cavirin

SOLUTION GUIDE

Continuous Security for GDPR Compliance

GDPR is "Privacy protection by design and by default"

The General Data Protection Regulation (GDPR), coming into force in 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 today's organizations? 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.

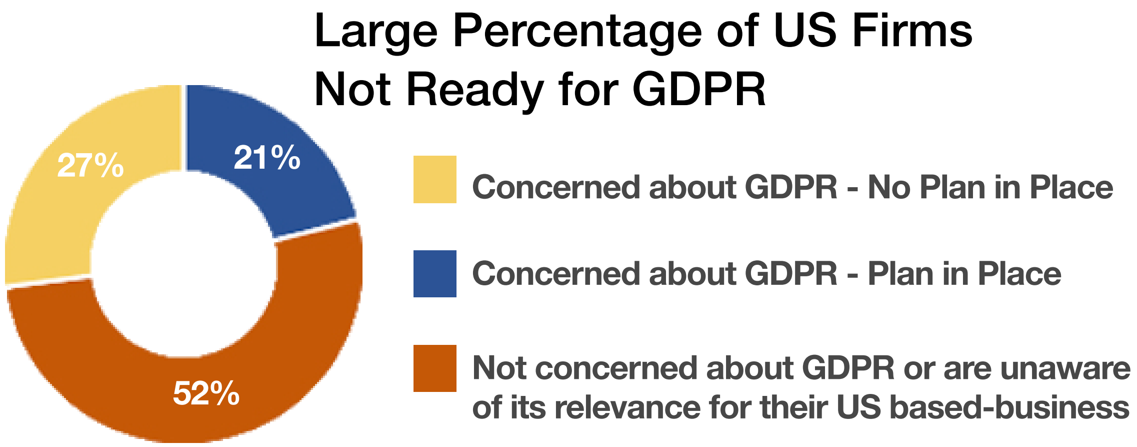
For most organizations, GDPR will add a new level of complexity, and anything they can put in place to automate their compliance will be of benefit. GDPR influences how data and cybersecurity is handled both within and outside of the EU, on-premises and in the cloud. According to a study by Veritas, only 7% of organizations feel they are ready for GDPR - the vast majority are concerned about losing market share, diminishing brand perception or going out of business as a result of their current state of GDPR readiness. A single breach is all it takes to invoke GDPR fines of 4% of an organization's annual revenues.

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: Ensuring individuals are safe from software vulnerabilities
- Personal Data Access controls: Ensuring 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-premise or in public clouds. The same requirements apply to any organization handling EU resident/citizen data, including cloud service providers.

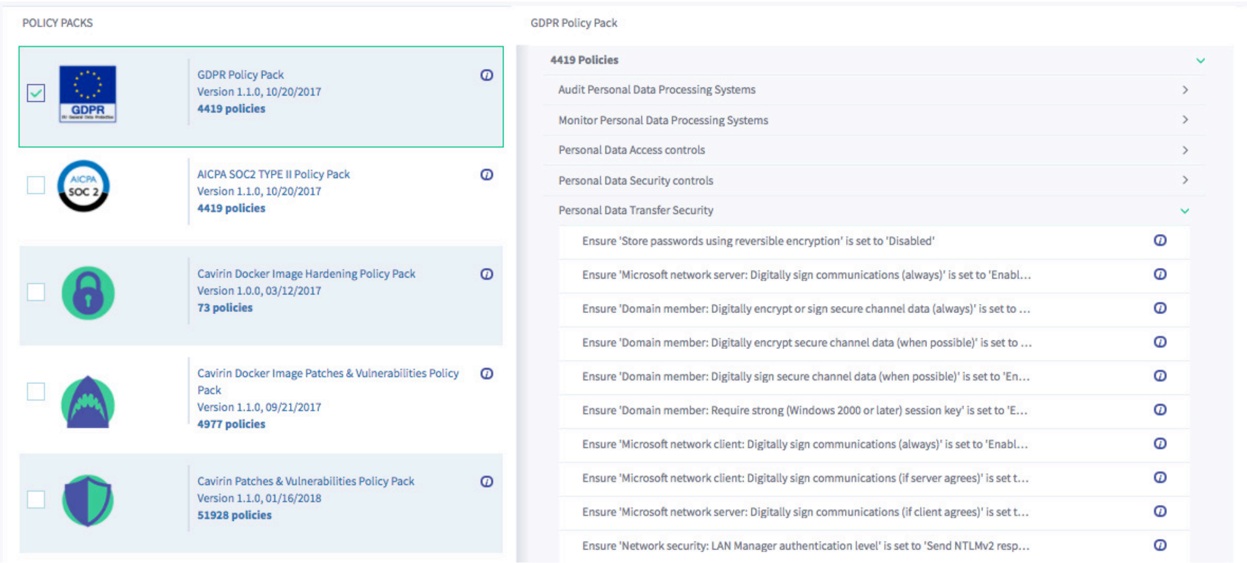


Large Percentage of US Firms Not Ready for GDPR

VMWorld 2017 Hytrust GDPR Survey (323 respondents)

