



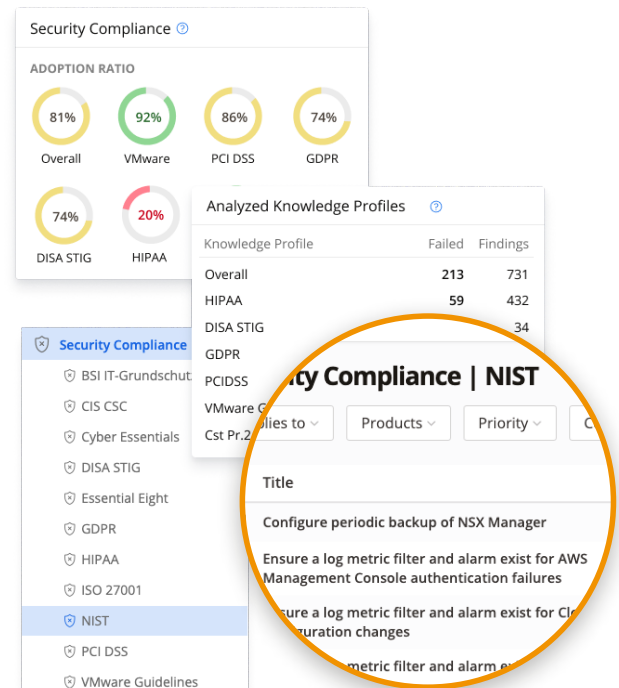
NIST Compliance

With Runecast

Automate your NIST compliance audits for AWS, Azure, OS and VMware

The National Institute of Standards and Technology (NIST) published the NIST special publication (SP) 800-53 in September 2020, which offers security and privacy controls for federal information systems and organizations. Per the Office of Management and Budget (OMB), the NIST standards and policies are mandatory for all non-national security systems run by federal agencies in the USA.

Keeping up with National Institute of Standards and Technology (NIST) standards is time consuming – and mandatory for federal information systems and organizations. NIST lays out the security and privacy controls within NIST SP 800-53 that are needed for US federal agencies to comply with FISMA and other regulations. While mandatory for all non-national security systems run by federal agencies, validating the entire virtual environment based on these NIST standards lists can be a painstaking and lengthy task.



SOLUTION: AUTOMATED NIST CLOUD SECURITY AUDITING AND COMPLIANCE

Runecast automates compliance audits with NIST standards for security and privacy controls for government agencies' virtual networks. (See the [Runecast Support Matrix](#).)

Runecast automates the process of checking VMware vSphere, vSAN, and NSX, AWS and Azure public cloud resources as well as Linux RHEL and Windows Server for compliance against NIST standards – with over 250 checks. Findings are mapped to each specific NIST control, clearly showing both the control ID and the relevant VMware Audit Item detailed in the standard. Each finding is also mapped back to the affected objects, giving you details on how to manually audit and remediate any non-compliances.

With Runecast, you get year-round, 24/7 visibility into your audit compliance posture. It allows you to get immediate visibility into risks and non-compliances in your environment, allowing you to identify gaps as soon as any objects move out of compliance.

The solution runs entirely on-premises, with no data leaving your control. All analysis takes place on the Runecast appliance.

Running the automated NIST audits with Runecast removes pain points by proactively detecting potential misconfigurations and best practices violations. Runecast incorporates the five core functions of the NIST framework – Identify, Protect, Detect, Respond and Recover – to enable IT teams and organizations to automate and improve their cybersecurity posture.

