Runecast

Solution Brief

REDUCING ATTACK SURFACE WITH RUNECAST VULNERABILITY ASSESSMENT

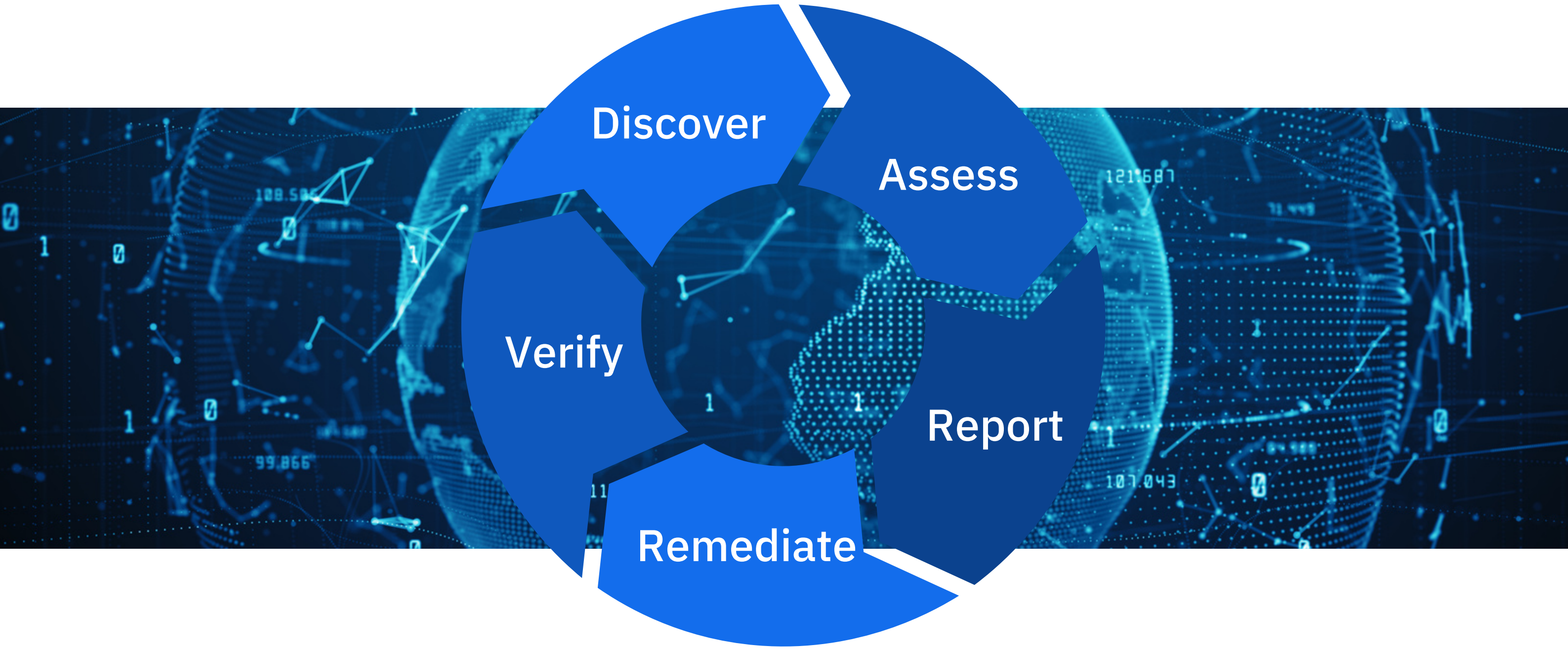
The increasing sophistication of cyber attacks, the difficulty of keeping up with security patches and system configuration, the accelerating use of the public cloud, or the implementation of third-party software dramatically expands an organization´s attack surface making vulnerability assessment a central piece of their cybersecurity strategy.

CYBER EXPOSURE LIFECYCLE

Knowing the level of cyber exposure in your environment is crucial to allow organizations to accurately evaluate the effectiveness of security postures against potential threats. While it is clear that it is impossible to be 100% protected against cyber attacks, organizations must adopt single source solutions that help to prevent these attacks from happening in the first place.

