Mut zur Lücke

Risikobasiertes Schwachstellen- und Patchmanagement

Johannes Carl | Expert Manager PreSales UEM & Security

ivanti

Nutzen Sie Vulnerability-Scanner?

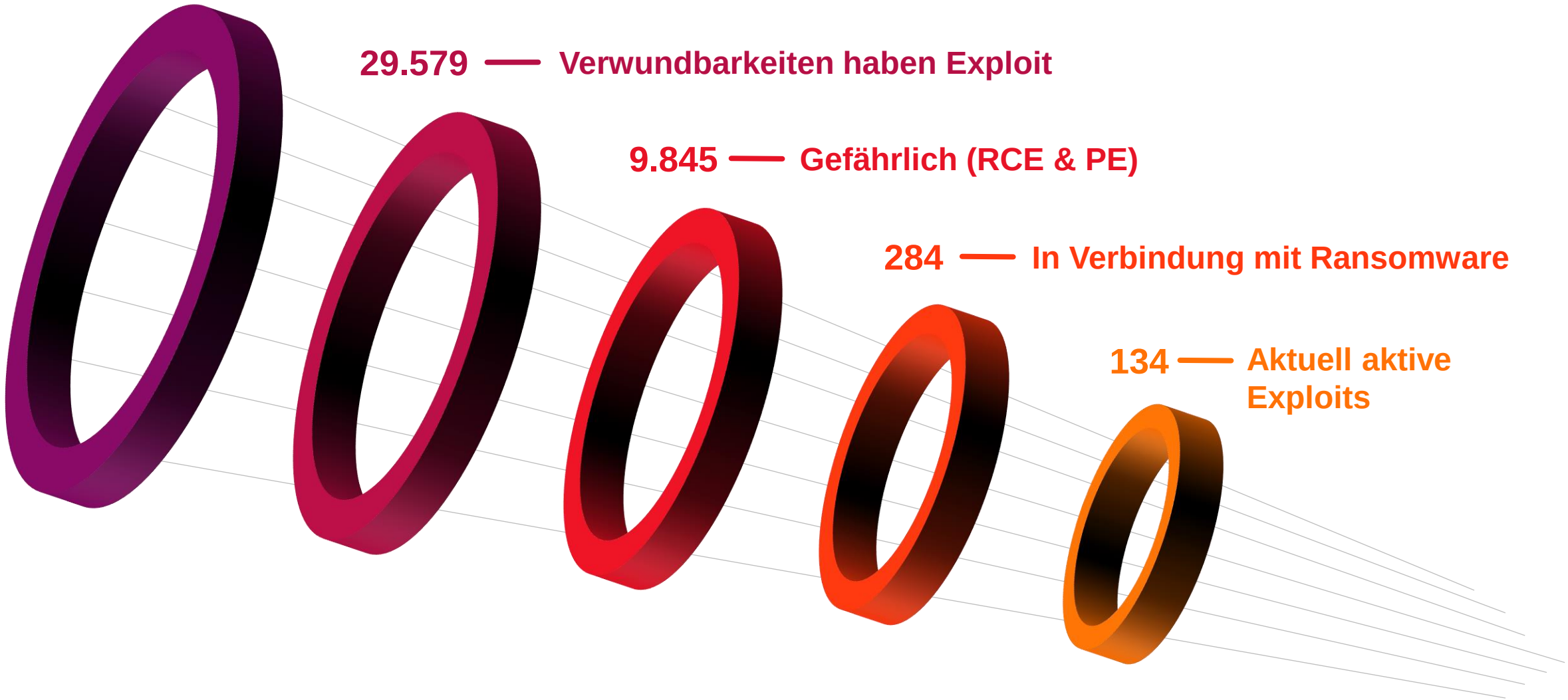
246.424 — Verwundbarkeiten in NVD

29.579 — Verwundbarkeiten haben Exploit

9.845 — Gefährlich (RCE & PE)

284 — In Verbindung mit Ransomware

134 — Aktuell aktive Exploits



Zahlen vom 06. September 2022

Quelle: Ivanti Neurons for Vulnerability Knowledge Base Q3 2022

Die bloße Anzahl an Verwundbarkeiten ist 2021 um 10% gestiegen und liegt damit erstmals über 20.000 im Jahr

In den letzten 5 Jahren hat sich die jährliche Anzahl an Verwundbarkeiten (CVEs) mehr als verdreifacht

Wie priorisieren Sie?

