Threat Exposure Management Snapshot

Report for <org>
Prepared for <point of contact>
Delivered <date>

Table of Contents

Why Customers Choose KeyCaliber:

The Business Context Difference

KeyCaliber’s Threat Exposure Management platform automatically gives you a clear and current snapshot of your cybersecurity and risk posture:

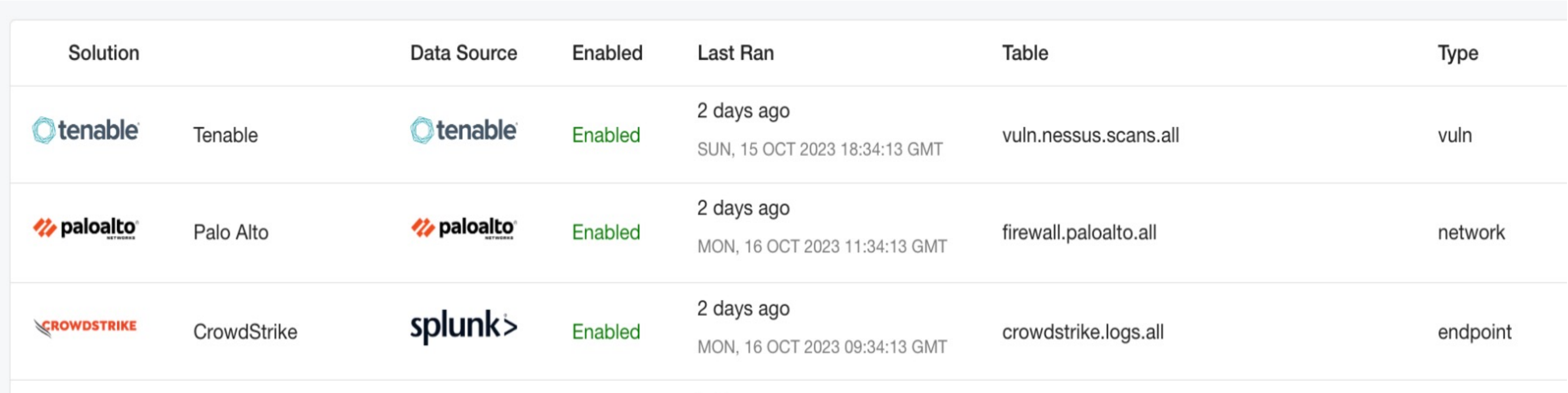
- Asset discovery and inventory
- Security tool coverage gaps

With the business context you need to prioritize actions and optimize resources:

- Asset impact scores
- Risk scores
- Connection maps

Your Data Sources

KeyCaliber requires 3 data sources to provide meaningful results: vulnerability scanner data, traffic data, and endpoint detection & response (EDR) data. These data sources were used for your assessment:



Solution		Data Source	Enabled	Last Ran	Table	Type
tenable	Tenable	tenable	Enabled	2 days ago SUN, 15 OCT 2023 18:34:13 GMT	vuln.nessus.scans.all	vuln
paloalto	Palo Alto	paloalto	Enabled	2 days ago MON, 16 OCT 2023 11:34:13 GMT	firewall.paloalto.all	network
CROWDSTRIKE	CrowdStrike	splunk>	Enabled	2 days ago MON, 16 OCT 2023 09:34:13 GMT	crowdstrike.logs.all	endpoint

Recommendations

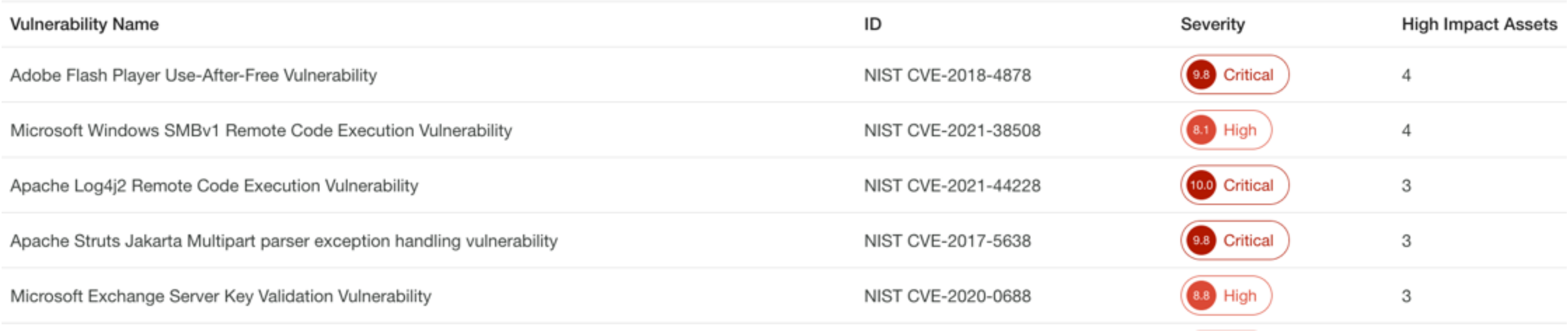
KeyCaliber provides the powerful and unique capability to automatically compute an Impact Score for every cyber asset in your environment to distinguish your high-impact assets (also known as mission-critical assets or “Crown Jewels”).

