The Role of OT Asset Management in ICS

Rockwell Automation

expanding **human possibility**®

VERVE
by ROCKWELL AUTOMATION

Safety Moment: Zero Trust for Device Cybersecurity

> Cybersecurity starts with you. A single vulnerable device can put your personal data at risk

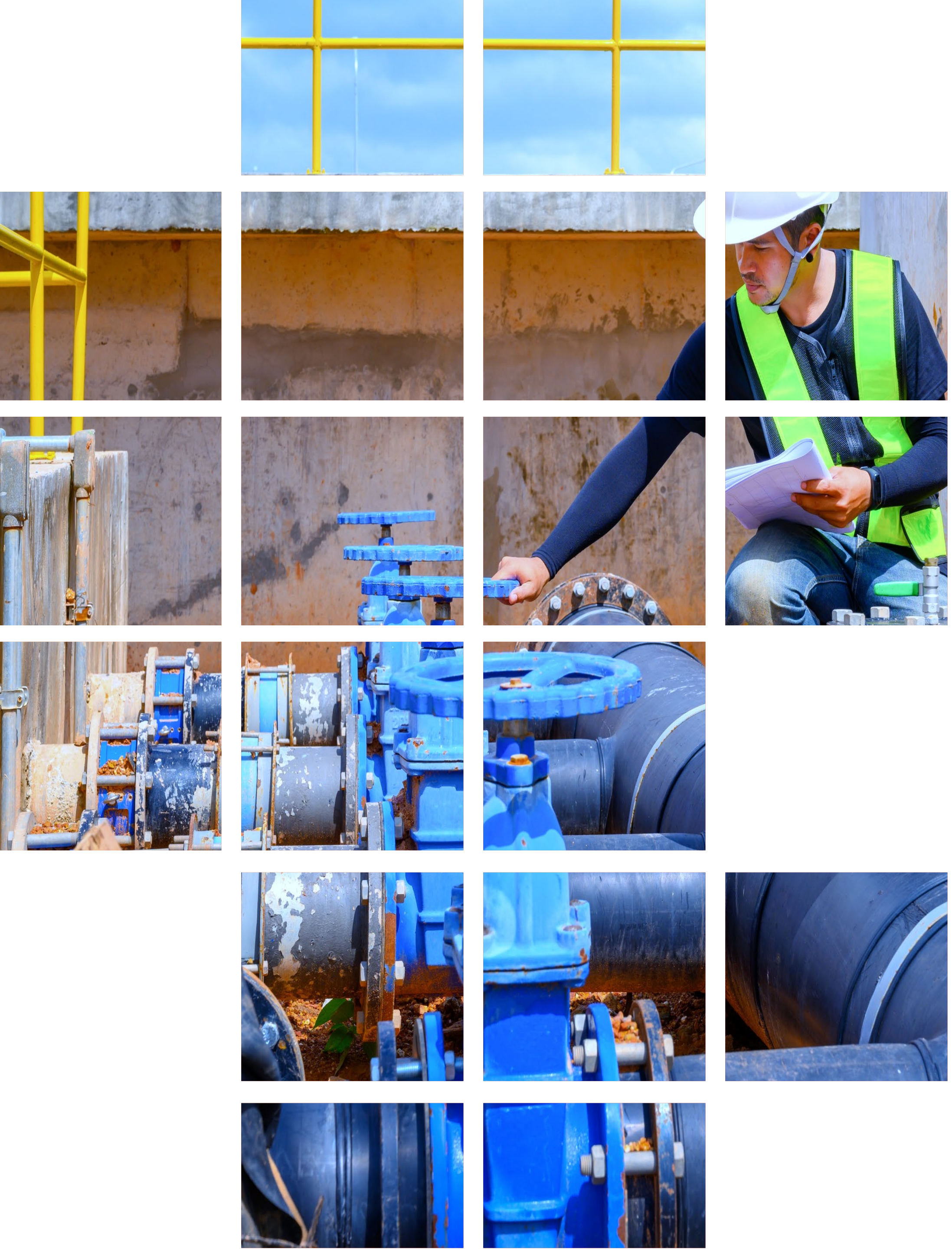
Why It Matters:

In today's connected world, every device—laptops, smartphones, IoT sensors, or industrial controllers—can be an entry point for cyberattacks. Traditional security models assume devices inside the network are trustworthy. **Zero Trust flips that assumption: trust nothing, verify everything**

Key Messages:

1. **Don't Assume Safety:** Even trusted devices can be compromised. Always verify before sharing sensitive info
2. **Update Regularly:** Install software and security updates as soon as they're available
3. **Use Strong Authentication:** Enable multi-factor authentication (MFA) on all accounts and devices
4. **Limit Access:** Only connect devices you truly need, and avoid using public Wi-Fi without a VPN
5. **Stay Alert:** Watch for unusual behavior—slow performance, unexpected pop-ups, or unknown apps.

INTERNAL • Copyright ©2025 Rockwell Automation, Inc.



Agenda

- Introduction
- Setting the scene – why?
- Multi-dimensional data model
- Resulting Insights
- Q&A

CONFIDENTIAL • Copyright ©2025 Rockwell Automation, Inc.

Rick Kaun

Rockwell Automation

Industrial Security Challenges

AGING INFRASTRUCTURE

In 2024, the average age of industrial equipment was 9.1 years

LACK OF VISIBILITY

80% of vulnerabilities reside deep within the ICS network

OT CYBER SKILLS GAP

Cybersecurity is the #1 skill manufacturers are seeking

REGULATORY REQUIREMENTS

74% of executives expect regulatory pressure on OT security to increase

COMPLEX SUPPLY CHAINS

65% of attacks on critical infrastructure expand into supply chains

PUBLIC • Copyright ©2025 Rockwell Automation, Inc.

