

SIMPLIFIED SECURITY WITH UNPARALLELED OPERATIONAL TRANSPARENCY

March 2022

AGENDA

- Runecast History
- Managing Infrastructure, Security & Compliance is Complex
- Problems for IT Operations & Security Teams
- Regulatory Compliance
- Runecast Future-Proofs your Organization
- Quick Time to Value
- Engagement Process
- Customer Success Stories

RUNECAST HISTORY

FOUNDERS

"We used to be Admins, and we wasted a lot of time firefighting. After years of that, we did an analysis and realized that over 90% of the root causes were already documented somewhere online."



Stanimir Markov

CEO

VCDX #74
IBM Redbook author
VCI Mentor
Design and architecture



Aylin Sali

CTO

VMware VCAP DCA & DCD
Six Sigma
ELK stack expert
ITIL Certified



Constantin Ivanov

Head of R&D

VMware VCAP DCA & DCD
Microsoft Certified Systems
Engineer



Ched Smokovich

VP of Sales & Marketing

Microsoft Certified IT
Professional
Business Development
ITIL Certified



Ionut Radu

Data Scientist

VMware VCAP
Microsoft specialist
MCTS Hyper-V

2014

THE START OF RUNECAST

A group of ex-IBM virtualization experts had a vision to provide real-time automated insights for mission-critical IT environments – using **human-readable ‘sources of truth’**, using **Natural Language Processing (NLP)** and **Artificial Intelligence (AI)** to create machine-readable rules from it, and building it all into **Runecast Analyzer**.



EDITOR'S CHOICE AWARD

Runecast Analyzer 1.0 was rolled out at VMworld San Francisco. Runecast won an **Editor's Choice Award** from Virtualization Review.



2015

2016

RUNECAS v1.5

Highly scalable **Runecast Analyzer 1.5** was released, supporting multiple vCenters; a Security Compliance focus was added to Runecast Analyzer with automated DISA STIG checks.

TECH TRAILBLAZER

Runecast won a **Tech Trailblazer Award** and was a Finalist for a **CRN Tech Innovators Award**.

2019

RUNECAS v3

Runecast Analyzer 3.0 launched with ESXi upgrade simulations against VMware's HCL, plus auto-remediation workflows. **IDG Connect** named Runecast one of **"20 Red-Hot, Pre-IPO Companies to Watch in the 2019 B2B Tech"** space. Runecast won a €1.9M EU Horizon 2020 grant to accelerate the development of its **Runecast AI Knowledge Automation (RAIKA)** technology.

RUNECAS v4

Runecast Analyzer 4.0 launched support for **AWS cloud**. As well, Runecast earned great recognition with a "VMworld Finalist Award" from **TechTarget** and additional finalist rankings for **Computing** magazine Technology Product Awards (Best Virtualisation Product and Technology Innovator of the Year), a **Computing** magazine Security Excellence Award (Security Automation), and an SDC Award (Digital Transformation Company of the Year).

2021

Releases

Runecast V4.7

Runecast 4.7 launched to give customers the **Cyber Essentials security standard and a ServiceNow Plugin**.

Runecast V5

Runecast 5.0 introduced **coverage for Microsoft Azure!**

Runecast V5.1

Runecast Analyzer 5.1 rolled out **Configuration Vault & Remediation** features and Best Practice analysis for vSphere on Nutanix.

Runecast V6

Runecast 6.0 revealed **OS-level support for Windows and Linux**.

Excellence

Additionally, Runecast earned multiple 2021 'FINALIST' awards, including a UK IT Industry Award for **Security Innovation of the Year** and several via **Computing**: Security Excellence Award for **Risk Management**; Cloud Excellence Award for **Cloud Security Product of the Year (SMEs)**; Digital Technology Leaders Award for **Development Team of the Year**; and AI & Machine Learning Award for **Best Emerging Technology in AI**.

RUNECAS v2

Runecast Analyzer 2.0 launched with a new dashboard and features including historical trending analysis and automated **PCI DSS** and **HIPAA** security checks – now integrated also with **vSAN**, **NSX**, and **Horizon**.

2018

2020

US PATENT

Runecast **obtained a US patent** and was named an EIT Digital Challenge Finalist for "sophisticated, hard-to-reproduce digital technologies that fuel digital transformation."

AWARDS & MORE

Awards and Acknowledgments

- Runecast was named a **Gartner Cool Vendor**
- Won **Computing's** SME awards for **Best Place to Work in Digital and Cloud Security Product of the Year**
- Runecast also won several 'FINALIST' awards, including:
 - Computing's** 2020 Leaders Award for Security Project of the Year
 - Rising Star Award including Company of the Year
 - SDC Awards' Data Security/Compliance Project of the Year

ENTERPRISE

Runecast Analyzer version 4 brought many new capabilities, including:

- Security audits for **CIS Benchmarks**
- SAP HANA** Insights
- NIST** audits for **VMware**