Having a good understanding of the principal vulnerabilities that may affect your systems, how attackers may exploit those gaps, and identifying the associated risks to prioritize remediation efforts, is the first step to reducing your potential attack surface, making threat actors' recognizance and subsequent payload distribution very difficult.

A mature cybersecurity strategy includes the implementation of a solution that can address the five stages of the Cyber Exposure Lifecycle:



Runecast provides an efficient solution for organizations to manage cyber risk by combining vulnerability assessment with continuous analysis of the environment against a wide range of security best practices and security hardening guides. This is how Runecast helps with each of these stages:

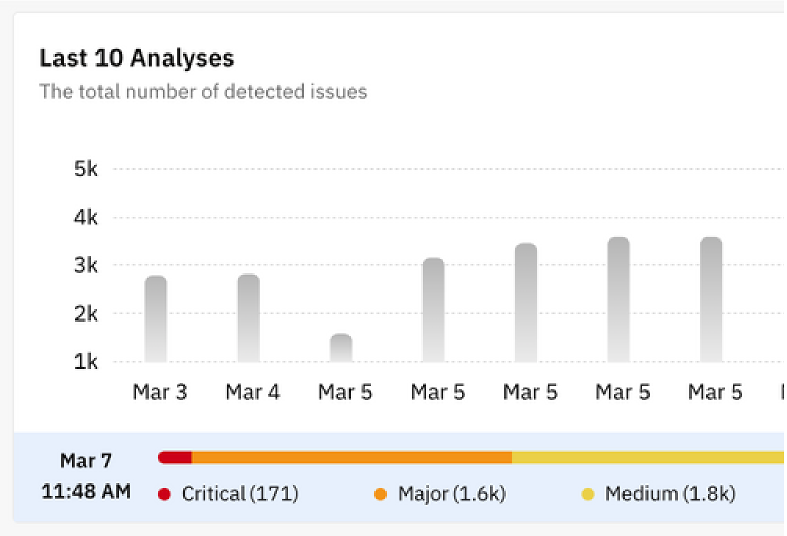
1. **Discover:** Runecast scans all the assets across your entire estate – AWS, Azure, GCP, Kubernetes, VMware, Windows, or Linux – providing inventories of hosts, VMs, services, networks, and disks. Runecast performs dynamic asset discovery, enabling easy identification of new assets that need to be licensed in order to be monitored.

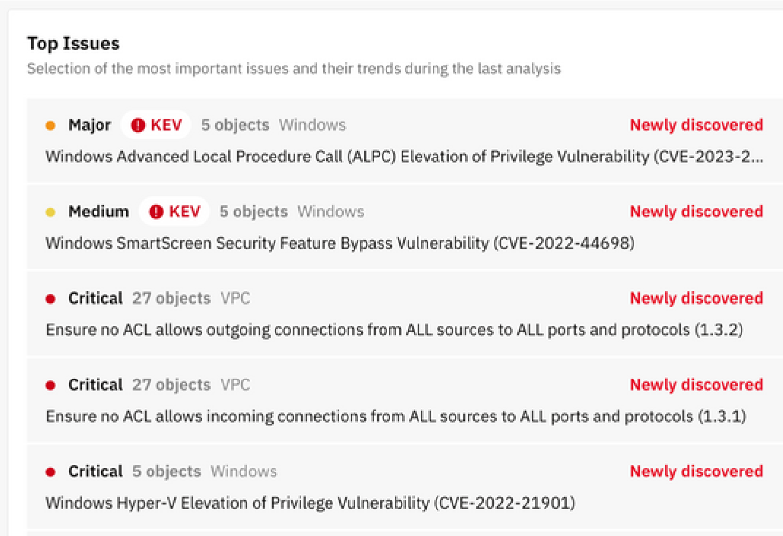
2. **Assess:** Runecast prioritizes vulnerabilities based on the severity level and impact scoring of identified Common Vulnerabilities and Exposures (CVEs), and Known Exploited Vulnerabilities (KEVs) from the Cybersecurity and Infrastructure Security Agency (CISA). In addition to verifying the host version and build number as other vendors do, Runecast evaluates additional criteria, specific to the use case, to accurately determine the validity of reported vulnerabilities.