Asset and Network Security Challenges

Assets

- Lack of asset ownership and responsibilities
- Managed and unmanaged assets on the plant floor
- Legacy hardware and operating systems
- Large variety of asset types
- Difficult to patch

Network

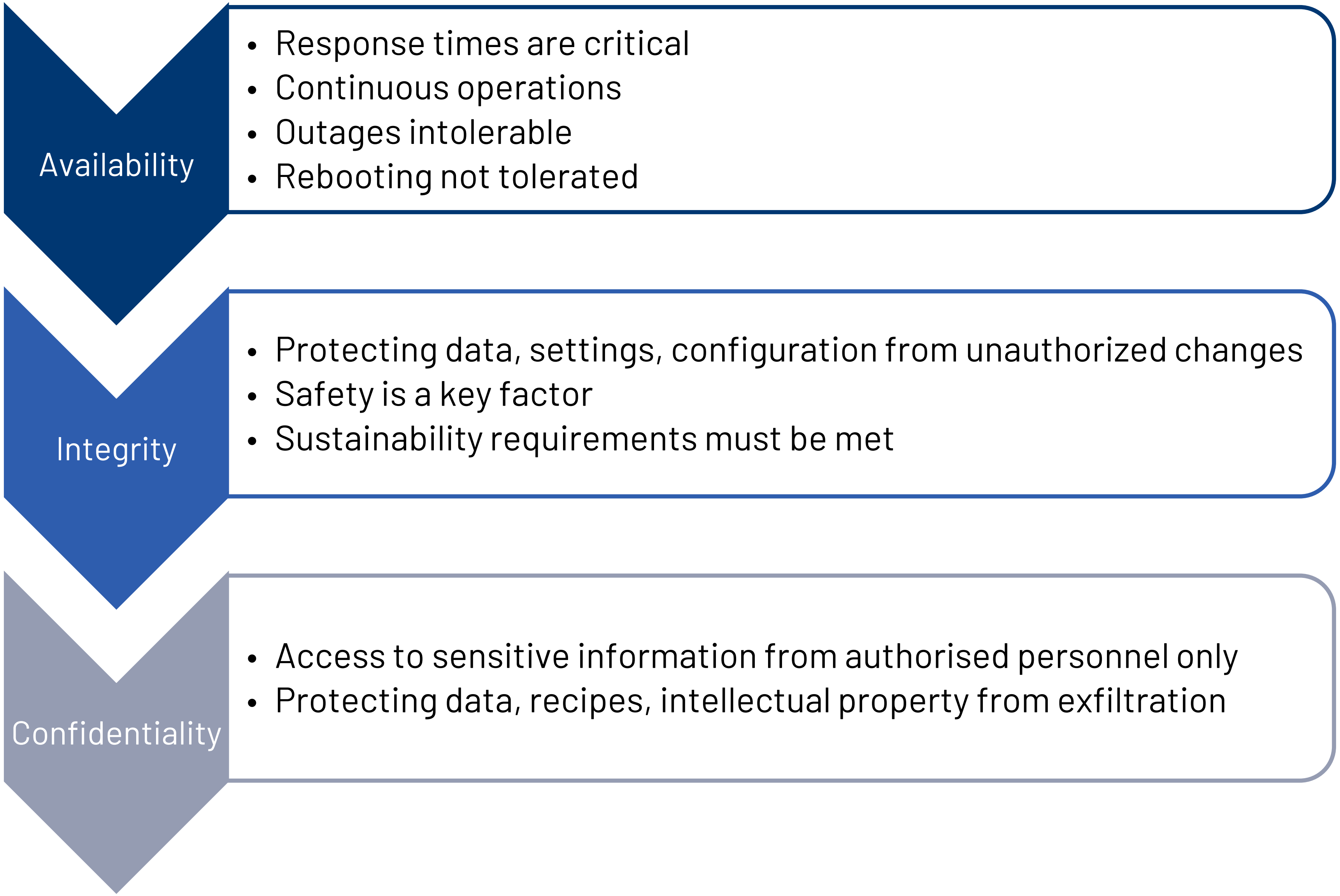
- Network complexity, many different types of communication and network protocols in place
- Legacy networking equipment
- Lack of network connectivity throughout sites
- Networks have grown organically, not designed with intent or security in mind

Policy and Procedures

- Lack of defined ownership or access control of assets on the plant floor
- No defined maintenance plans for security updates
- Poorly maintained asset inventories

PUBLIC • Copyright ©2024 Rockwell Automation, Inc.

Security Priorities, Getting it Right



Availability

- Response times are critical
- Continuous operations
- Outages intolerable
- Rebooting not tolerated

Integrity

- Protecting data, settings, configuration from unauthorized changes
- Safety is a key factor
- Sustainability requirements must be met

Confidentiality

- Access to sensitive information from authorised personnel only
- Protecting data, recipes, intellectual property from exfiltration

The priorities are different in an OT or IACS environment compared to that of an IT or enterprise

Not all control systems are created equally

ISA62443-1-1, sub clause 5.2 Security Objectives

Remediation in OT is different...

- Legacy equipment doesn’t support modern IT security tools
- Scanning of endpoints can cause disruptions
- Automated remediation can cause bigger problems
- We want to be ‘like IT’ but we are just not

