Runecast

Solution Brief

DEFENDING AGAINST RANSOMWARE ATTACKS

Ransomware attacks are becoming increasingly common and are causing significant damage to organizations, exploiting vulnerabilities in a system to gain access and spread throughout the network often causing irreparable damage by encrypting mission-critical workloads.

HOW RANSOMWARE WORKS

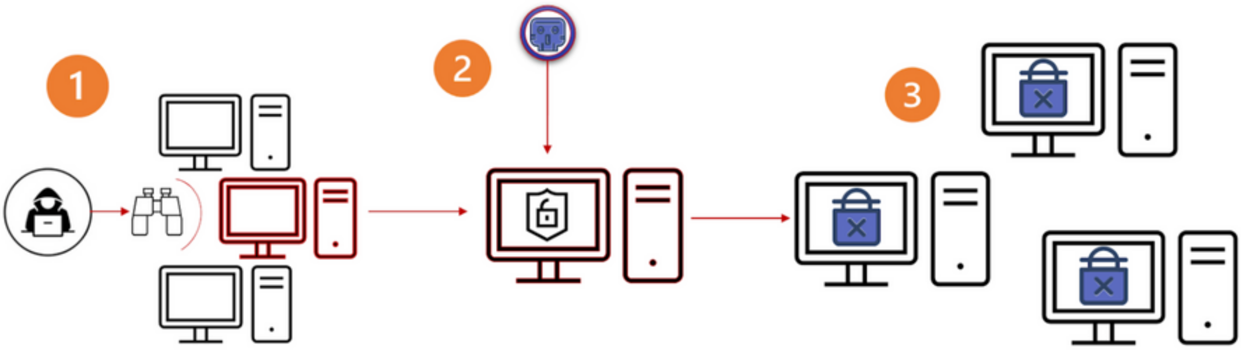


Figure 1: Ransomware attack path

Most ransomware attacks (and many other cyber security threats) start with a reconnaissance phase (1) where threat actors will survey the infrastructure of an organization for any potential target systems that have outdated, un-patched, or otherwise vulnerable software packages or services running.

Once a system is identified, attackers will enter the second phase (2) by exploiting the vulnerability and gaining access to the vulnerable system. This is only rudimentary access in most scenarios (remote code execution etc) but is sufficient to connect to a command & control server and download the payload which will then rapidly spread across the network and encrypt (3) workloads, including mission-critical workloads and in many cases backup storage as well, leaving the affected organization with very few options to regain control of their data.

ATTACK SURFACE REDUCTION WITH RUNECAST

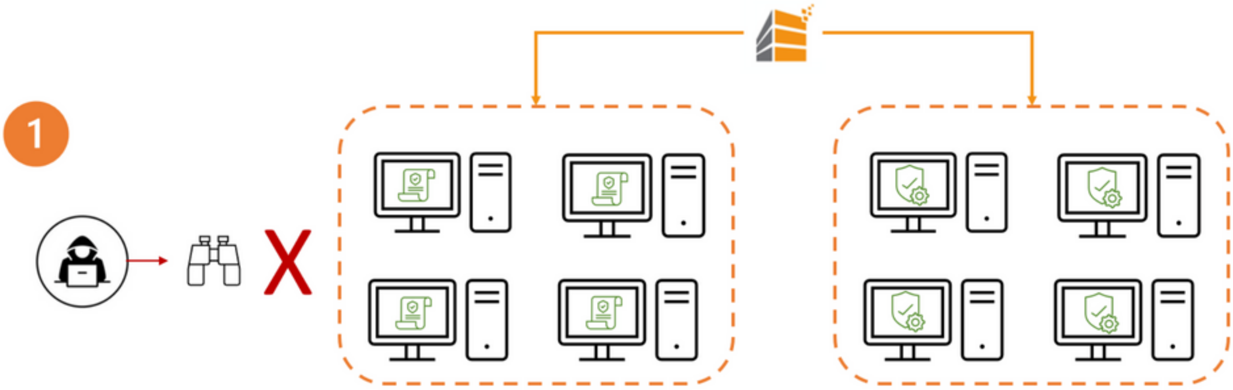


Figure 2: Ransomware protection with Runecast

ATTACK SURFACE REDUCTION WITH RUNECAST

The most efficient protection against any form of cyber-attack is to prevent it from happening in the first place.

Runecast provides an efficient solution to prevent cyber-attacks from happening in the first place by reducing the potential attack surface by combining vulnerability assessment with continuous analysis of the environment against a wide range of security best practices and security hardening guides. This results in a drastic reduction of reducing the potential attack surface, making threat actors' recognisance and subsequent payload distribution very difficult.