3. **Report:** Analysis results are displayed through an intuitive web-based dashboard. Users can download custom reports as well as enable email alerts to automatically receive a report of findings to the configured recipients. These reports allow teams to track the security posture and identify trends over time. Runecast has dedicated integrations for engineering teams that automatically create records in ticketing systems such as ServiceNow or Jira.

4. **Remediate:** Runecast provides remediation information for every issue reported. It offers custom-tailored scripts to run in PowerCLI, AWS CLI, or as Ansible playbooks ensuring swift, proactive remediation of environments.

5. **Verify:** With every new analysis, users can quickly see the evolution of actions taken to remediate issues through different views and widgets and understand how the impact of those vulnerabilities has decreased, and therefore, how the attack surface reduced.





Top Issues

Selection of the most important issues and their trends during the last analysis

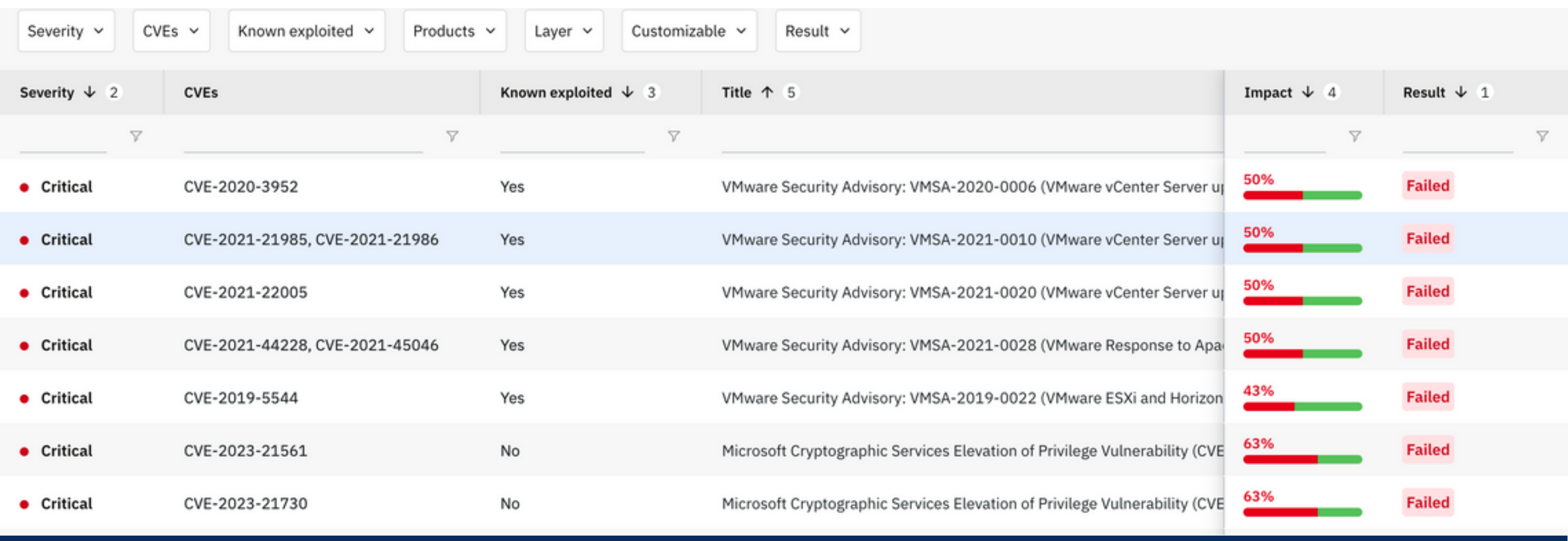
● Major ❗KEV 5 objects Windows — Newly discovered
Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability (CVE-2023-2...