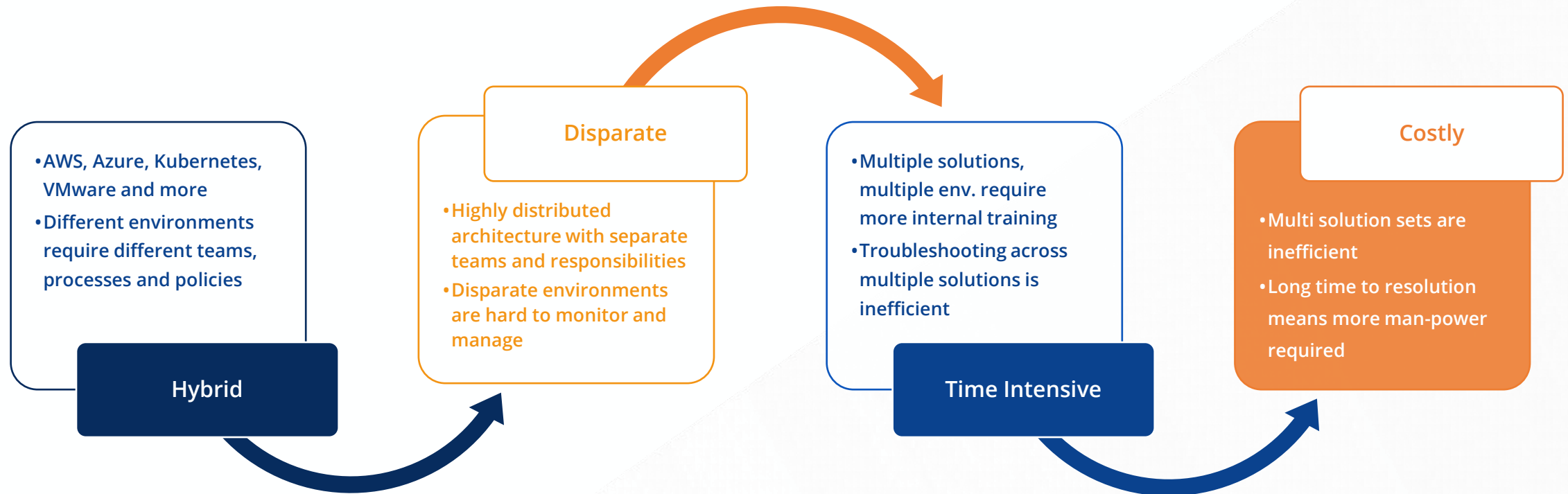
This was followed by:

- A new **Enterprise Console**
- vSphere 7** support
- AWS Audits for **NIST** and **GDPR**
- The launch of **Kubernetes** coverage
- Custom Profiles**
- Security audits for **ISO 27001**
- Coverage for **NSX-T**

Gartner
COOL
VENDOR
2020

MANAGING INFRASTRUCTURE, SECURITY & COMPLIANCE IS COMPLEX

MANAGING INFRASTRUCTURE, SECURITY & COMPLIANCE IS COMPLEX



Modern enterprise is fueled by many different systems. Whether these are cloud, on-prem or hybrid, each requiring monitoring, troubleshooting and security. Managing the complexity of these systems, more often than not, is in the hands of individual teams, using several solutions which in turn leads to disconnect in policies, processes and potentially costly ill-preparedness.