70%

OT assets are non-Windows

8-10 years

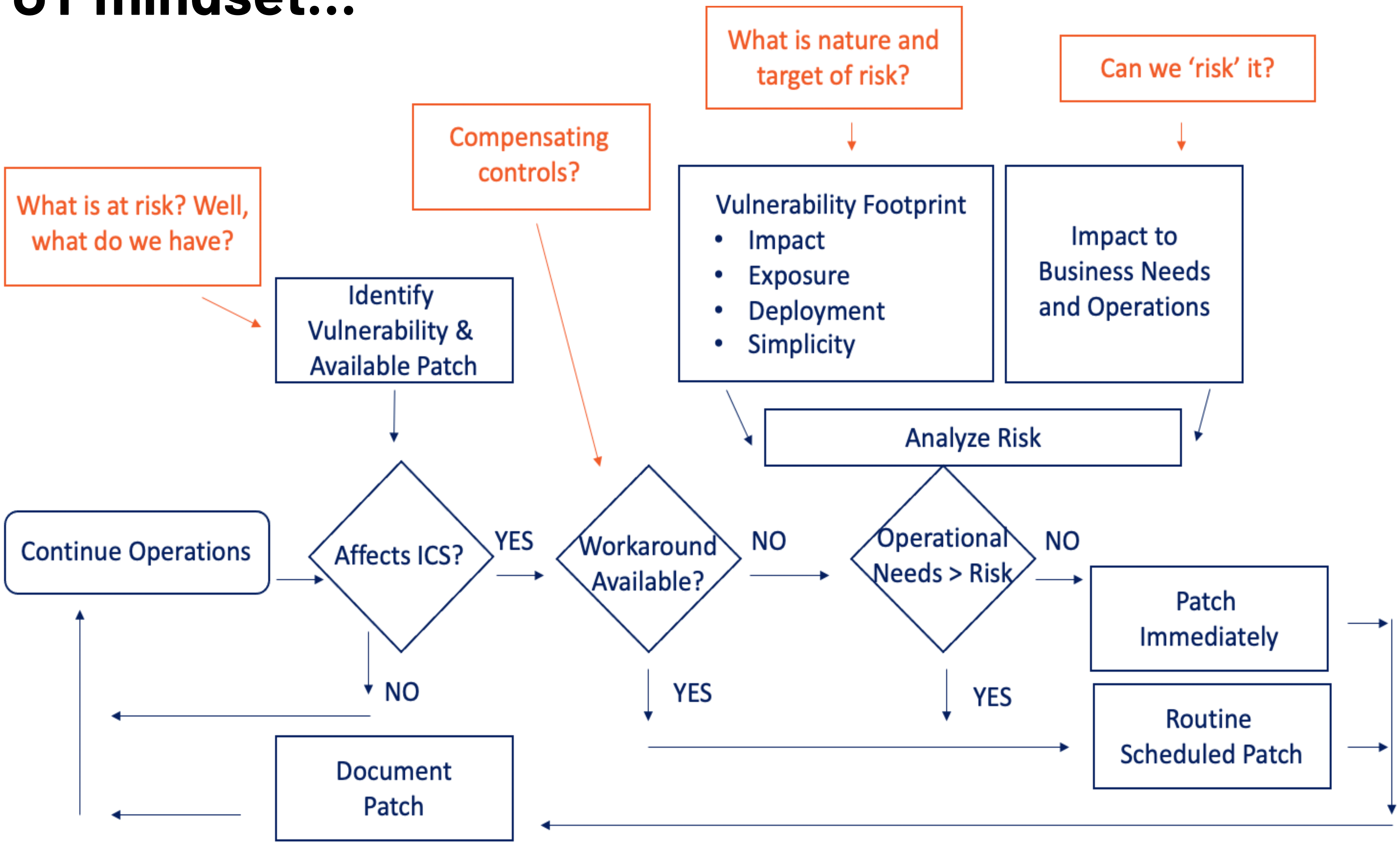
Average age of OT device kernel

>450

Different ICS/OT protocols (majority unsecured)

VERVE by ROCKWELL AUTOMATION

Typical OT mindset...



What is at risk? Well, what do we have?

Compensating controls?

What is nature and target of risk?

Can we 'risk' it?

Identify Vulnerability & Available Patch

Vulnerability Footprint

- Impact
- Exposure
- Deployment
- Simplicity

Impact to Business Needs and Operations

Analyze Risk

Continue Operations

Affects ICS?

Workaround Available?

Operational Needs > Risk

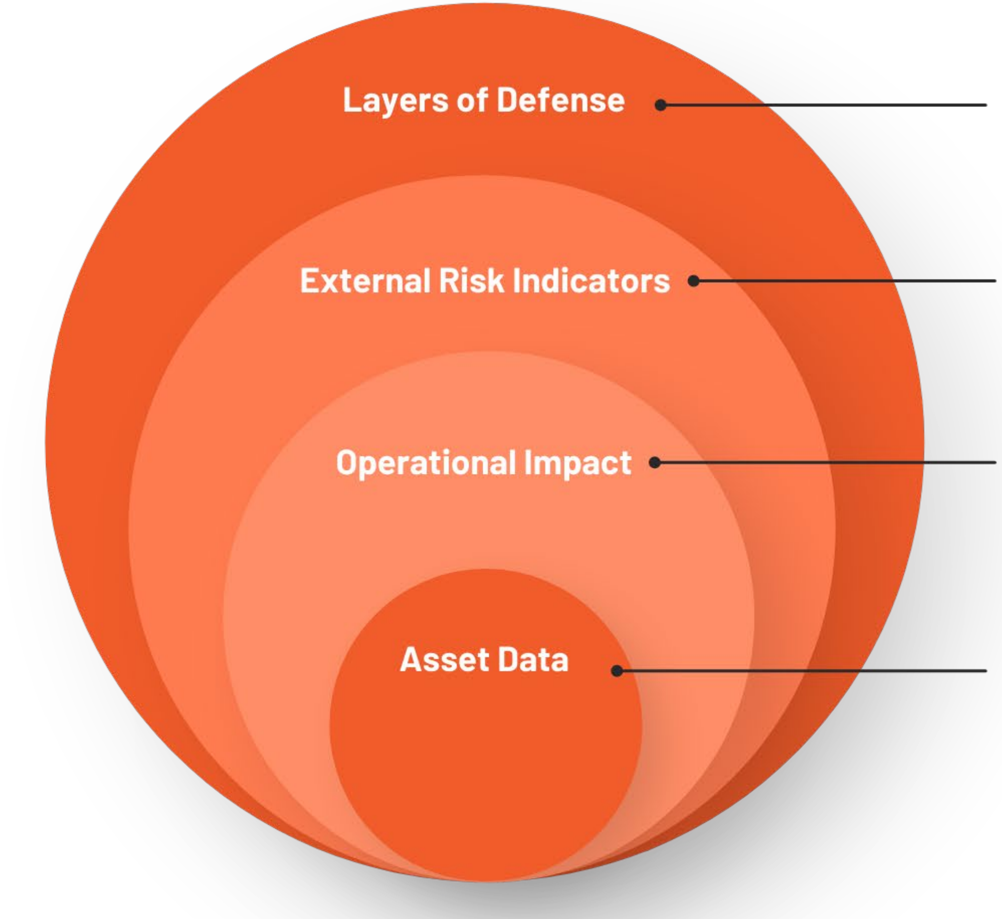
Patch Immediately

Routine Scheduled Patch

Document Patch

CONFIDENTIAL • Copyright ©2025 Rockwell Automation, Inc.

How to build context in the OT environment



Backups • Segmentation • AV/WL
Identifies and verifies security layers in place — enabling faster incident response and targeted improvements.

Vulnerabilities • Exploits • Patches • Advisories
Surfaces exploitable vulnerabilities in context — helping teams act on what's relevant now, not just what's theoretically risky.

Process Criticality • Downtime Impact
Prioritizes remediation based on operational risk — not generic IT metrics — so the most critical assets get secured first.

Config • Users • Software • EOL • Type
Provides a live, unified asset inventory — essential for visibility, compliance, and action across all NIST-CSF functions.

CONFIDENTIAL • Copyright ©2025 Rockwell Automation, Inc.