● Medium ❗KEV 5 objects Windows — Newly discovered
Windows SmartScreen Security Feature Bypass Vulnerability (CVE-2022-44698)

● Critical 27 objects VPC — Newly discovered
Ensure no ACL allows outgoing connections from ALL sources to ALL ports and protocols (1.3.2)

● Critical 27 objects VPC — Newly discovered
Ensure no ACL allows incoming connections from ALL sources to ALL ports and protocols (1.3.1)

● Critical 5 objects Windows — Newly discovered
Windows Hyper-V Elevation of Privilege Vulnerability (CVE-2022-21901)



Severity ↓ 2	CVEs	Known exploited ↓ 3	Title ↑ 5	Impact ↓ 4	Result ↓ 1
● Critical	CVE-2020-3952	Yes	VMware Security Advisory: VMSA-2020-0006 (VMware vCenter Server u	50%	Failed
● Critical	CVE-2021-21985, CVE-2021-21986	Yes	VMware Security Advisory: VMSA-2021-0010 (VMware vCenter Server u	50%	Failed
● Critical	CVE-2021-22005	Yes	VMware Security Advisory: VMSA-2021-0020 (VMware vCenter Server u	50%	Failed
● Critical	CVE-2021-44228, CVE-2021-45046	Yes	VMware Security Advisory: VMSA-2021-0028 (VMware Response to Apa	50%	Failed
● Critical	CVE-2019-5544	Yes	VMware Security Advisory: VMSA-2019-0022 (VMware ESXi and Horizon	43%	Failed
● Critical	CVE-2023-21561	No	Microsoft Cryptographic Services Elevation of Privilege Vulnerability (CVE	63%	Failed
● Critical	CVE-2023-21730	No	Microsoft Cryptographic Services Elevation of Privilege Vulnerability (CVE	63%	Failed

RUNECAST VULNERABILITY ASSESSMENT COMPONENTS

1. Discover and prioritize based on risk prioritization

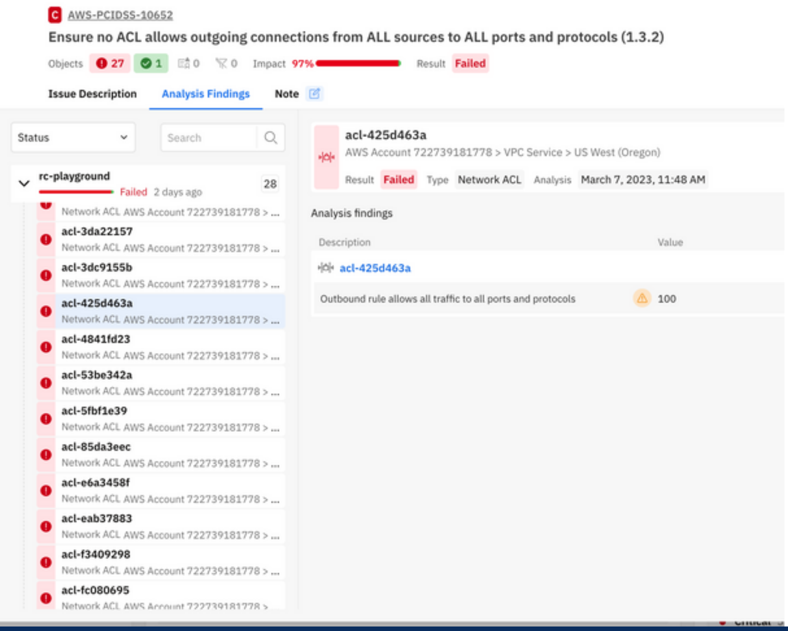
Discover, categorize, and prioritize issues based on the level of risk they can bring to your infrastructure.

- Gain complete visibility of the vulnerabilities across your entire tech stack: From VMware or Kubernetes infrastructure to OS and cloud environments like AWS, Azure, or Google Cloud.
- Benefit from sophisticated vulnerability and security hardening assessment: In Runecast an "Issue" represents a problematic combination of values such as configuration settings, log patterns, software and hardware type, and versions, and vulnerabilities based on information from various sources including VMware articles, industry Best Practices, CVE databases, and the KEV catalog.
- Prioritize issues based on the level of risk: vulnerabilities are categorized based on their CVSS severity levels and Known Exploited Vulnerabilities information (KEVs) from the Cybersecurity and Infrastructure Security Agency (CISA). This helps organizations focus their efforts on addressing the most critical vulnerabilities first, reducing their overall risk of compromise.

2. Analyze the context to prioritize remediation

Runecast provides remediation information for every issue reported.