Runecast provides:

- **Sophisticated VMware vulnerability and security hardening assessment** - 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. For example, in the EXSiArgs ransomware attack, the Runecast platform analysed as additional criteria, whether the OpenSLP service was active and if vulnerable ports were open.
- **Focused priorities** - User-friendly dashboards offer a comprehensive overview and more detailed analysis through available filters. Every dashboard displays pertinent information, allowing users to identify which remediation efforts should be made first, such as Known Exploited Vulnerabilities (KEVs), PSOD, or any other serious issues the system may be facing. Prioritization is based on severity levels and impact scoring, simplifying the remediation choices for your organization.
- **Quick response** - The Runecast AI Knowledge Automation Platform (RAIKA) receives the latest information on Common Vulnerabilities and Exposures (CVEs), Known Exploited Vulnerabilities (KEVs), and over 10 security compliance standards in seconds. When a vulnerability is disclosed, Runecast customers receive automated and proactive real-time guidance for it directly to their dashboard, via its patented rules engine.
- **Tailored remediation** - In addition to remediation instructions, customers find customized scripts tailored specifically to their environments.
- **Reduced noise** - Runecast is renowned for having a minimal amount of inaccurate alerts, leading to reduced noise and more efficient identification and solving of issues. Whenever there have been any false positives, the support team has worked diligently and swiftly to address them within 24 hours, due to the feedback functions available on the platform.
- **Best time to value on the market** - As an agentless platform, Runecast provides results in minutes rather than hours or days (on average 15 minutes from first deployment to first results).
- **Unmatched deployment flexibility and security** with secure deployment methods that support even air-gapped environments.

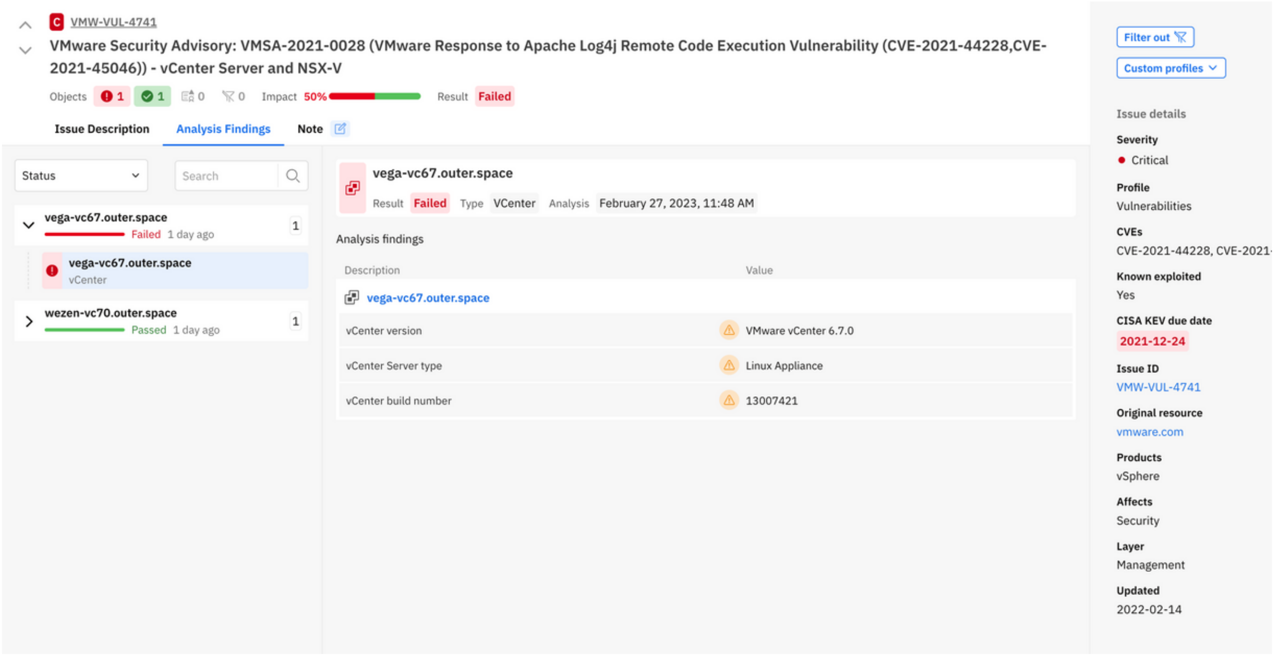
By integrating Runecast into the threat detection and assessment workflow and following its recommendations, organizations can:

- **Greatly reduce the attack surface**: By automating threat and vulnerability detection and management, Runecast helps organizations stay ahead of the risks of malicious actors and threats, including ransomware that could compromise their infrastructure.
- **Prioritize mitigation activities**: Runecast prioritizes vulnerabilities based on their 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.
- **Maintain a hardened configuration** to reduce attack surfaces: Runecast scans virtual infrastructures and provides detailed information on any security vulnerabilities or misconfigurations that could leave systems open to attack.
- **Save time with automation:** Runecast automates many security-related tasks, including remediation. This can save organizations significant time and effort compared to manual security management.