The importance of accurate Risk Scoring

A risk score is produced by a risk formula

Each asset has a score

Scores update dynamically as details of the asset change

Formulas are consistent across an instance

Asset Criticality

Manual property or simple calculated field, describes business criticality of the asset

×

Likelihood

Manual property used to let operators indicate which parts of their environment seem more/less protected

×

Exposure

Dynamically derived based on Verve®'s knowledge of asset state (as reflected by properties). Is composed of several selected "risk factors", each of which have a corresponding weight.

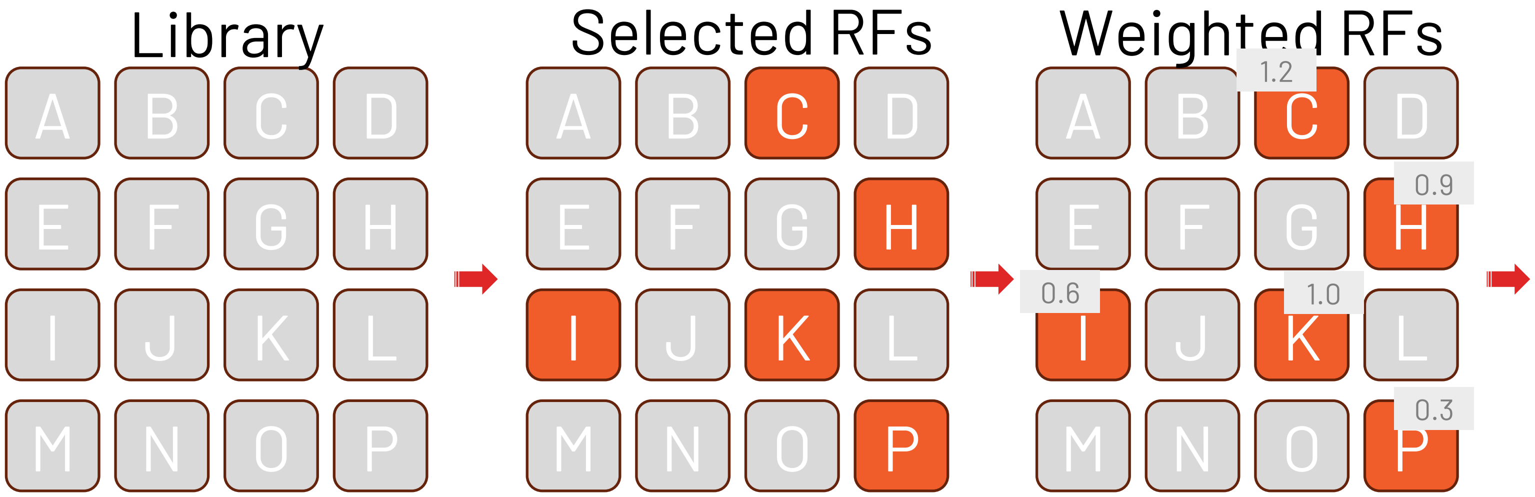
= **Risk Score**

Risk Scoring – Exposure & Risk Factors

A *risk factor (RF)* turns *property values* into a normalized indication of one kind of risk

- RFs are special (calculated) properties
  - RFs update dynamically with PVs of other properties
- Most RFs are configurable
- RF values are in the set (null, 0-100)

- A library of ~50 pre-defined RFs to choose from
- 0..N of them are *added* to a risk formula ("enabled")
  - No arbitrary limits on how many, but
  - We recommend ~5-10 to be used in a normal case
- Each selected factor has a weight (default 1) that determines its importance vis-à-vis other enabled factors



Exposure Calculation

$$\text{Exposure} = \frac{(1.2*C)+(0.9*H)+(0.6*I)+(K)+(0.3*P)}{1.2+0.9+0.6+1+0.3}$$

Note: exposure will always be in the range 0..100 (because math)

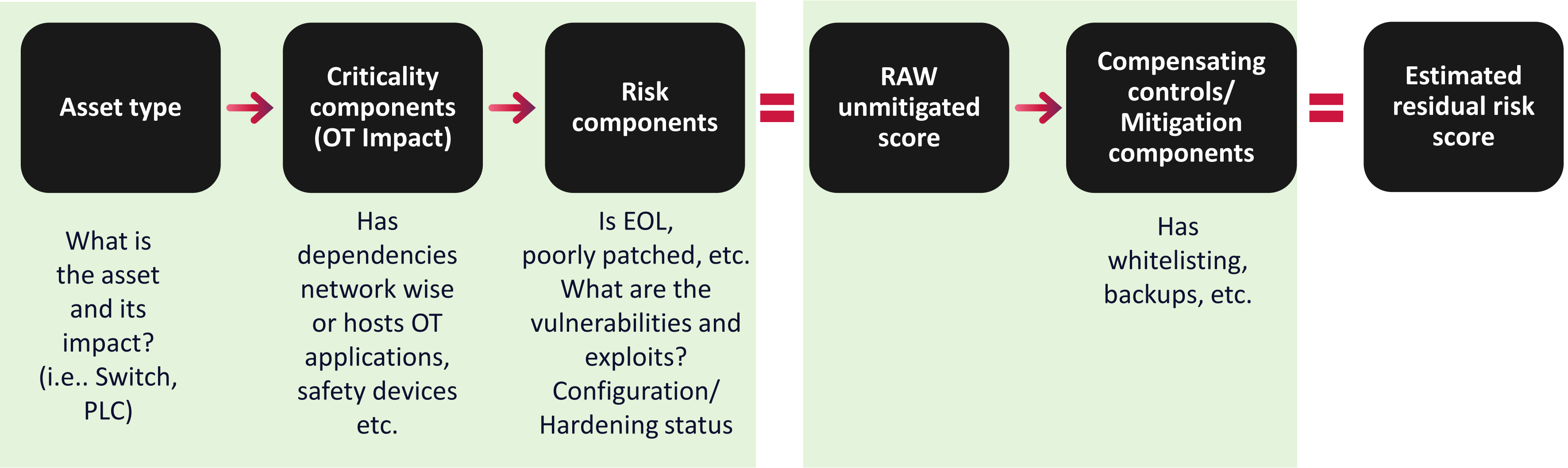
Enhancing OT security with Verve's risk prioritization

Identify & prioritize:
Categorize OT assets for focused protection of critical elements.

Assess & analyze:
Evaluate risks considering asset importance and vulnerabilities like EOL status.