Forward-thinking organizations that rely on Runecast



SCANIA

Swedbank



avast

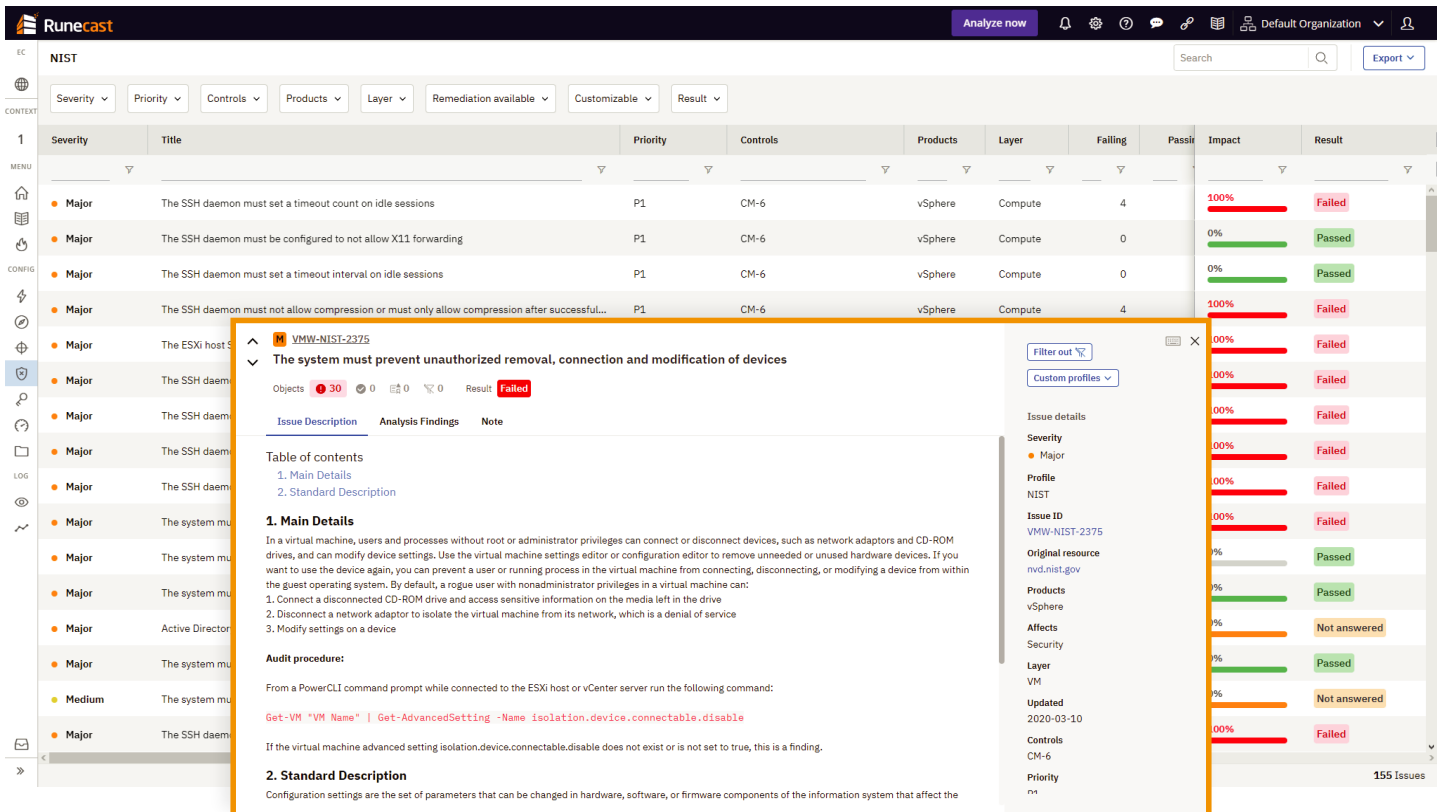
NYC HEALTH+HOSPITALS

DocuSign

RUNECAST HIGHLIGHTS

Runecast is a patented enterprise IT platform that provides IT ops and security teams one platform for configuration monitoring, vulnerability management, security compliance, remediation, upgrade planning and reporting.

- ✓ Proactive solution that automates proactive analysis of logs, configuration drift, and security posture within your environment.
- ✓ Simple, lightweight platform that is super-easy to deploy and operates securely on-premises (no data needs to leave your control) to provide you with remediation steps before any issues can lead to a PSOD or downtime.
- ✓ Operational transparency and best practices alignment
- ✓ Real-time configuration management, vulnerability scanning and security compliance audits
- ✓ Freed up team resources (to work proactively on growth drivers and compensate for skills shortages)



The screenshot displays the Runecast NIST interface. At the top, there's a navigation bar with 'Runecast' and 'NIST' tabs, along with an 'Analyze now' button and user settings. Below this is a filter bar with dropdowns for Severity, Priority, Controls, Products, Layer, Remediation available, Customizable, and Result. The main area shows a table of findings with columns: Severity, Title, Priority, Controls, Products, Layer, Failing, Passed, Impact, and Result. A modal window is open, showing details for a specific issue titled 'The system must prevent unauthorized removal, connection and modification of devices'. This modal includes a table of contents, a main details section with a description of the issue, an audit procedure, and a standard description. On the right side of the modal, there's a sidebar with filters and a list of related issues.

"We designed this platform so sysadmins never have to waste valuable time identifying, diagnosing or searching for error codes ever again"



Stanimir Markov
Runecast CEO, Co-Founder