A TYPICAL SOLUTION SET



THE POWER OF RUNECAST

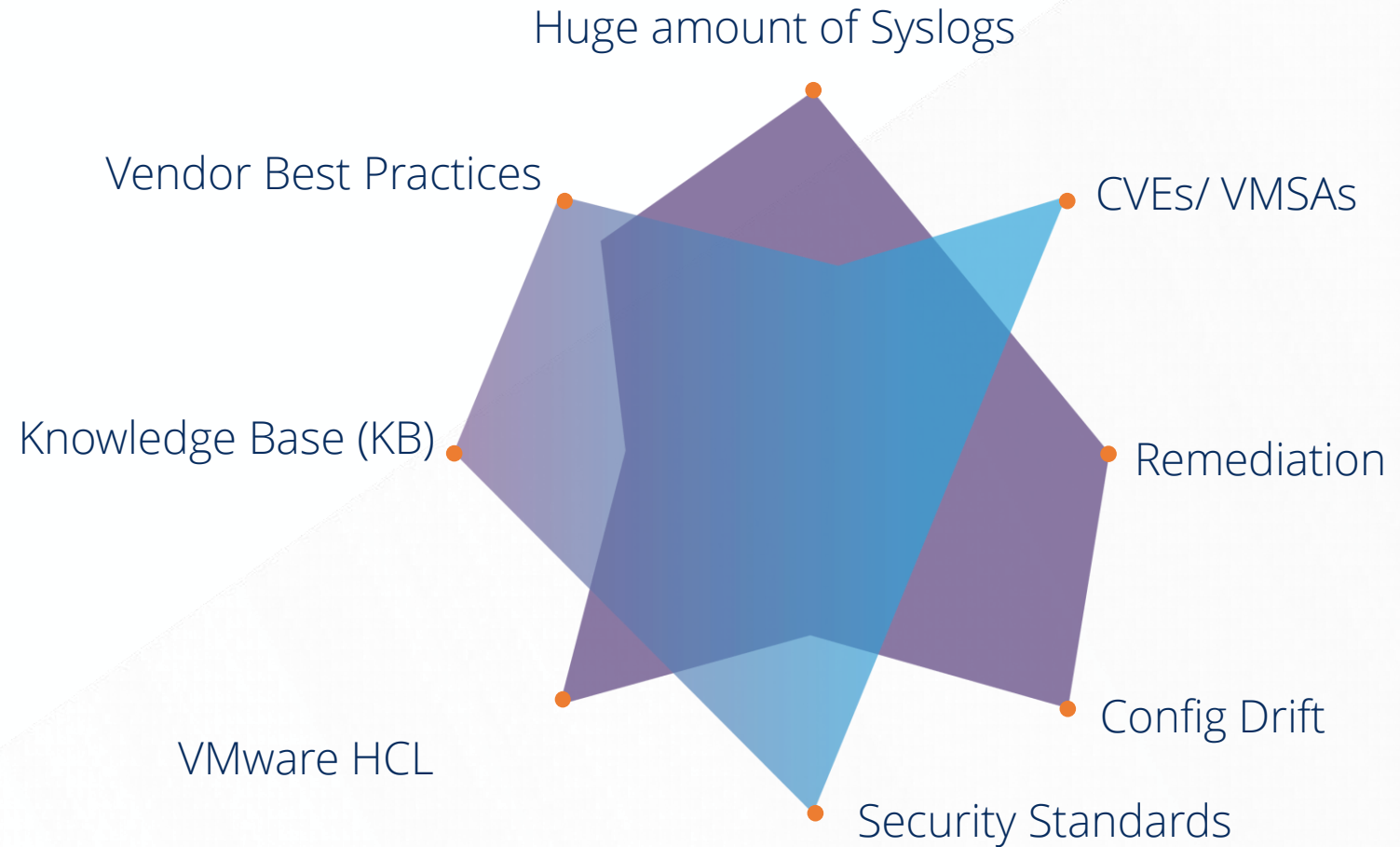
SIMPLIFIED SECURITY WITH UNPARALLELED OPERATIONAL TRANSPARENCY



PROBLEMS FOR IT OPERATIONS & SECURITY TEAMS

TYPICAL INFO CHALLENGES FOR IT SECURITY AND OPERATIONS TEAMS TO STAY ON TOP OF

It's not humanly possible
to keep up with it all



PROBLEMS IN IT OPERATIONS

Over **90% of issues** are already documented, but documentation is used only reactively.

It is no longer humanly possible to monitor known knowledge sources (knowledge bases, best practices, forums, blog articles, social media).

Automation in this area is essential for a proactive approach.

"How are you helping the enterprise realize more value while assessing and managing risk, security and even safety? The best way to bring value to your organization today is to leverage automation."

–Katell Thielemann, VP Analyst, Gartner Security and Risk Management Summit 2019



Break/Fix reactive troubleshooting cycle



Manual Security Compliance efforts



Best Practices **not used**



Increasing complexity and decreasing transparency of IT systems; declining efficiency of IT teams



Skills gap and **costly mistakes** in public/hybrid cloud setups

BEFORE REMEDIATION, THE ROOT CAUSE MUST FIRST BE DISCOVERED

Remediation usually takes hours of searching, reading and filtering through documentation in:

- VMware Knowledge Base
- Best Practices
- Security Hardening Guides
- Forums etc.

This great wealth of knowledge is only being leveraged reactively, after issues happen.

**Now you can apply these
vast resources *proactively***



REGULATORY COMPLIANCE

Regulatory compliance requires that organizations adhere to a set of laws, regulations and/or policies agreed upon by industries and/or governments as an essential level of security.

WHAT HAPPENS WHEN YOU FAIL A COMPLIANCE AUDIT?

Loss of trust/reputation

- Failing a compliance audit (or worse, suffering a breach) can cause long-term damage to the organization, as customers/partners can no longer trust that you are securely handling their data. Such an event can take years from which to recover financially.

Loss of money

- **Fines**
 - If there is a chance that any fines might be covered by banks or insurance companies, e.g. in the event of credit card fraud, won't they somehow try to get it back from you?
- **Lawsuits**
 - Many big-name players have had to pay out MILLIONS in lawsuits after a breach with stolen data exposed. Can your organization afford it?
- **Internal Costs**
 - Failure to pass an audit means reactively spending time and money to investigate why and where those vulnerabilities occurred (costing productivity in parallel). Which teams will suffer most from the additional costs?

Going under a microscope

- If a government agency performing an audit finds the company out of compliance, it will likely put the organization solidly on their radar from that point forward.

HOW WE CAN ENSURE COMPLIANCE

Best Practices Compliance

Best Practices

Severity Layer Affects Products Result Customizable Search 206 issues

Severity	Title	Issue ID	Layer	Affects	Products	Passing	Failing	Unknown	Result
Critical	Ensure Public Network Access Is...	AZURE-GBP-3497	Storage	Security	SQL Server	1	15		Failed
Critical	Ensure EC2 Instance Metadata Service...	AWS-GBP-3754	Compute	Security	EC2	0	15		Failed
Critical	Configure NTP time synchronization	VMW-GBP-874	Compute	Security	vSphere	9	4	7	Failed
Critical	Ensure no security groups allow...	AWS-GBP-2021	Compute	Security	EC2	54	4		Failed
Critical	Ensure there are no Public Accessible...	AWS-GBP-3326	Storage	Security	RDS	1	2		Failed
Critical	Ensure there are no Internet facing...	AWS-GBP-3333	Management	Security	EC2	0	2		Failed
Critical	Ensure Application Load Balancer has...	AWS-GBP-3788	Compute	Security	EC2	0	2		Failed
Critical	Validate that CloudFront...	AWS-GBP-3790	Network	Security	CloudFront	0	2		Failed
Critical	Use supported NSX-T Controller cluste...	VMW-GBP-3148	Management	Availability	NSX-T	0	1		Failed
Critical	Ensure latest TLS Version is used on...	AZURE-GBP-3491	Storage	Security	MySQL Server	0	1		Failed

show 25 entries < Prev 1 2 3 4 ... 9 Next > 206 best practices

Security Compliance

Security Compliance | PCI DSS

Milestone Applies to Products Results Customizable Search

Title	Issue ID	Milestone	Applies to	Products	Objects	Control ID
The system must configure the firewall to restrict access to services running on the host (1.1.4)	VMW-PCIDSS-382	2	Compute	vSphere	4	1.1.4