Schwierigkeiten bei der Prioriserung von Verwundbarkeiten

73,61%

…der von Ransomware genutzten Verwundbarkeiten sind von CVSS v3 nicht als “Kritisch” eingestuft.*

91%

… der von aktueller Ransomware genutzten Verwundbarkeiten wurden vor 2021 entdeckt.*

22 Tage

… ab der Veröffentlichung einer Verwundbarkeit vergehen im Durchschnitt bis zum Exploit.

*Quelle: *Cyber Security Works, Cyware, Ivanti, “2022 Ransomware Spotlight Report”*
***RAND Corproration*

Priorisierung durch Hersteller in der Realität

Microsoft hat 2021 23 Zero-Day Exploits geschlossen

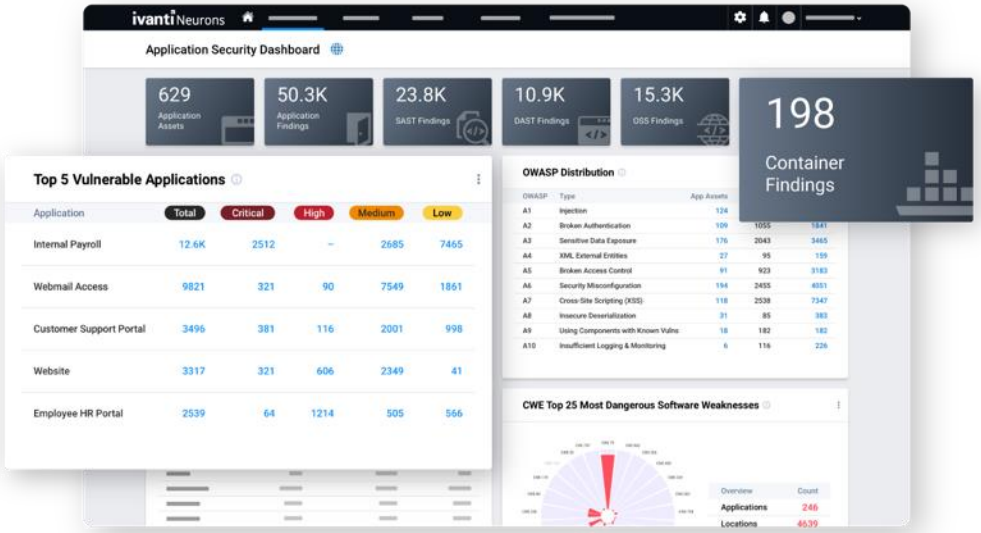
15 der 23 bekanntermaßen ausgenutzten Verwundbarkeiten hatten die Priorität “Wichtig”