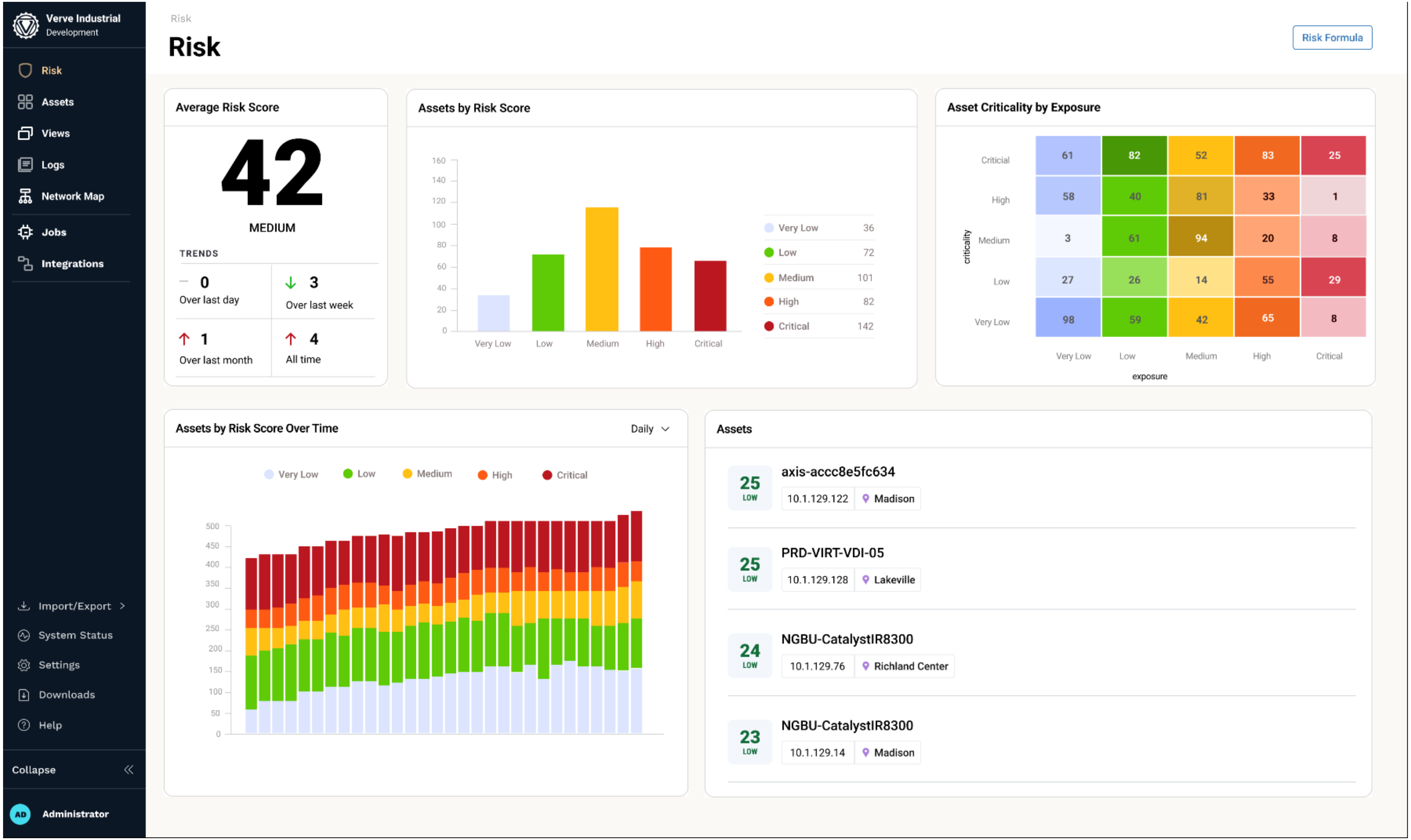
Mitigate & control:
Apply targeted mitigations, such as whitelisting and backups, to lower exposure.

Evaluate & adjust:
Review risk scores before and after mitigation, adjusting for asset significance and evolving threats.


Asset type
Criticality components (OT Impact)
Risk components
=
RAW unmitigated score
Compensating controls/ Mitigation components
=
Estimated residual risk score
What is the asset and its impact? (i.e.. Switch, PLC)
Has dependencies network wise or hosts OT applications, safety devices etc.
Is EOL, poorly patched, etc. What are the vulnerabilities and exploits? Configuration/ Hardening status
Has whitelisting, backups, etc.

User Visible Label	Backend Score Ranges
Critical	76-100
High	51-75
Medium	26-50
Low	1-25

Benefits:
Resource Allocation: Optimize and prioritize security resource deployment for maximum impact.