Details Findings Note Ignore Copy

Issue ID: VMW-PCIDSS-382

Knowledge profile: PCI DSS

Reference: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

Milestone: 2

Applies to: Compute

Technical Description: ESXi hosts have a firewall to control and monitor traffic at the host level. This requirement is addressed through ensuring that access is restricted only to specifically allowed traffic flows. Unrestricted services running on an ESXi host can expose a host to outside unauthorized access. Reduce the risk by configuring the ESXi host to allow access from authorized networks.

CHECK DESCRIPTION: From the vSphere Client select the ESXi Host and go to Config Security Profile. Under the Firewall section select properties and enabled service click Firewall and review the allowed IPs, or From a PowerCLI command prompt while connected to the ESXi host run the following command:

Configure the ESXi host firewall to restrict access to services running on the host (1.2.1)	VMW-PCIDSS-1626	2	Compute	vSphere	4	1.2.1
Ensure no ACL allows incoming connections from ALL sources to ALL ports and protocols (1.2.1)	AWS-PCIDSS-2050	2	Network	VPC	23	1.2.1
Ensure that the Forged Transmits policy is set to reject: reject-forged-transmit (1.3.3)	VMW-PCIDSS-594	2	Network	vSphere	33	1.3.3
Ensure that the Forged Transmits policy is set to reject: reject-forged-transmit-dvportgroup (1.3.3)	VMW-PCIDSS-500	2	Network	vSphere	1	1.3.3
Ensure that the MAC Address Change policy is set to reject: reject-mac-changes (1.3.3)	VMW-PCIDSS-595	2	Network	vSphere	33	1.3.3

Hardware Compliance

Configuration Vault

View Selected analysis Hosts October 11, 2021, 3:01 AM (latest) Check historical drift Show charts

Connection state

Vendor

Model

Hosts differences 0 unchanged 7 changed

Filter any column...

Differences	Name	Connection state	Vendor	Model
Remove baseline	Desired configuration baseline:	CONNECTED	VMware, Inc.	VMware7,1
Changes: 20	10.0.0.11 Office Lab > host > 10.0.0.11 > 10.0.0.11	NOT_RESPONDING	HP	ProLiant DL360p Gen8
Changes: 17	delimos.solar.system Solar System > host > SOLAR Cluster >	CONNECTED	Dell Inc.	PowerEdge R640
Changes: 17	moon.solar.system Solar System > host > SOLAR Cluster >	CONNECTED	Dell Inc.	PowerEdge R640

CHOOSE FROM A MULTITUDE OF COMPLIANCE OPTIONS (IN ADDITION TO CUSTOM PROFILES)



Bundesamt
für Sicherheit in der
Informationstechnik



RUNECAST FUTURE-PROOFS YOUR ORGANIZATION

RUNECAST OVERVIEW

Proactive, patented platform for vulnerability and configuration drift management, security compliance, best practice alignment and remediation in the areas of:

- IT Operations Management (ITOM)
- Cloud Security Posture Management (CSPM)
- Kubernetes Security Posture Management (KSPM)

Using Runecast AI Knowledge Automation (RAIKA) with a patented rules engine, it analyzes the IT infrastructure – including the OS level – and exposes potential issues before they can cause major outages or lead to security breaches.

Security Hardening Guides
BSI, CIS, Cyber Essentials,
DISA STIG, Essential 8,
GDPR, HIPAA, ISO 27001,
NIST, PCI DSS