REAL-WORLD EXAMPLES

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.



C VMW-VUL-4741

VMware Security Advisory: VMSA-2021-0028 (VMware Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228,CVE-2021-45046)) - vCenter Server and NSX-V

Objects 1 1 0 0 Impact 50% Result Failed

vega-vc67.outer.space 1 Failed 1 day ago

vega-vc67.outer.space vCenter

wezen-vc70.outer.space 1 Passed 1 day ago

vega-vc67.outer.space

Result Failed Type VCenter Analysis February 27, 2023, 11:48 AM

Analysis findings

Description	Value
vega-vc67.outer.space	
vCenter version	VMware vCenter 6.7.0
vCenter Server type	Linux Appliance
vCenter build number	13007421

Issue details

Severity
● Critical

Profile
Vulnerabilities

CVEs
CVE-2021-44228, CVE-2021-

Known exploited
Yes

CISA KEV due date
2021-12-24

Issue ID
VMW-VUL-4741

Original resource
vmware.com

Products
vSphere

Affects
Security

Layer
Management

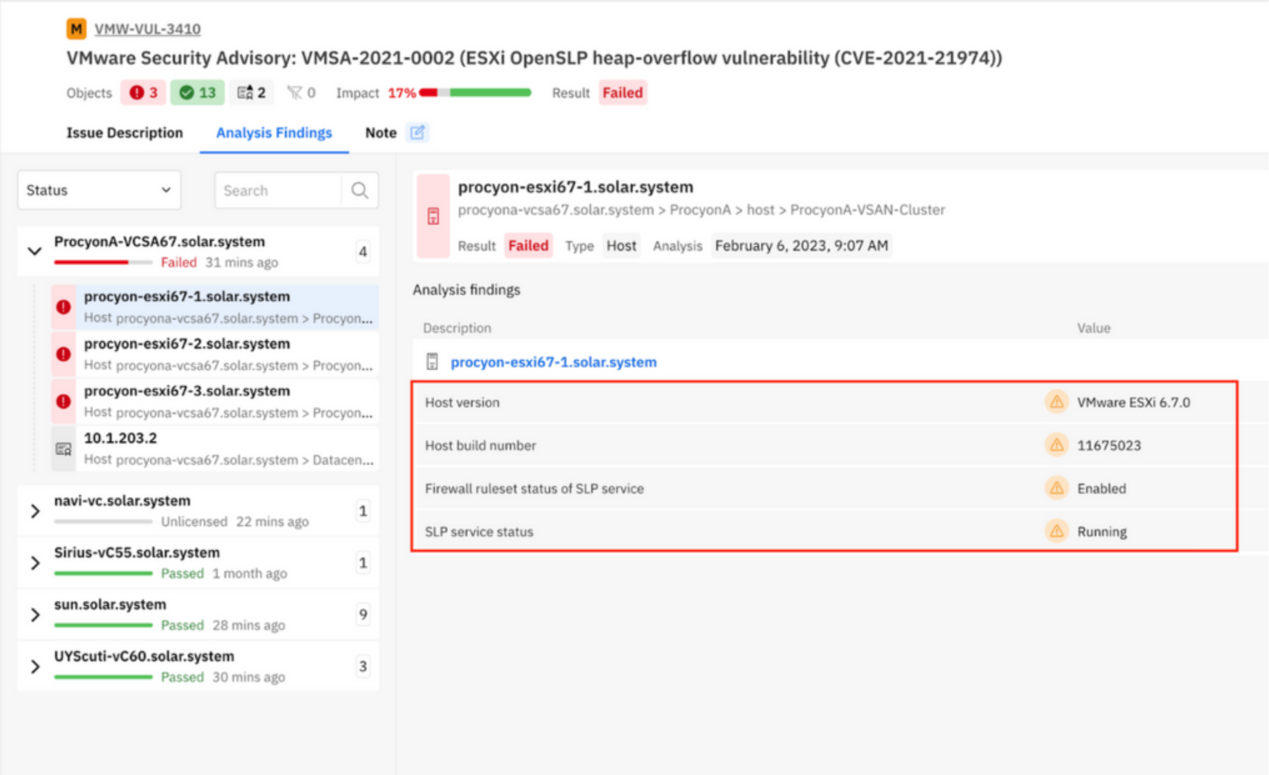
Updated
2022-02-14

Figure 3: Issue description of the VMSA-2021-0028, Log4Shell KEV

ESXiArgs Ransomware Attack

Runecast had been proactively protecting its users for two years prior to the ESXiArgs ransomware attack by providing detailed information and analysis findings on their infrastructure.