Die CVSS Bewertung von 19 der 23 CVEs lag unter 8,0

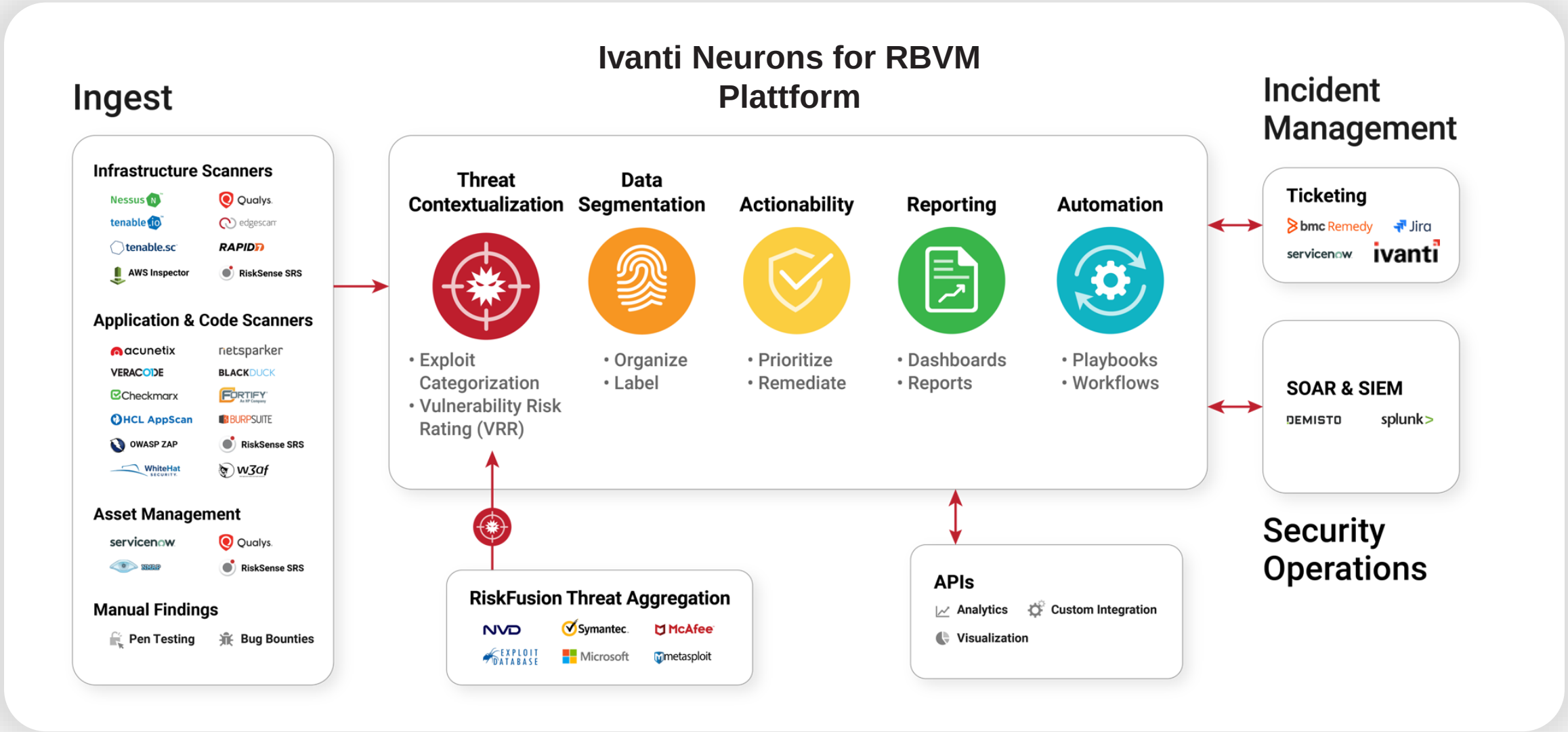
Kaum Aufmerksamkeit sofern sie nicht mit bedrohlichen Namen in den Schlagzeilen gelandet sind (PrintNightmare, HAFNIUM, PuzzleMaker, usw.)

ivanti Neurons
Risk-Based Vulnerability Management

ivanti Neurons
App Security Orchestration & Correlation



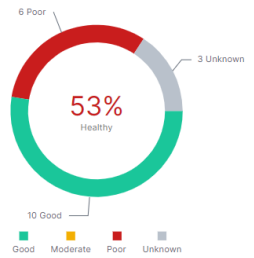
So funktioniert Risk Based Vulnerability Management



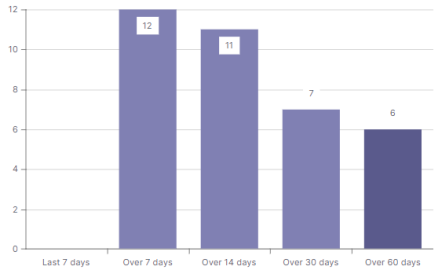
ivanti Neurons
For Patch Management

Endpoint vulnerability

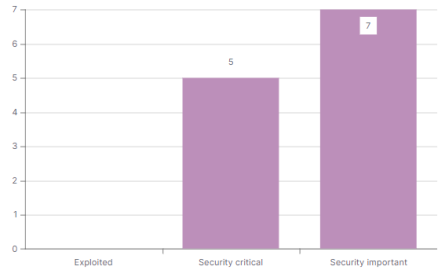
Device health
Device health is measured using the risk score.