VMware Knowledge Base
VMware HCL

Best Practices
Blogs
Social Media



vSphere

vSAN

NSX

Horizon

vCD

K8s

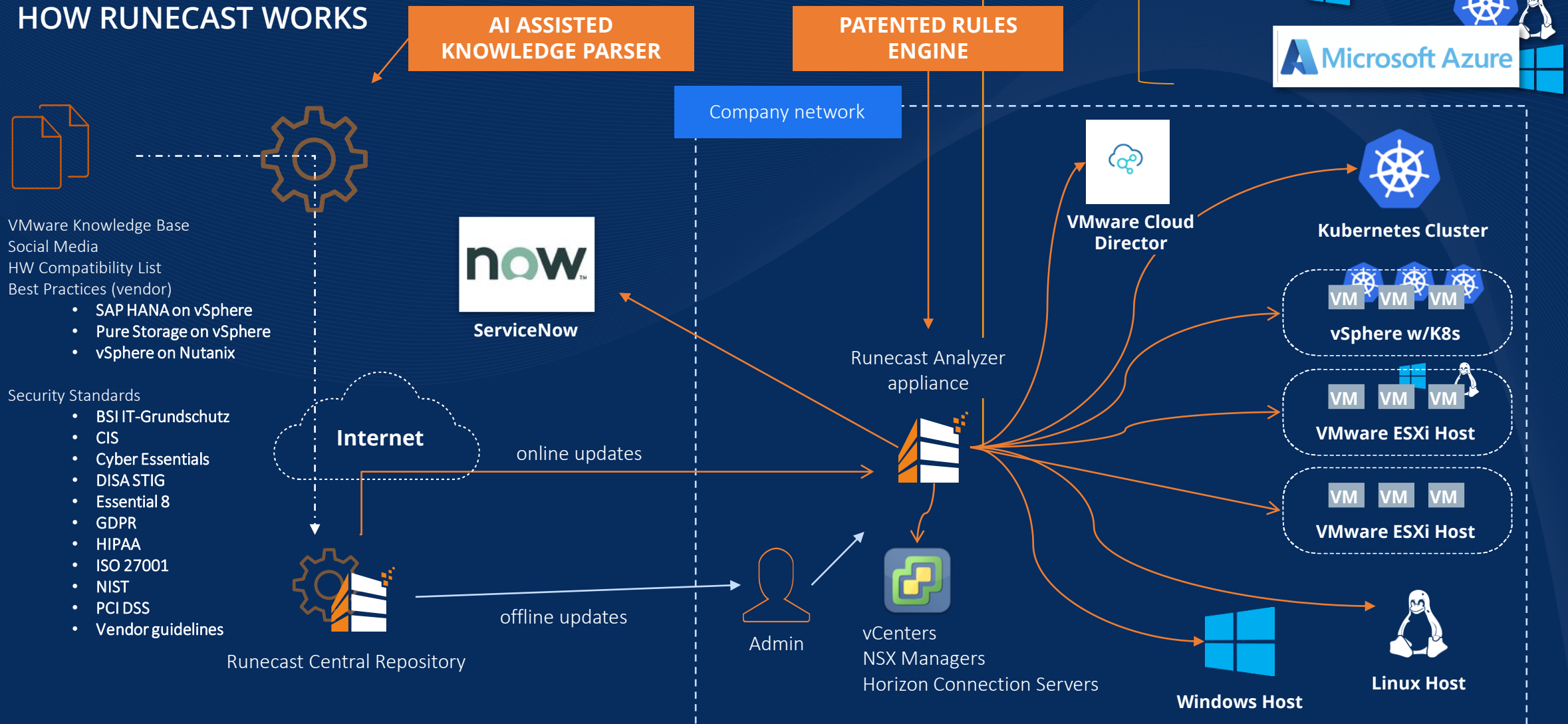
AWS

Azure

Windows

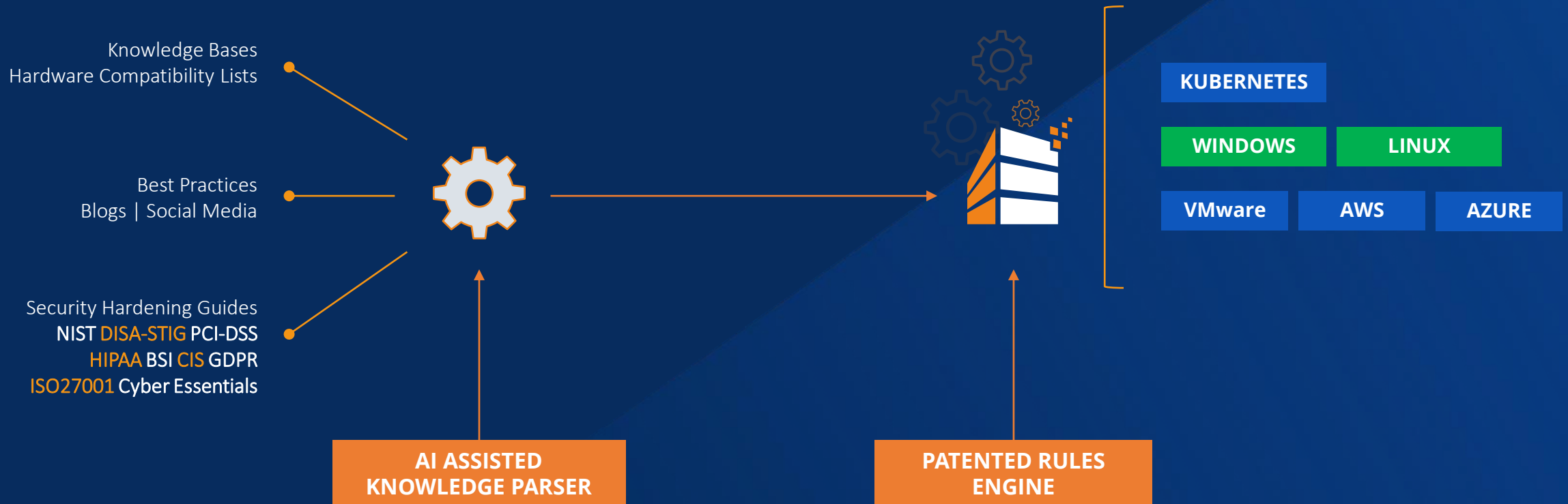
Linux

HOW RUNECAST WORKS



HOW RUNECAST WORKS (SIMPLIFIED)

Proactive Hybrid Cloud management – uses **AI assisted knowledge parsing** and **patented rules engine** to **expose risk** before they cause **outages** or **security issues**.