- Obtain detailed analysis findings for each issue, identifying which are the affected assets and the potential impact on your environment. Issues context includes relevant information from various sources, such as VMware articles, CVE databases, and the KEV catalog.
- Speed up remediation efforts by following detailed remediation steps based on the best practices and recommendations from VMware, cloud providers, industry experts, and Runecast's in-house team of specialists.
- Run custom-tailored scripts in PowerCLI, AWS CLI, or Ansible playbooks ensuring swift, proactive remediation of environments.



AWS-PCIDSS-10652

Ensure no ACL allows outgoing connections from ALL sources to ALL ports and protocols (1.3.2)

Objects 27 1 0 0 Impact 97% Result Failed

rc-playground 28
Failed 2 days ago

Network ACL AWS Account 722739181778 > ...

acl-3da22157
Network ACL AWS Account 722739181778 > ...

acl-3dc9155b
Network ACL AWS Account 722739181778 > ...

acl-425d463a
Network ACL AWS Account 722739181778 > ...

acl-4841fd23
Network ACL AWS Account 722739181778 > ...

acl-53be342a
Network ACL AWS Account 722739181778 > ...

acl-5fbf1e39
Network ACL AWS Account 722739181778 > ...

acl-85da3eec
Network ACL AWS Account 722739181778 > ...

acl-e6a3458f
Network ACL AWS Account 722739181778 > ...

acl-eab37883
Network ACL AWS Account 722739181778 > ...

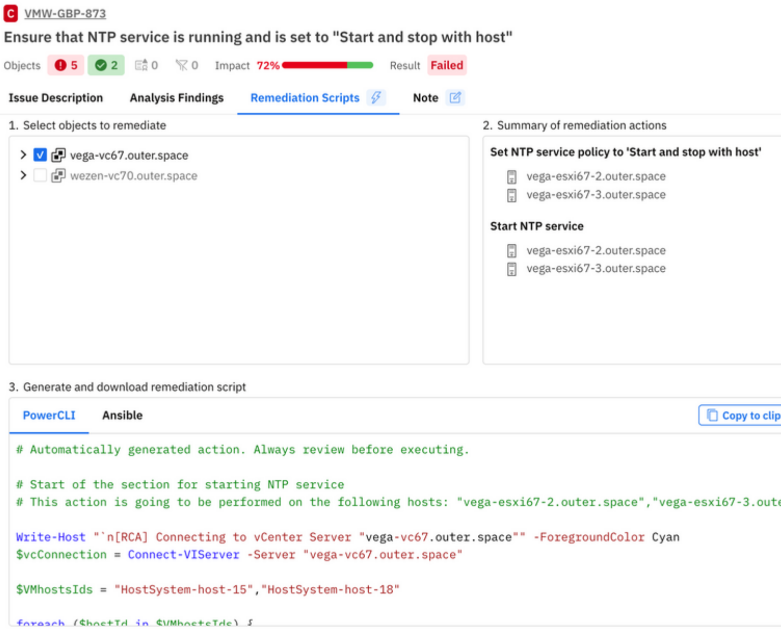
acl-f3409298
Network ACL AWS Account 722739181778 > ...

acl-fc080695
Network ACL AWS Account 722739181778 >

acl-425d463a
AWS Account 722739181778 > VPC Service > US West (Oregon)
Result Failed Type Network ACL Analysis March 7, 2023, 11:48 AM

Analysis findings

Description	Value
acl-425d463a	
Outbound rule allows all traffic to all ports and protocols	⚠ 100



VMW-GBP-873

Ensure that NTP service is running and is set to "Start and stop with host"

Objects 5 2 0 0 Impact 72% Result Failed

1. Select objects to remediate

☑ vega-vc67.outer.space
□ wezen-vc70.outer.space

2. Summary of remediation actions

Set NTP service policy to 'Start and stop with host'
vega-esxi67-2.outer.space
vega-esxi67-3.outer.space

