

## Solution Brief

# SAFEGUARDING SENSITIVE DATA WITH RUNECAST COMPLIANCE ASSESSMENT

Compliance frameworks are designed to secure critical data, including sensitive information such as personal, medical, financial, or business data. However, adopting compliance measures to manage and minimize the risk of cyber breaches can be an intricate, challenging, costly, and time-consuming task – even when there is a minimum set of security requirements in place.

Organizations need a comprehensive solution that automates multi-cloud and cross-platform scanning of best practices and security regulations to overcome these challenges. Such a solution would ensure continuous compliance through a single source of truth, establishing a robust security and compliance posture that minimizes the risk of cyber-attacks and data breaches.



## 5 STEPS TO ACHIEVE CYBERSECURITY COMPLIANCE

In today's digital landscape, organizations are constantly preparing for the next audit due to a rise in regulatory compliance requirements, market demands for adherence to security standards and best practices, and a continual influx of updates and additions to existing standards. Unfortunately, a shortage of experienced administrators in the industry often leads organizations to firefight, rather than proactively manage their environments. This creates a never-ending cycle of reactive measures to meet audit requirements.

This, added to the fact that most organizations are running their workloads in a combination of technologies in distributed environments, not only increases the risk of blind spots but also turns the effort of keeping environments up-to-date with the latest standards and best practices into a time-consuming and cost-prohibitive task without the aid of automated processes.

To establish a comprehensive cybersecurity strategy, organizations should adopt a framework enabling them to proactively assess and improve their compliance capabilities. This is commonly referred to as the Compliance Maturity Model and it helps organizations to develop compliance practices with the purpose of enhancing their overall cybersecurity posture.



### **OPTIMISED**

Continuous compliance is established, security awareness and compliance at all levels. Complete cross geo, stach tech and functional processes and policies. High measurability and continuous improvement for compliance automation.

### **INTEGRATED**

Established teams and budgets, established clear policies. Effective controls, measurable compliance, irregular automation

### **DEFINED**

Leadership established, general policies established, controls to measure and monitor created, basic automation.

### **PRELIMINARY**

Established needs, basic policies, basic controls.

### **REACTIVE**

Ad-hoc, uncoordinated.

Runecast provides an AI-powered platform that allows minimizing tool sprawl in the environment while moving uncoordinated, policy-less, manual, reactive efforts to proactive, automated, continuous compliance. It resides in the “Optimized Level” as a single source of truth to identify and address compliance risks with full reporting capabilities, presenting an audit-ready environment over time.

This is how Runecast helps to implement the 5 steps to achieve cybersecurity compliance:

## **1 Identify applicable best practices, regulations, and standards**

Runecast automates security standards compliance audits for enterprise-scale environments on AWS, Azure, GCP, Kubernetes, VMware, Windows, and Linux.

It enables continuous compliance with industry regulations and security standards such as BSI-ITgrundschutz, CIS CSC, DISA STIG, GDPR, ISO27001, HIPAA, and NIST as well as allowing organizations to create their own baseline by copying existing issues to a custom profile.

In addition, Runecast automatically monitors all the assets in the infrastructure, highlighting configuration issues and identifying security weaknesses, enabling organizations to quickly identify applicable best practices and security compliance to protect sensitive data and avoid penalties for non-compliance.

## **2 Conduct a risk assessment**

Within minutes, Runecast can identify compliance risks across widely distributed infrastructures. Users can enable specific security profiles tailored to their industry or interests. This allows for analysis that covers various security compliances, vulnerabilities, best practices, and vendor knowledge bases. Users can filter these profiles by applicable systems to customize the scope of the analysis.

Runecast then automates scans of the infrastructure to detect compliance exposures and best practice inconsistencies across all selected systems. This significantly reduces the time the Operations and Security teams need to spend to gain visibility into the compliance state of the environment.