Risk

Risk

Average Risk Score

42

MEDIUM

TRENDS

— 0 Over last day	↓ 3 Over last week
↑ 1 Over last month	↑ 4 All time

Assets by Risk Score

● Very Low	36
● Low	72
● Medium	101
● High	82
● Critical	142

Asset Criticality by Exposure

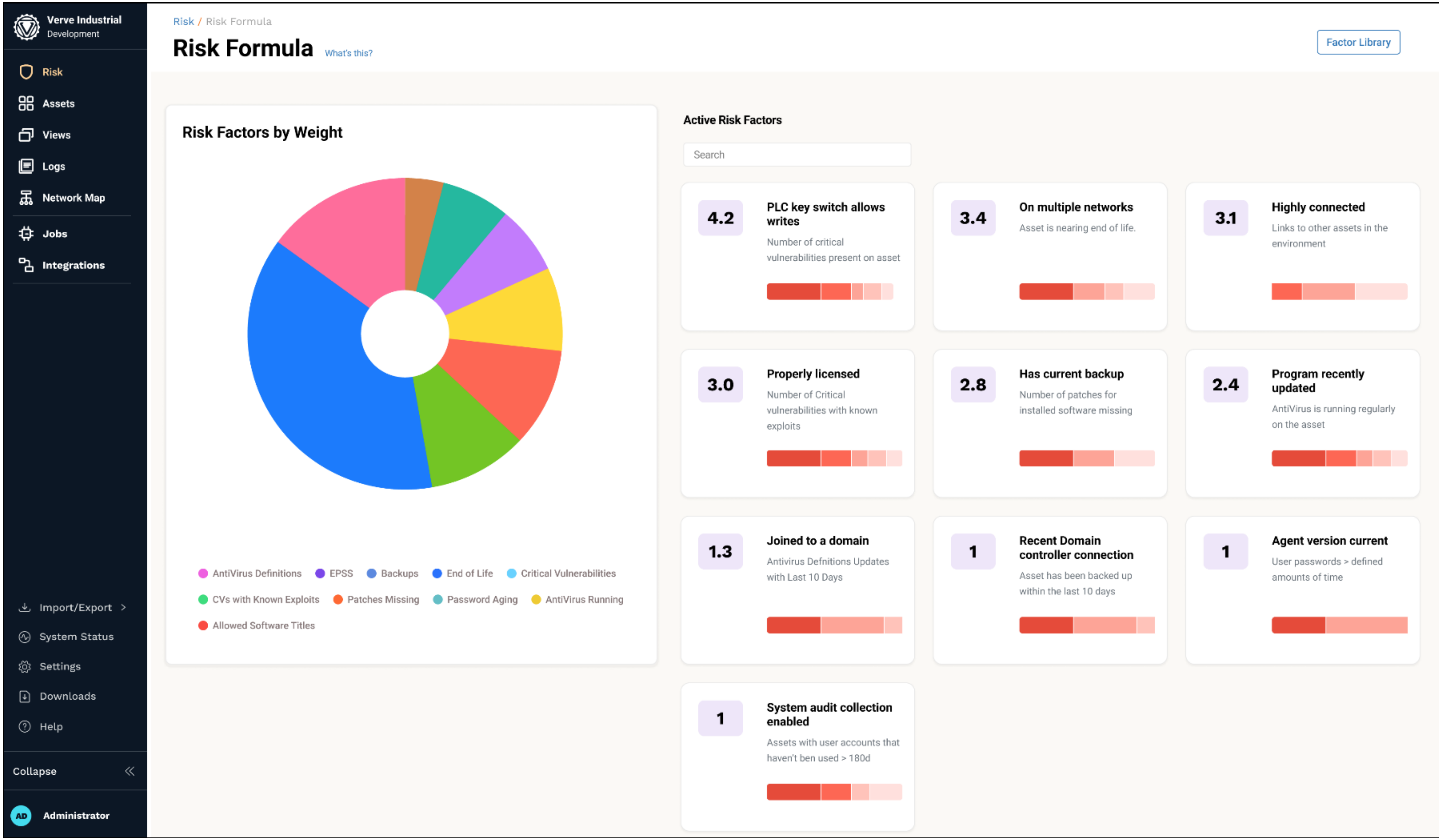
criticality \ exposure	Very Low	Low	Medium	High	Critical
Criticial	61	82	52	83	25
High	58	40	81	33	1
Medium	3	61	94	20	8
Low	27	26	14	55	29
Very Low	98	59	42	65	8

Assets by Risk Score Over Time

Assets

25 LOW	axis-accc8e5fc634	10.1.129.122	Madison
25 LOW	PRD-VIRT-VDI-05	10.1.129.128	Lakeville
24 LOW	NGBU-CatalystIR8300	10.1.129.76	Richland Center
23 LOW	NGBU-CatalystIR8300	10.1.129.14	Madison

CONFIDENTIAL • Copyright ©2025 Rockwell Automation, Inc.



Risk Formula

What's this?

Risk Factors by Weight

Active Risk Factors

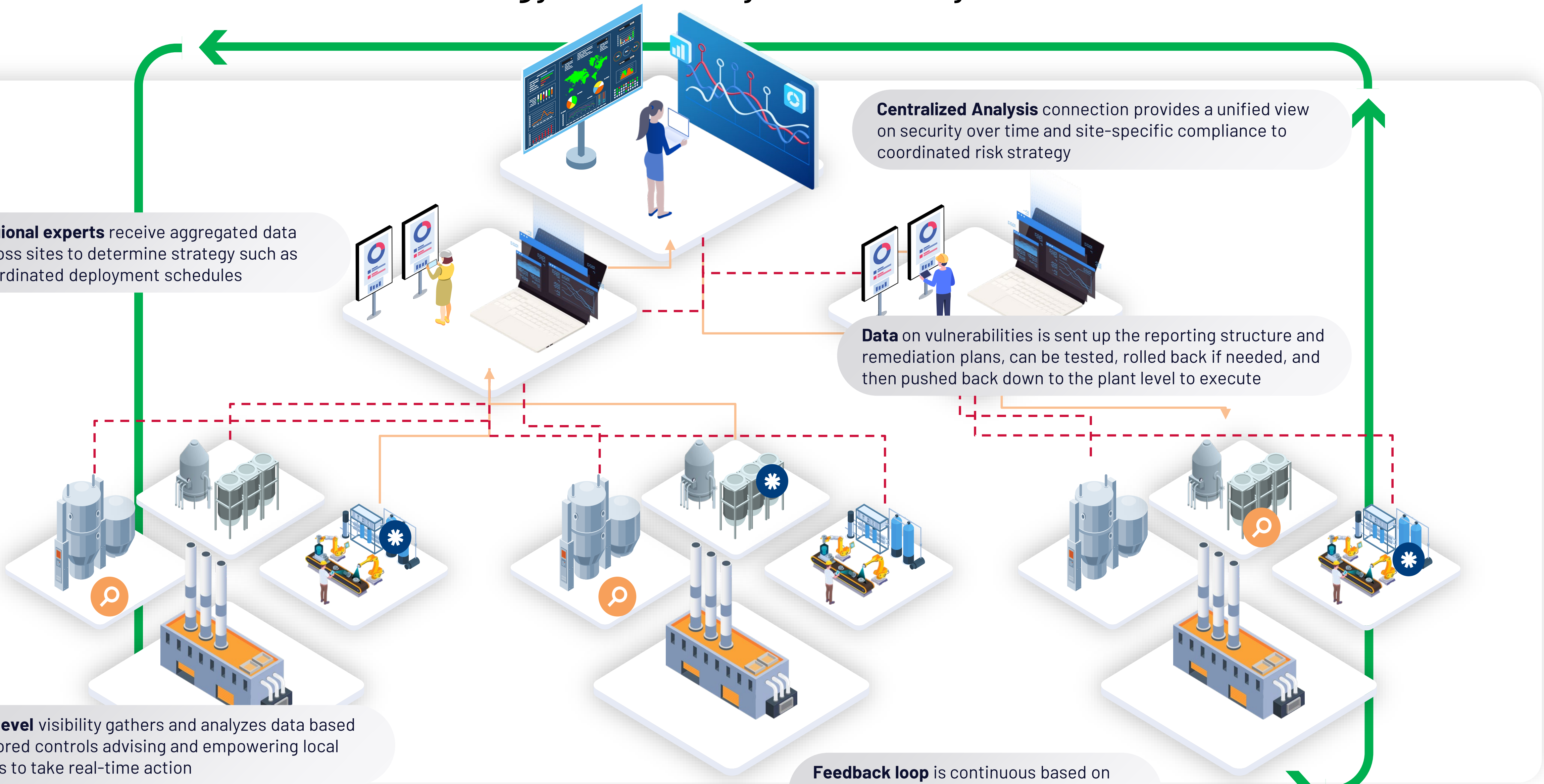
Weight	Factor	Description
4.2	PLC key switch allows writes	Number of critical vulnerabilities present on asset
3.4	On multiple networks	Asset is nearing end of life.
3.1	Highly connected	Links to other assets in the environment
3.0	Properly licensed	Number of Critical vulnerabilities with known exploits
2.8	Has current backup	Number of patches for installed software missing
2.4	Program recently updated	AntiVirus is running regularly on the asset
1.3	Joined to a domain	Antivirus Definitions Updates with Last 10 Days
1	Recent Domain controller connection	Asset has been backed up within the last 10 days
1	Agent version current	User passwords > defined amounts of time
1	System audit collection enabled	Assets with user accounts that haven't ben used > 180d