Last scanned
Number of days since devices last scanned



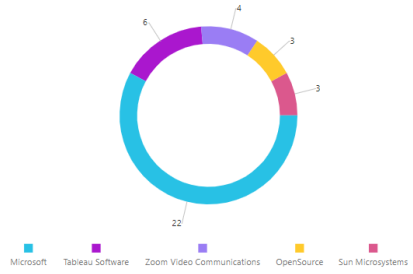
Devices by risk
Devices affected by severity



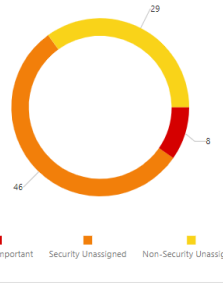
Patch Intelligence

All Patches | My Environment — Latest patches

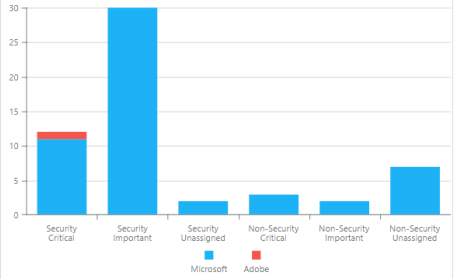
Top Vendors
Ranked by release frequency in past 14 days



Patch Types
Ranked by vendor severity in past 14 days



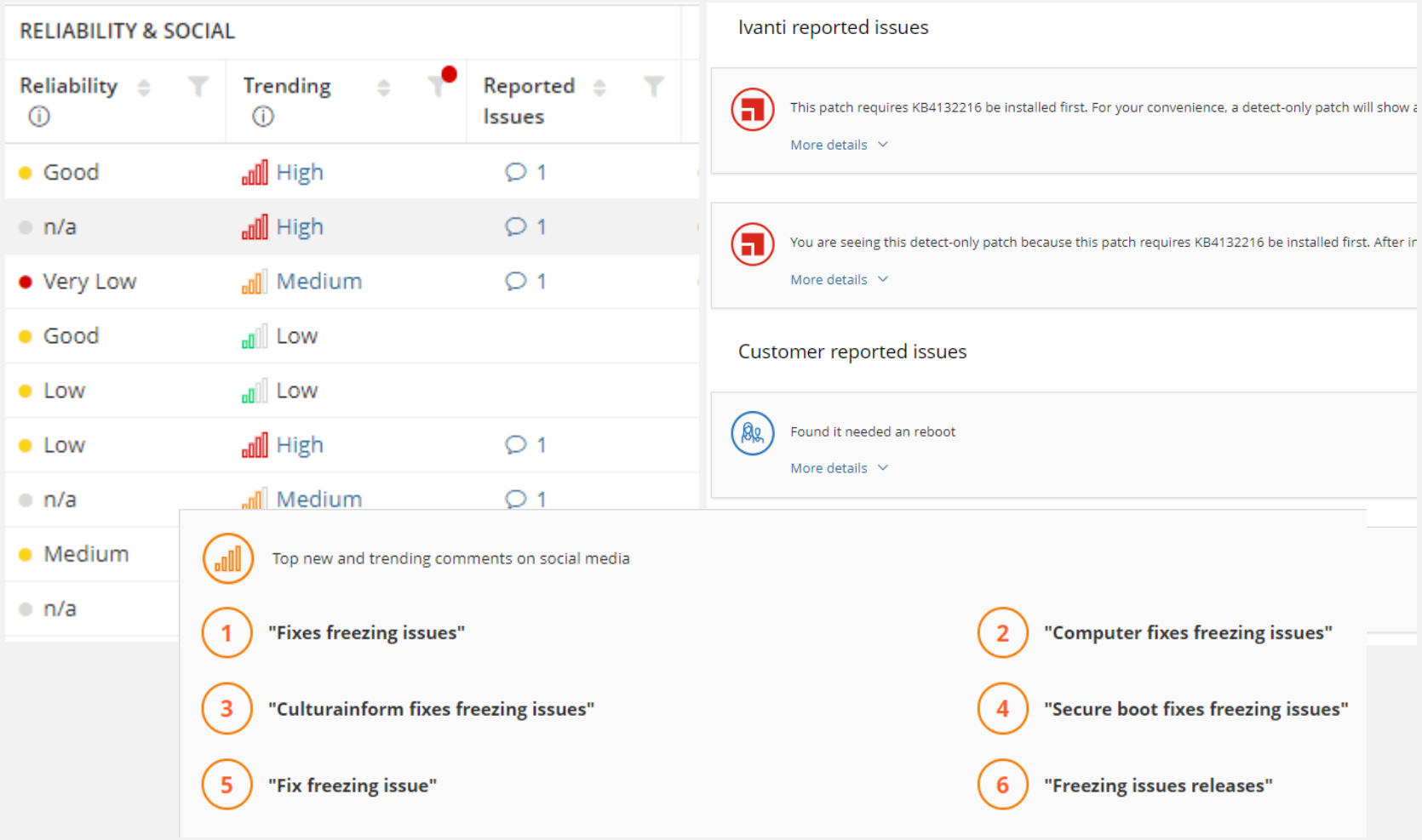
Patch Tuesday
51 patches released by severity