## **3 Prioritize and remediate security gaps**

Both compliance and best practice vulnerabilities are sorted based on the severity levels set by the corresponding government, industry, organization, or technology vendor. Runecast also provides a visual representation of issues, broken down to show the impact across infrastructure and the number of objects affected, making it very easy to identify the most critical vulnerabilities that should be addressed first.

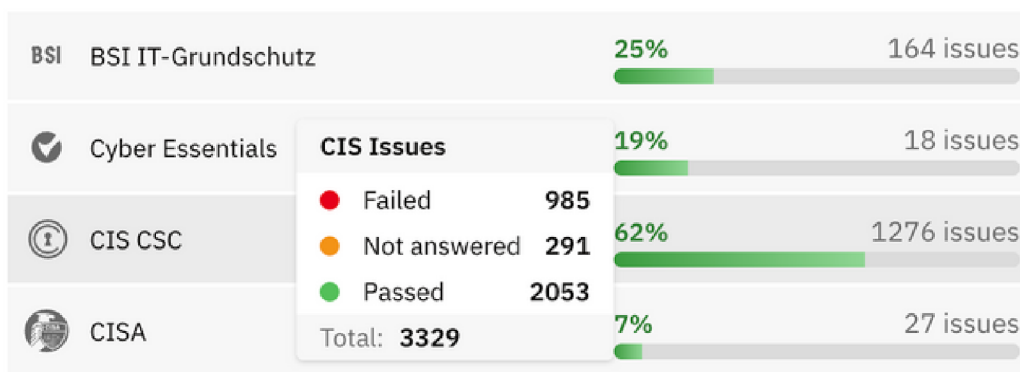
By clicking any of the issues, users will be able to find gap analysis reports as well as remediation steps, and in some cases, custom-tailored scripts to speed up the path to remediation.

## 4 Continuous monitoring and reviewing

Runecast enables organizations to continuously monitor and review the impact of the actions taken to address issues through various views and widgets and by creating baselines that can be used to track compliance security gaps and deviations from best practices over time. These baselines serve as benchmarks for current data, enabling users to gauge the evolution of their security compliance posture and identify any areas that may require attention.

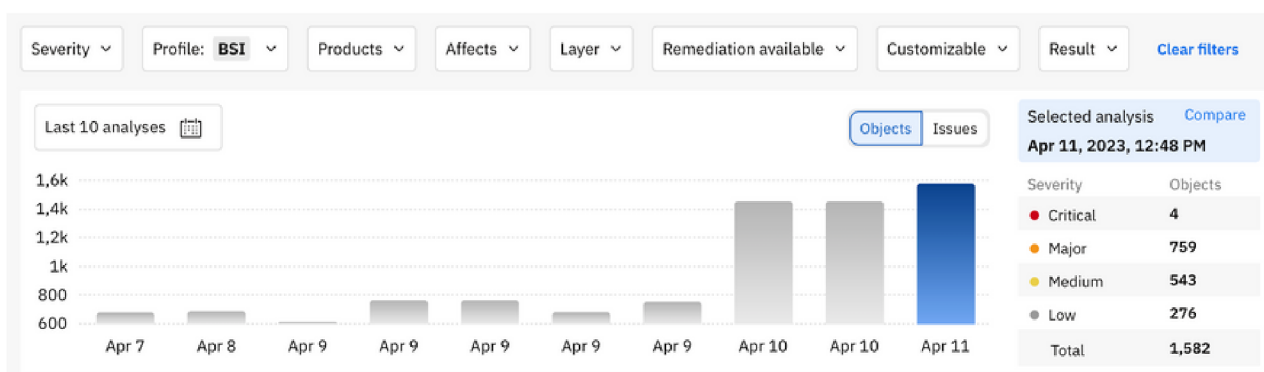
The platform also offers the option to automate alerts to receive real-time notifications about any new issues or changes to existing vulnerabilities, allowing users to take swift action to address them.




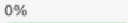

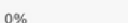

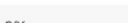
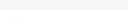
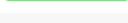
These functionalities provide Operations and Security teams with effective resources to measure the reduction of issue impact and non-compliance levels.