Runecast's patented Rules Engine goes beyond verifying the host version and build number, as other vendors do. It evaluates additional criteria specific to the use case to accurately determine the validity of reported vulnerabilities. For example, in the case of the ESXiArgs ransomware attack, Runecast also evaluated whether the vulnerable service was in use and whether the ESXi forward port was open. Thus, Runecast can provide a more accurate assessment of the security of the environment to help organizations take proactive steps to prevent attacks like ransomware.



M VMW-VUL-3410

VMware Security Advisory: VMSA-2021-0002 (ESXi OpenSLP heap-overflow vulnerability (CVE-2021-21974))

Objects 3 13 2 0 Impact 17% Result Failed

ProcyonA-VCSA67.solar.system — Failed 31 mins ago — 4
- procyon-esxi67-1.solar.system — Host procyona-vcsa67.solar.system > Procyon...
- procyon-esxi67-2.solar.system — Host procyona-vcsa67.solar.system > Procyon...
- procyon-esxi67-3.solar.system — Host procyona-vcsa67.solar.system > Procyon...
- 10.1.203.2 — Host procyona-vcsa67.solar.system > Datacen...

navi-vc.solar.system — Unlicensed 22 mins ago — 1

Sirius-vC55.solar.system — Passed 1 month ago — 1

sun.solar.system — Passed 28 mins ago — 9

UYScuti-vC60.solar.system — Passed 30 mins ago — 3

procyon-esxi67-1.solar.system
procyona-vcsa67.solar.system > ProcyonA > host > ProcyonA-VSAN-Cluster

Result Failed Type Host Analysis February 6, 2023, 9:07 AM

Analysis findings

Description	Value
procyon-esxi67-1.solar.system	
Host version	VMware ESXi 6.7.0
Host build number	11675023
Firewall ruleset status of SLP service	Enabled
SLP service status	Running

Figure 4: Example of Analysis findings of the VMSA-2021-002

Providing peace of mind on vulnerability assessment coverage goes hand in hand with the ability to efficiently and effectively gain insights into the exact part of the infrastructure that is at risk and which steps are required to address and remediate discovered vulnerabilities.

WHAT OUR CUSTOMERS SAY

Runecast is a leading provider in the market for securing VMware environments. We count amongst our customer's several organizations that manage large virtual infrastructures. Before using Runecast, some of these customers had no visibility of compliance and they even dealt with manual processes for a long time to keep their VMware infrastructure protected against vulnerabilities and up to date with security regulations.

These are examples of how Runecast helps organizations to automate security compliance, have real-time visibility into potential security threats, and reduce the manual effort required for the remediation of security vulnerabilities.

"As a bank, it is imperative that our IT operations ensure maximum reliability and security for our clients. Our IT team has too much to work on and simply needs automated proactive monitoring tools. Runecast helps us detect errors in logs and configuration issues before they lead to critical failures. This not only saves dozens of man-hours but also provides a reliable prevention mechanism. Our datacenters uptime is now greater than ever."

Daniel Ugarte
System Engineer & IT Administrator
Laboral Kutxa

Read online

More case studies

Städtisches
KRANKENHAUS KIEL

“With remediation scripts alone, if I had to do all of that myself, Runecast has saved us already 100s of hours in the first few months[...] We’ve saved already two months of manual work in mitigating vulnerabilities."
Read online

مطارات عُمان
Oman Airports

“We chose Runecast mainly initially looking at the virtualisation layer that we have and ensuring compliance with the best practices that are released by VMware, or even by the other compliance providers like CIS,”
Read online

temperfield
mastery driving into your digital journey

“Runecast does half the work, it shows what issues you have and what you need to do to comply with best practices, security, etc... the other half is to allocate yourself time to decide what is good to focus on first for your specific org or not.”
Read online

SUMMARY

Runecast leverages the power of automation and threat intelligence to help organizations stay ahead of malware and ransomware risks by detecting, managing, and assessing vulnerabilities in their infrastructure. With reduced noise and prioritization by severity, KEV, and impact scores, Runecast provides a platform that requires no learning curve and delivers unparalleled insights into your environment.

By including Runecast in the threat assessment and mitigation workflow, organizations can proactively defend against cyber threats, maintain a secure virtual environment, and free up time for admins to focus on other responsibilities.

Runecast

Gartner
COOL
VENDOR
2020

High
Performer
WINTER
2023

Best
Support
WINTER
2023

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