Patch Groups | Export CSV | Search...

SUMMARY					RELIABILITY & SOCIAL			THREAT & RISK		
Name	Platform	Unpatched Devices	Date	Vendor	Reliability	Trending	Reported Issues	RiskSense VRR Group	Cve Count	Vendor Severity
Security Cumulative Update for Windows 10 and Server 2019 V...	Windows	2	12 Apr 2022	Microsoft	Medium	Low		Critical	93	Security Critical
Security update for Secure Boot DBX: January 12, 2021 (KB453...	Windows	1	12 Jan 2021	Microsoft	High	High	1	Medium	1	Security Important
KB5010794: Out-of-band update for Windows 8.1 and Window...	Windows	1	17 Jan 2022	Microsoft	Good	Medium	1	No Data	0	Security Unassigned
January 11, 2022-KB5009595 (Security-only update)	Windows	1	11 Jan 2022	Microsoft	Medium	High	1	Critical	49	Security Critical
Security Cumulative Update for Windows 10 Version 20H2, 21...	Windows	1	12 Apr 2022	Microsoft	Low	High	1	Critical	97	Security Critical
KB4589212: Intel microcode updates for Windows 10, version ...	Windows	1	25 Jan 2021	Microsoft	Medium	Medium	1	Critical	4	Non-Security Unassigned

Zuverlässigkeit von Patches und “Stimmungsbild”



Ivanti Security Controls

Stand Alone

- Einfache Installation und Bedienung
- Umfangreiche Steuerung
- Agentless/Agent-based
- Patchen von externen Geräten ohne VPN
- Perfekt für kleine und mittelgroße Umgebungen

Ivanti Patch Manager / Ivanti Patch for EPM

Integration in EPM

Stand Alone

- Sehr umfangreich und granular zu steuern
- Keine neue Infrastruktur für EPM-Kunden
- Peer Download
- Rollout Projekte
- Perfekt für mittlere bis sehr große Umgebungen

Ivanti Patch for SCCM/MEM

Integration in SCCM

- Minimaler Installationsaufwand
- Keine zusätzliche Infrastruktur
- Kein Schulungsaufwand
- Perfekt für SCCM/MEM-Kunden

Ivanti Neurons for Patch Management

Cloud

- Erfordert keine zusätzliche Infrastruktur
- Komplettes Patchmanagement aus der Cloud
- Integration in Ivanti Neurons Plattform

Ivanti Neurons Patch for MEM

Integration in Intune

- Erfordert keine zusätzliche Infrastruktur
- Minimaler Installationsaufwand
- Integration von Patches in Microsoft Intune

Vielen Dank

ivanti

Welche IT-Herausforderungen beschäftigen Sie?