SCOPE OF COVERAGE

	Configuration Drift Management	Security Compliance Management	Vulnerability Management	Proactive Problem Management	Agentless	Upgrade Planning
VMware	✓	✓	✓	✓	✓	✓
Kubernetes	✓	✓	✓	✓	✓	
AWS	✓	✓	N/A	✓	✓	N/A
Azure	✓	✓	N/A	✓	✓	N/A
Windows	✓	✓	✓			
Linux	✓	✓	✓			

NEW WINDOWS & LINUX COVERAGE (DIFFERENTIATORS)



Leverages an agent that is **secure, lightweight and easy to deploy and maintain**



Integrates with our **patented rules engine**



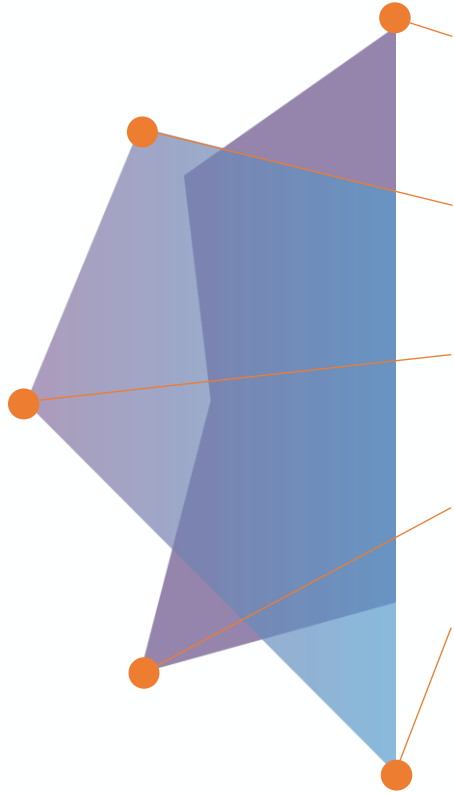
Displays in the same Runecast UI for **single point of control**



Covers **vulnerability assessment, security compliance assessment, configuration drift management**



Provides **fully offline capabilities scan**



Proactive ITOM, CSPM, KSPM
aligned to best practices.

Configuration Analysis
to get ahead of drift.

Security Compliance Checks
to keep you audit-ready.

Upgrade Simulations
against VMware HCL
to see future impact.

Log Analysis
in real-time against KBs to
find problematic logs.

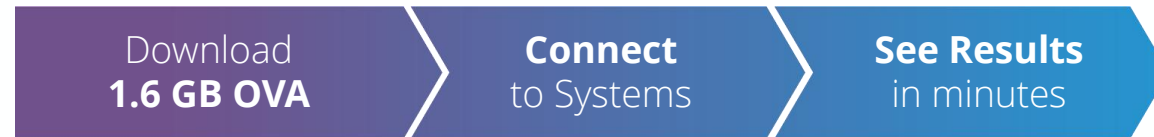
CORE CAPABILITIES

Runecast proactively identifies the **known causes** of issues before they occur, does all the root cause analysis work for you and provides the solution to remediate.

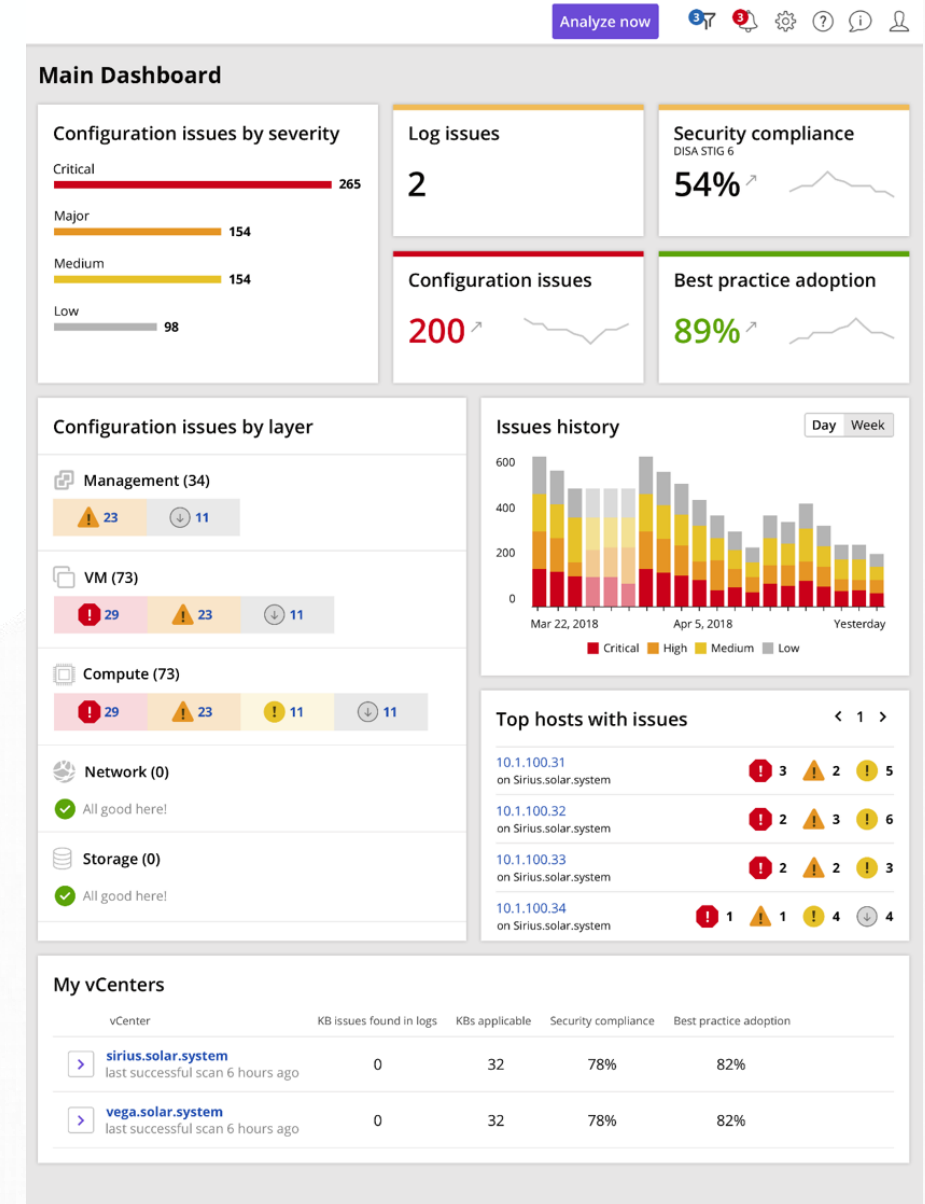
All of that with REMEDIATION
for major time savings.