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-premise 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
4419 policies

□ AICPA SOC2 TYPE II Policy Pack
Version 1.1.0, 10/20/2017
4419 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

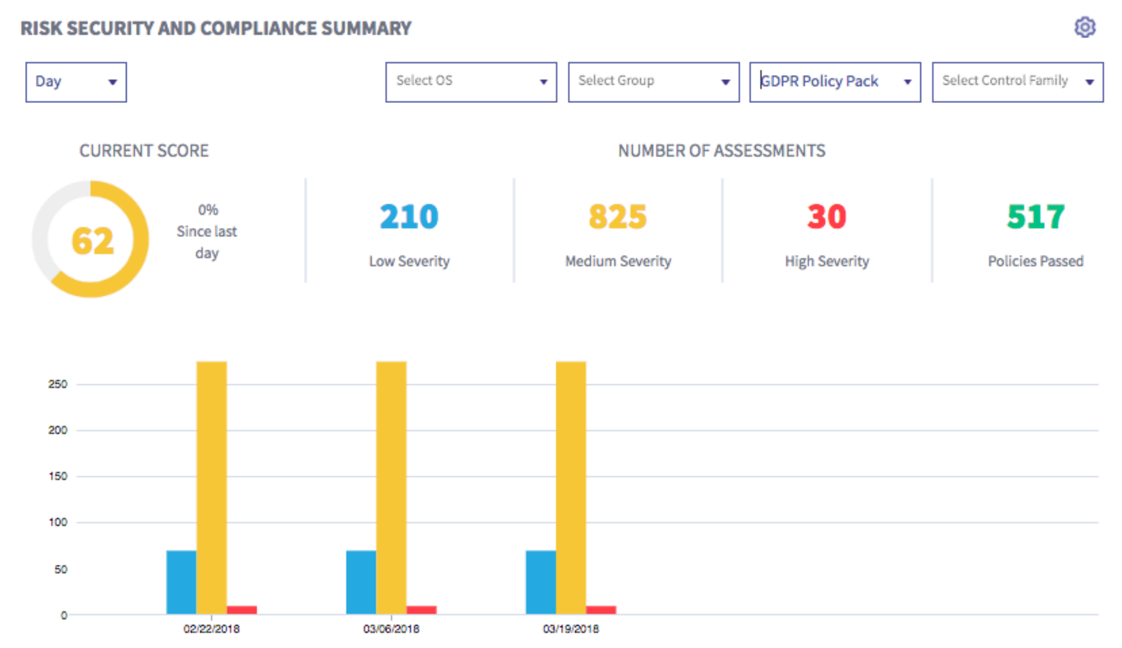
□ Cavirin Patches & Vulnerabilities Policy Pack
Version 1.1.0, 01/16/2018
51928 policies

GDPR Policy Pack

4419 Policies

- Audit Personal Data Processing Systems
- Monitor Personal Data Processing Systems
- Personal Data Access controls
- Personal Data Security controls
- Personal Data Transfer Security
  - Ensure 'Store passwords using reversible encryption' is set to 'Disabled'
  - Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabl...
  - Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to ...
  - Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to ...
  - Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'En...
  - Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'E...
  - Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabl...
  - Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set t...
  - Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set t...
  - Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 resp...

Select GDPR and/or any of the curated policy packs available on the Cavirin Platform



RISK SECURITY AND COMPLIANCE SUMMARY

Day

Select OS | Select Group | GDPR Policy Pack | Select Control Family

CURRENT SCORE: 62 — 0% Since last day

NUMBER OF ASSESSMENTS

210	825	30	517
Low Severity	Medium Severity	High Severity	Policies Passed

Dashboard shows one integrated view of overall GDPR cyberposture with drill down analytics.

ABOUT CAVIRIN

Cavirin delivers cyberposture intelligence for the hybrid cloud by providing real-time risk & cybersecurity posture management, continuous compliance, and by integrating security into DevOps. The Cavirin platform combines automated discovery, infrastructure risk scoring, predictive analytics, and intelligent remediation to help organizations of all sizes leverage the cost savings and agility of the cloud without increasing operational risk or reducing their security posture. For more information, visit www.cavirin.com or follow us at www.twitter.com/cavirin.

“Risk assessments must be made with the focus on protecting data subject rights, as opposed to protecting the organization” - GDPR