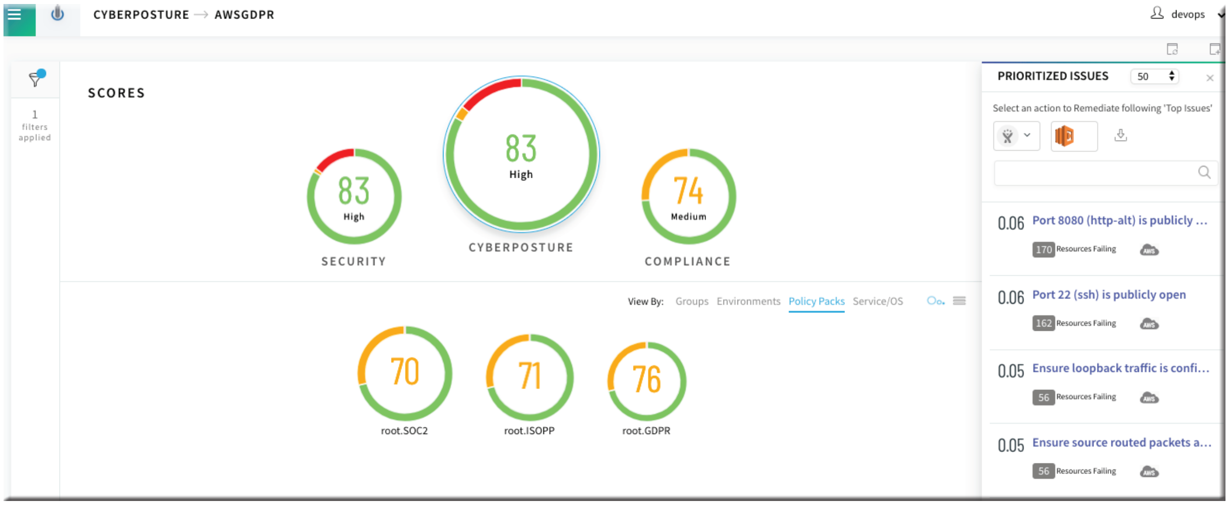
GDPR Policy Pack

4358 Policies

- Audit Personal Data Processing Systems
- Monitor Personal Data Processing Systems
- Personal Data Access controls
- Personal Data Security controls
- Personal Data Transfer Security
  - Use Only Approved Cipher in Counter Mode
  - Use Only Approved Cipher in Counter Mode
  - Ensure only approved MAC algorithms are used
  - Ensure only approved MAC algorithms are used
  - Ensure only approved ciphers are used
  - Ensure only approved MAC algorithms are used
  - Ensure only approved ciphers are used
  - Ensure only approved MAC algorithms are used
  - Ensure 'Store passwords using reversible encryption' is set to 'Di...
  - Ensure 'Domain controller: LDAP server signing requirements' is ...
  - Ensure 'Domain member: Digitally encrypt or sign secure chann...

THE CAVIRIN SOLUTION

Cavirin offers a way out by securing workloads both on-premise and in the cloud. Cavirin's continuous security assessment and remediation platform permits mid-size organizations to quickly adopt best practices, by offering the automation critical to balance limited manpower. And, if in a regulated industry, it ensures the risk compliance of their servers. Although not replacing conventional perimeter defenses like firewalls, Cavirin offers an added level of security, looking from the inside out, by acting as a counter balance to the less robust perimeter security offered by some Unified Threat Management (UTM) systems. At a low cost of entry and the deployment of no new hardware, the business, be it $10M or $1B, now has access to true enterprise-grade hybrid cloud security.



PRIORITIZED ISSUES 50

Select an action to Remediate following 'Top Issues'

0.06 Port 8080 (http-alt) is publicly …
170 Resources Failing

0.06 Port 22 (ssh) is publicly open
162 Resources Failing

0.05 Ensure loopback traffic is confi…
56 Resources Failing

0.05 Ensure source routed packets a…
56 Resources Failing

Cavirin also offers deployment flexibility. If the business operates an on-premise data center, the solution is easily deployed. In the same way, deployment within AWS, GCP, and Microsoft Azure are options. Soon, the organization may also consume the offering as an offering by their MSSP of choice. This last option is important for companies that may not have the in-house capabilities to deploy or manage the service. Forrester has cited that almost a third of midmarket enterprises go this path to take advantage of more specialized skills. In all cases, the customer has a consistent view across all deployment models.