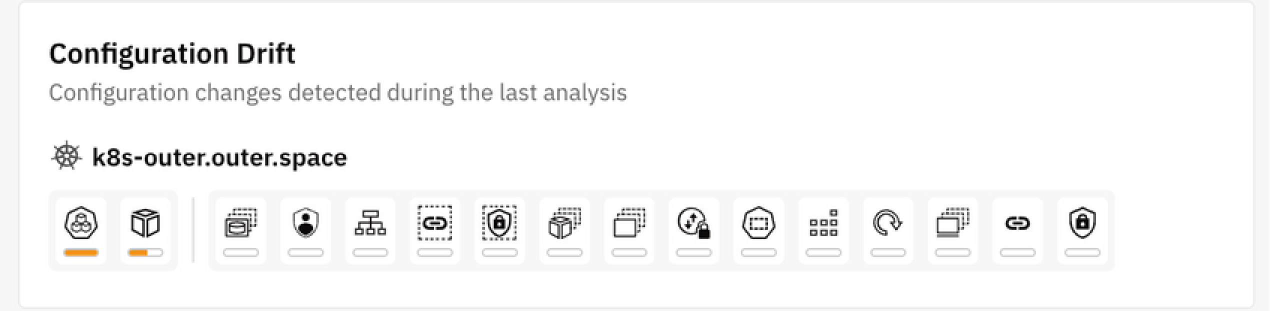
Start NTP service
vega-esxi67-2.outer.space
vega-esxi67-3.outer.space

3. Generate and download remediation script

```
# Automatically generated action. Always review before executing.

# Start of the section for starting NTP service
# This action is going to be performed on the following hosts: "vega-esxi67-2.outer.space","vega-esxi67-3.oute

Write-Host "`n[RCA] Connecting to vCenter Server "vega-vc67.outer.space"" -ForegroundColor Cyan
$vcConnection = Connect-VIServer -Server "vega-vc67.outer.space"

$VMhostsIds = "HostSystem-host-15","HostSystem-host-18"

foreach ($hostId in $VMhostsIds) {
```

3. Detect security misconfigurations and mitigate drift across all your systems

- Track and analyze the impact of configuration changes on your IT infrastructure over time, even for deleted virtual machines.
- Turn any object into a baseline to see differences and shorten troubleshooting time.
- Identify quickly those drifts that can expose your systems to network and data breaches, downtime, and security vulnerabilities or compliance issues.



Configuration Drift

Configuration changes detected during the last analysis

k8s-outer.outer.space

4. Agentless vulnerability scanning

Runecast provides agentless monitoring of your AWS, Azure, Google Cloud, Kubernetes, VMware, and now also for Operating Systems.

- Discover issues in minutes without the need of installing agents or enabling extra modules. In 15 minutes you will gain insights into your hybrid, multi-cloud, or on-prem environments.
- Reduce the attack surface eliminating the need of installing an extra piece of software in your mission-critical assets.
- Automatic dynamic asset discovery to streamline asset management, eliminating the need for manual tracking and inspection.
- Scale vulnerability scanning without the need of installing agents on each of the new assets added to your infrastructure.

5. Rapid response situations: real-world examples

Runecast's AI-powered automation system crawls thousands of trusted sources in seconds to quickly report the latest vulnerabilities and provide visibility of affected assets and remediation steps. This includes the latest information on CVEs, KEVs, and over 10 security compliance standards.

Log4Shell Vulnerability

Only 48 hours after the vulnerability was disclosed, Runecast customers were able to identify where Log4Shell was present in the environment and take mitigation steps to reduce the immediate risk, providing them with a quick response to prevent the attack.

ESXiArgs Ransomware Attack

Runecast had been proactively protecting its users for two years prior to the ESXiArgs ransomware attack. Runecast's patented Rules Engine goes beyond verifying the host version and build number, as other vendors do. It also evaluated also whether the vulnerable service was in use and whether the ESXi forward port was open.

IN SUMMARY

As organizations undergo digital transformation, cyber-attacks become more sophisticated and pose a greater risk. With a more complex and distributed IT infrastructure, vulnerabilities can be exploited and lead to unauthorized access, data theft, and leakage. Therefore, assessing an organization's level of cyber exposure is vital to reduce vulnerable entry points and increasing security posture.

Runecast combines vulnerability assessment with continuous analysis of the environment against a wide range of security best practices and security hardening guides providing a solution that allows organizations to address the five stages of the Cyber Exposure Lifecycle protecting mission-critical workloads while reducing operational overhead, potential attack surface and speeding up the performance of security and operations teams.

Learn more
For more information please visit runecast.com or try Runecast on your environment by requesting an online demo at runecast.com/runecast-analyzer-online-demo.

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