A central and unified strategy to security with ability for localized execution

ENTERPRISE

REGIONAL

PLANT



Centralized Analysis connection provides a unified view on security over time and site-specific compliance to coordinated risk strategy

Regional experts receive aggregated data across sites to determine strategy such as coordinated deployment schedules

Data on vulnerabilities is sent up the reporting structure and remediation plans, can be tested, rolled back if needed, and then pushed back down to the plant level to execute

Plant-level visibility gathers and analyzes data based on tailored controls advising and empowering local experts to take real-time action

Feedback loop is continuous based on remediation activities and as new assets and vulnerabilities are discovered

CONFIDENTIAL • Copyright ©2025 Rockwell Automation, Inc.

Global Food and Beverage Manufacturer Case Study

Before	After
High 90s Average Risk Score	**Low 60s** Average Risk Score
Reactive No remediation aligned to planned outage	**Proactive** Patches, updates, config changes automated for outage
EOL No scope or plan	**5 Year Budget** Proactive capital planning for equipment refresh

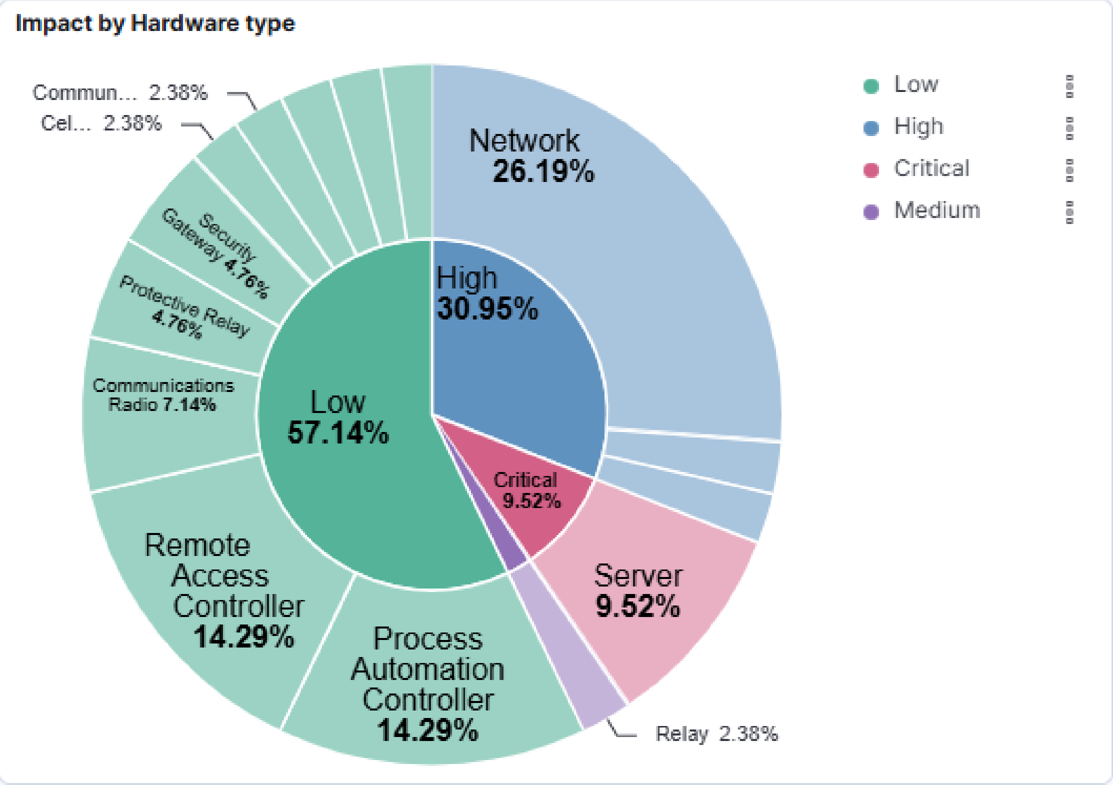
- ✗ Disjointed IT-centric tools; no OT view
- ✗ Reactive fixes, no outage-aligned plan
- ✗ 20,000+ total vulns

- ☑ Inventory 99% complete (20,000 assets)
- ☑ Clear view of missing patches and accepted risk levels
- ☑ Contextual risk-based scoring to guide/direct activities and spend