## 5 Document and report

Runecast enables users to automate reporting and access historical reporting going back for any selected time period, to prove evidence of compliance with any of the security standards the platform covers. Templates can be created for on-the-spot reporting, allowing teams to share filtered dashboards and create PDF or CSV documents, should they be needed.



Severity ↓ 3	Title ↑ 6	Impact ↓ 5	Result ↓ 2
Major	1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)'	0% 	Passed
Major	1.1.2 Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'	0% 	Passed
Major	1.1.3 Ensure 'Minimum password age' is set to '1 or more day(s)'	0% 	Passed
Major	1.1.4 Ensure 'Minimum password length' is set to '14 or more character(s)'	0% 	Passed
Major	1.1.5 Ensure 'Password must meet complexity requirements' is set to 'Enabled'	0% 	Passed
Major	1.1.6 Ensure 'Relax minimum password length limits' is set to 'Enabled'	0% 	Passed
Major	1.1.7 Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	0% 	Passed
Major	1.2.1 Ensure 'Account lockout duration' is set to '15 or more minute(s)'	0% 	Passed
Major	1.2.2 Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'	0% 	Passed
Major	1.2.3 Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'	0% 	Passed

## RUNECASST COMPLIANCE ASSESSMENT COMPONENTS

### • MEET REGULATORY AND INDUSTRY STANDARDS

- Gain valuable insights into hundreds of industry best practices for AWS, Azure, GCP, Kubernetes, PowerShell, and VMware.
- Comply with over 13 industry security standards provided out of the box, including BSI-ITgrundschutz, CIS CSC, DISA STIG, GDPR, ISO27001, HIPAA, TISAX, and NIST.
- Create custom in-house security frameworks to comply with company-specific requirements and auditing.

### • CONDUCT RISK MANAGEMENT

- Visualize risks scored by severity levels set by the corresponding government, industry, organization, or technology vendor.
- Protect sensitive data by quickly identifying applicable best practices and security compliance standards to protect sensitive data in the environment.

### • STREAMLINE COMPLIANCE PROCESSES

- Instantly see newly discovered issues, configuration drift, compliance adoption, and hardware incompatibilities through automated alerts.
- Take advantage of built-in best practices and industry security compliance for AWS, Azure, and GCP.
- Deploy across AWS, Azure, GCP, Kubernetes, and VMware environments with an agentless appliance, for hassle-free visibility.

## IN SUMMARY

Without the correct compliance assessment solution in place, organizations run the risk of their infrastructure being exposed to cyber-attacks. With diverse and dispersed infrastructure and many monitoring tools for varying technologies, reducing complexity, lowering operational overhead, and having full visibility of your environment becomes a critical burden to address.

Runecast provides automated, optimized compliance, bringing organizations an integrated approach to tracking exposure risk, compliance status, and environmental health via a single source of truth. By utilizing Runecast, organizations can become optimized through security awareness and compliance at all levels, reducing operational overhead and potential attack surfaces, and speeding up the performance of security and operations teams.

### Learn more

For more information please visit [runecast.com](https://runecast.com) or try Runecast on your environment by requesting an online demo at [runecast.com/runecast-analyzer-online-demo](https://runecast.com/runecast-analyzer-online-demo).



When your organization increases the complexity of its IT architecture and your workload spans across multiple systems and technologies, reducing complexity, lower operational overhead, and having full visibility of your environment becomes a critical burden to address.

To achieve unified issue visibility and reporting, organizations need to adopt a single platform that connects all disparate infrastructure technologies, from bare metal and hypervisor technologies to cloud service providers and containerized workloads.

Runecast brings organizations an integrated approach to security and compliance by tracking the exposure risk, compliance status, and environmental health via a single and automated platform.

For more information please visit [runecast.com](https://runecast.com)

### Runecast Solutions Ltd.

124 City Road,  
London, EC1V 2NX  
United Kingdom

### Runecast Solutions Inc.

300 Delaware Ave  
Suite 210, Box #241  
Wilmington, DE 19801  
USA