QUICK TIME TO VALUE

EASE OF DEPLOYMENT



- 5-minute deployment, near real-time results, intuitive UI
- Eliminates complexity and the need for strong technical expertise and manual efforts
- Proactive detection of all known issues and recommendations
- Automated security compliance audits (over 10 standards)
- Validates and simulates hardware against current HCL and upgrades
- Secure architecture, highly scalable with a single virtual appliance. All data stays under your control



CUSTOMERS REPORT IMMEDIATE ROI



Major time savings

Less time troubleshooting. Faster time to resolution.



Reduced outages

Discover and remediate hidden issues before they cause outages.



Improved security

Continuous security compliance, security KBs, secure architecture.



Minimized risk with continuous compliance

Your environment now follows industry best practices and is optimally configured.



Reduce costs

Prevent outages, save time and avoid audit penalties.

CISOs, CIOs, SECURITY AND OPS TEAMS THAT BENEFIT FROM RUNECAST INTELLIGENCE

OUR CUSTOMERS REPORT:

- Between 75% to 90% time saved on troubleshooting and upgrade planning
- Up to 100% uptime
- Increased operational efficiency and observability
- 100% of required security audits passed successfully

Source: Runecast Customer Success Stories



de volksbank



DocuSign®



A FEW KEY BENEFITS

Deploy and configure in the time it takes to get a cup of coffee

Deploys as an OVA, Helm chart or natively from cloud marketplaces

Single platform with insights for AWS, Azure, Kubernetes, VMware, Windows, Linux

vSphere, vSAN, NSX, Horizon & VMware Cloud Director

Certified for VMware Cloud on AWS

Never uploads data from your environment

Extremely fast and Easy-to-use

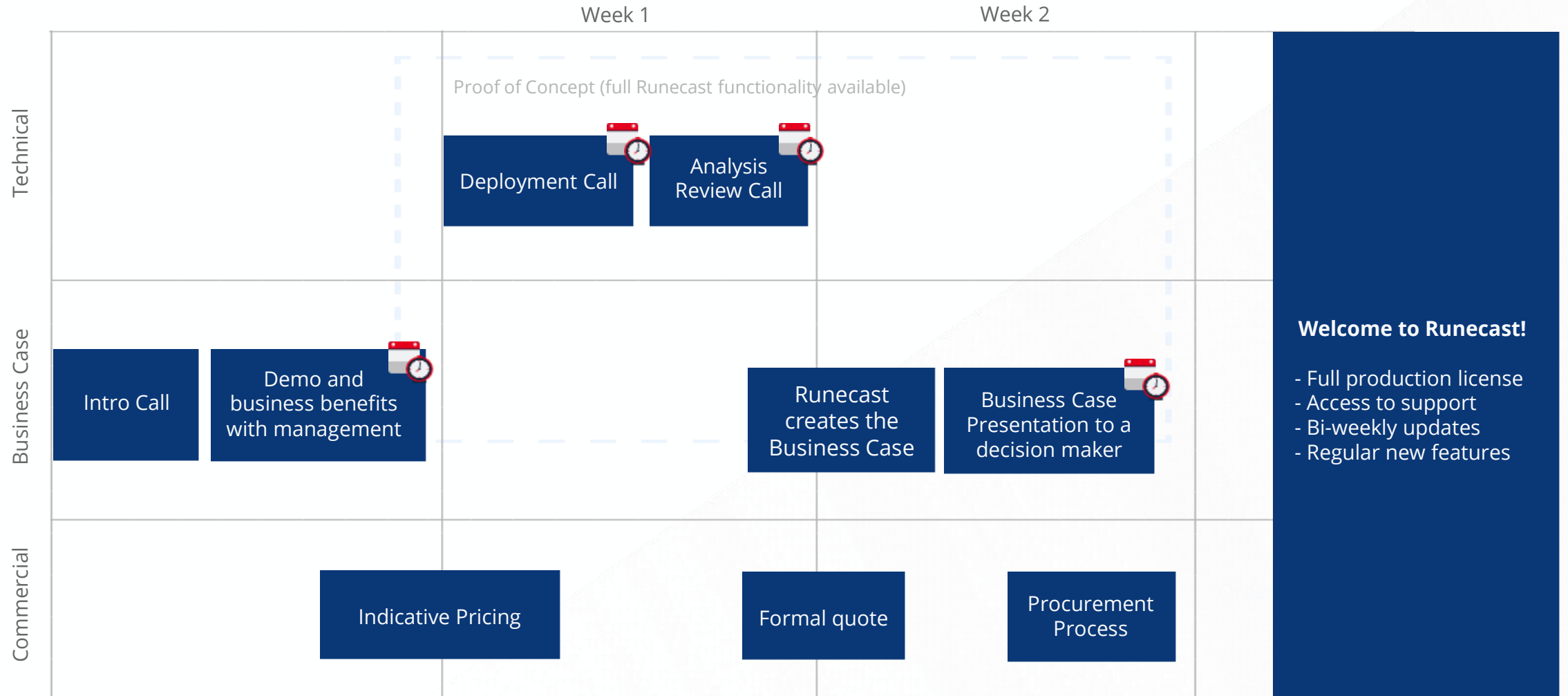
RESTful API, vSphere Client plugin, ServiceNow integration