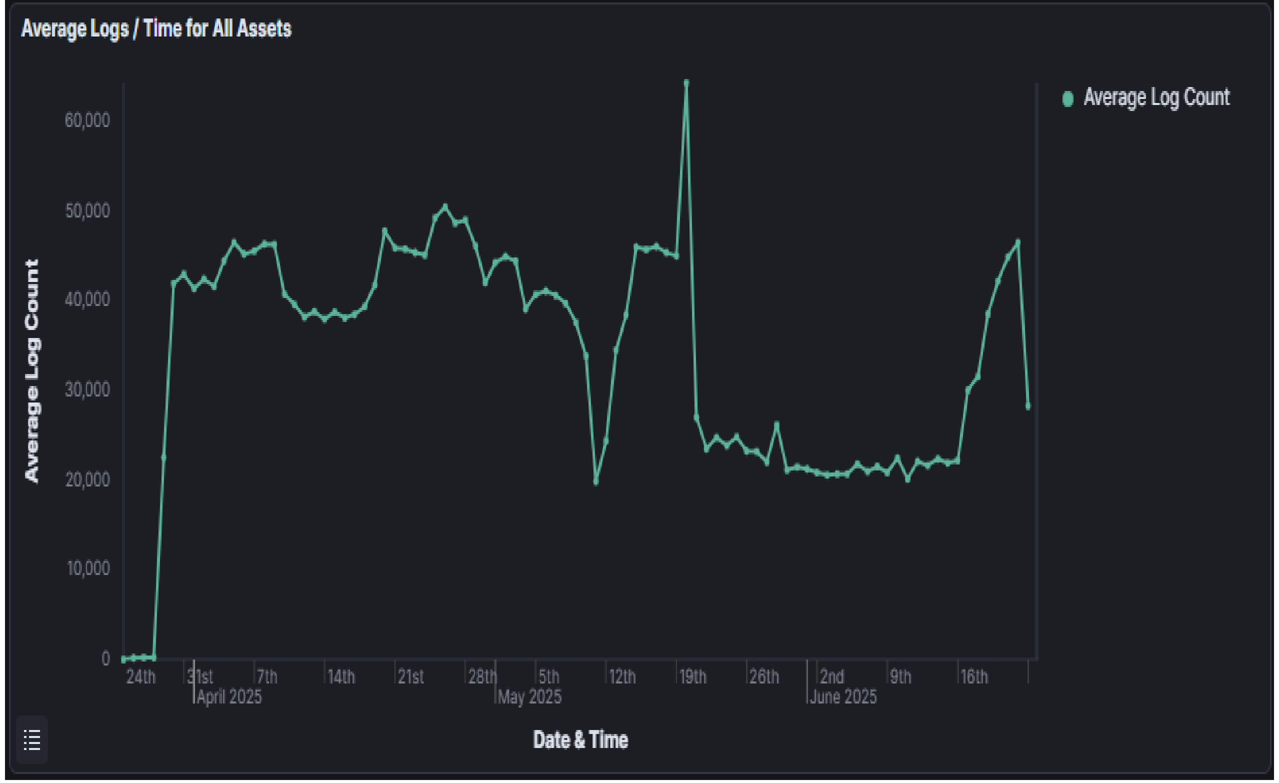
CONFIDENTIAL • Copyright ©2025 Rockwell Automation, Inc.

TSA/Regulatory Dashboards – Case Study

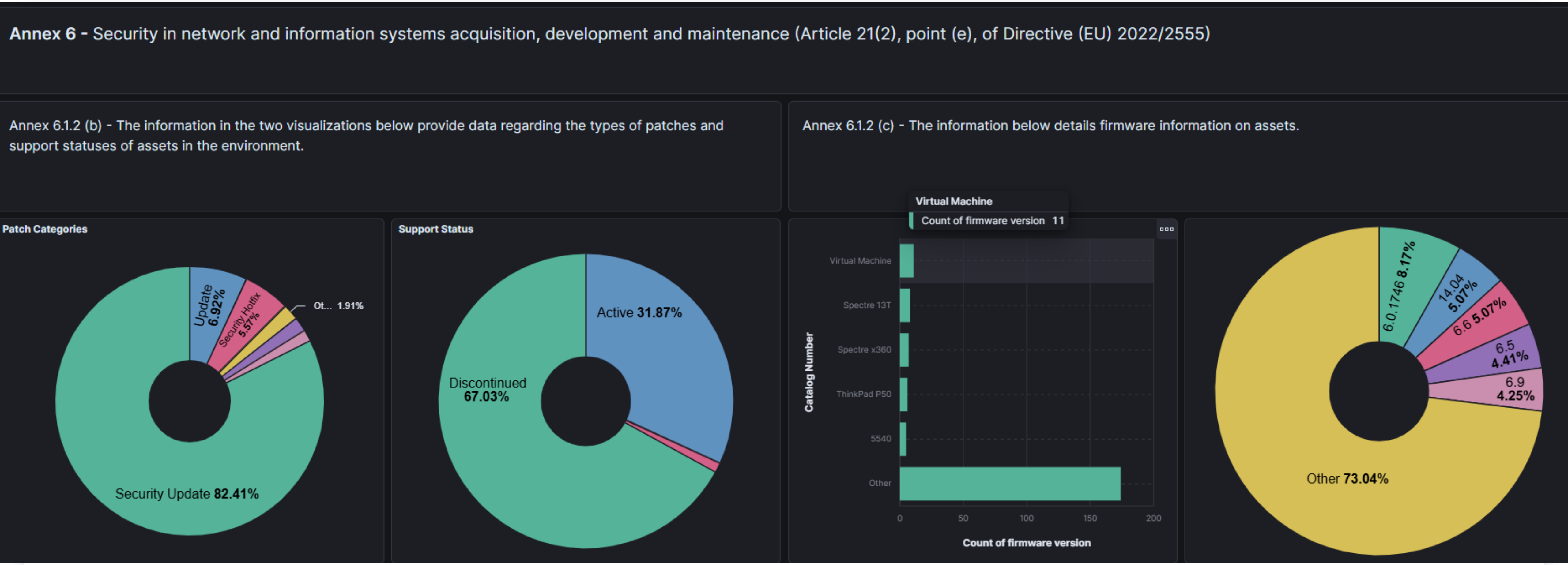
Annex 2.1.2 (b) - Below is a breakdown of impact by hardware type of assets, to use in determining risk appetite.



Annex 3.2.3 (k) - Log activity over time, including starting/stopping of log collection, is shown in the histogram below.



TSA/Regulatory Dashboards – Case Study



Annex 6 - Security in network and information systems acquisition, development and maintenance (Article 21(2), point (e), of Directive (EU) 2022/2555)

Annex 6.1.2 (b) - The information in the two visualizations below provide data regarding the types of patches and support statuses of assets in the environment.

Annex 6.1.2 (c) - The information below details firmware information on assets.

Download the Free Guide:

OT Cybersecurity- The essential guide to securing oil and gas operations

Scan the code to begin the download or to request a personalized consultation

CONFIDENTIAL • Copyright ©2025 Rockwell Automation, Inc.

Registration is Open

CONNECT
COLLABORATE
CREATE

Visit rok.auto/automationfair

NOV
17-20
2025
CHICAGO, IL
UNITED STATES

Rockwell Automation

VERVE

Thank you

Rick Kaun
Rick.Kaun@rockwellautomation.com

www.rockwellautomation.com