Remediation through Power CLI and Ansible scripts

Support extends also to the OS level (Windows & Linux)

ENGAGEMENT PROCESS

ENGAGEMENT PROCESS



CUSTOMER SUCCESS STORIES

SUCCESS STORY

NOTINO

Retail/eCommerce | Global

HIGHLIGHTS

- VMware related incidents reduced by 80% (from 5 a month to 1 a month)
- Identified and prevented 10 VMware issues in the first two weeks
- Full FTE was freed up to focus on business critical issues rather than issue troubleshooting
- Minimum savings: 78,000 EUR per year (VMware Support) + FTE
- Less reliant on external support



NOTINO

T O D A Y I S Y O U R S

“Runecast saves us from issues before they happen, the value of which cannot be overstated. In addition, Runecast’s real-time data saves us weeks and months that were previously spent on dealing with VMware support.”

Michal Kopečný
IT Administrator

SUCCESS STORY

NEAR EAST BANK

Banking/Financial | North Cyprus

HIGHLIGHTS

- Runecast revealed +30 issues (some Critical or Major) in a single week
- Team is now able to resolve issues proactively
- Able to more efficiently utilize current staff
- 90% time savings on reactive troubleshooting
- Customizable reporting options demonstrate compliance
- Time freed up to deliver more value from IT ops



“Runecast Analyzer has helped us to mitigate risk by improving our security and ensuring we are compliant. We can now also prove our compliance when necessary.”

Renan Avni
IT Group Manager

SUCCESS STORY

DHU Health Care

Healthcare (NHS service provider) | UK

HIGHLIGHTS

- About 10 minutes to deploy & get a first scan
- Revealed pre-Runecast approach as reactive at best
- Critical issues now visible, able to be worked on proactively
- Know exactly which issues to prioritize and work on first
- Stability of mission-critical urgent-healthcare systems (i.e. NHS 111 emergency call service)
- Easy to justify the investment



"We didn't really know that we had such a problem of addressing issues only reactively until we saw the contrast[...] With Runecast, we can now look at one screen and have the visibility and transparency to know what we are working on and why."

Nathanael Pearson
Head of IT & Telecoms

SUCCESS STORY

FLEXdata Solutions Pty Ltd

IT Services | Australia

HIGHLIGHTS

- Minimum of 60-70% time savings
- Expected 90% time savings in upgrade planning
- Deployment and first analysis report took only 15 minutes
- Prevented an ESXi host crash and post-incident review (PIR)
- Provides a proactive security compliance posture
- Extends value back to clients



“Runecast Analyzer was a no-brainer, we instantly saw that it would save us a whole lot of time, and for us time is money.”

Luke Mulcahy
Solution Architect / Director

SUCCESS STORY

German Aerospace Center (DLR)

Aerospace | Germany

HIGHLIGHTS

- Early, proactive information about potential bugs and security risks that could lead to severe or critical operational problems
- More leverage in keeping vSphere environment up to date
- Advance warning of potential problems
- Increased stability and performance
- Helping them to stabilize greenhouse mission to grow food in space



DLR
Deutsches Zentrum
für Luft- und Raumfahrt

"We use Runecast Analyzer mostly as a solution to warn us of potential problems with new versions or updates before they manifest as real issues. Runecast Analyzer increases the stability and performance of our environment."

Michael Szczuka
Senior Engineer

SUCCESS STORY

University of St Andrews

Education | Scotland

HIGHLIGHTS

- 80% reduction in monthly incidents and issues
- Identified/Corrected misconfigured NTP & syslog settings
- Visibility over configuration & adherence to best practices
- 75-85% troubleshooting time savings
- Simple, functional tool that requires very little configuration
- Runecast team “impressively responsive” to feedback



University of
St Andrews

“Runecast was up and running within a couple of hours. It is a very simple, yet powerful, cost-effective solution.”

Jason Cormie
Technical Architect

Visit runecast.com
to request a trial and/or PoC for your
environment

Or reach out to us at roi@runecast.com