Impact Scores are computed using available data sources and KeyCaliber’s patent-pending machine learning that utilizes over 1,000 features to conduct asset behavior analytics, examining how each asset interacts with other systems and users, and what is running on the asset.

Recommendations center around addressing your high-impact assets first so that you can prioritize and focus your limited resources efficiently and effectively.

High Priority Vulnerabilities to Patch:
Known Exploited Vulnerabilities (KEVs) & Internet-Facing

These are the vulnerabilities in CISA’s Known Exploited Vulnerabilities Catalog that exist in your environment on Internet-facing, high-impact assets. These are the highest priority to patch because cyber attackers can utilize these vulnerabilities to directly reach your high-impact assets.

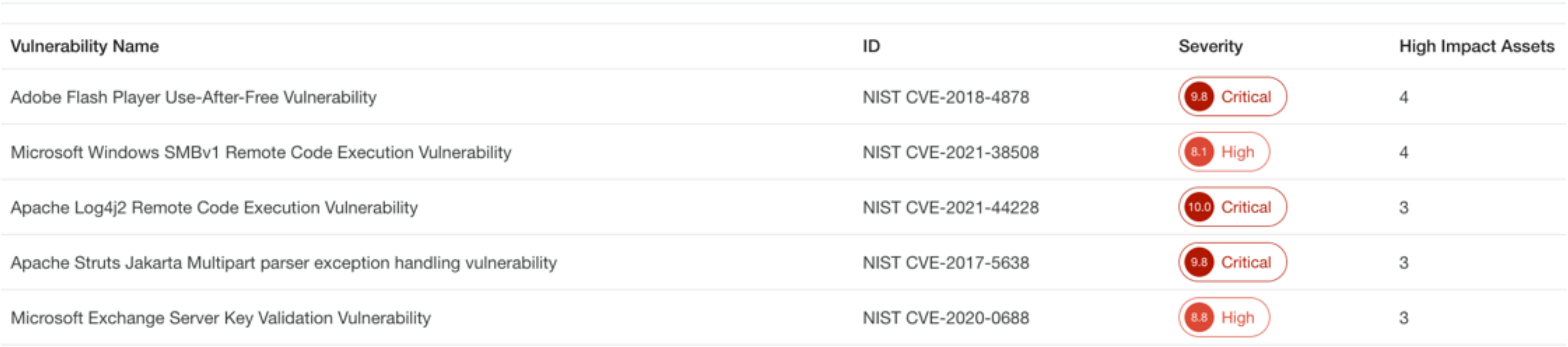


Vulnerability Name	ID	Severity	High Impact Assets
Adobe Flash Player Use-After-Free Vulnerability	NIST CVE-2018-4878	9.8 Critical	4
Microsoft Windows SMBv1 Remote Code Execution Vulnerability	NIST CVE-2021-38508	8.1 High	4
Apache Log4j2 Remote Code Execution Vulnerability	NIST CVE-2021-44228	10.0 Critical	3
Apache Struts Jakarta Multipart parser exception handling vulnerability	NIST CVE-2017-5638	9.8 Critical	3
Microsoft Exchange Server Key Validation Vulnerability	NIST CVE-2020-0688	8.8 High	3

The full list of these vulnerabilities is available as a spreadsheet in Appendix A.

High Priority Vulnerabilities to Patch:
Known Exploited Vulnerabilities (KEVs)

These are vulnerabilities in CISA's Known Exploited Vulnerabilities Catalog that exist in your environment on high-impact assets that are not Internet-facing. These are the second highest priority to patch.

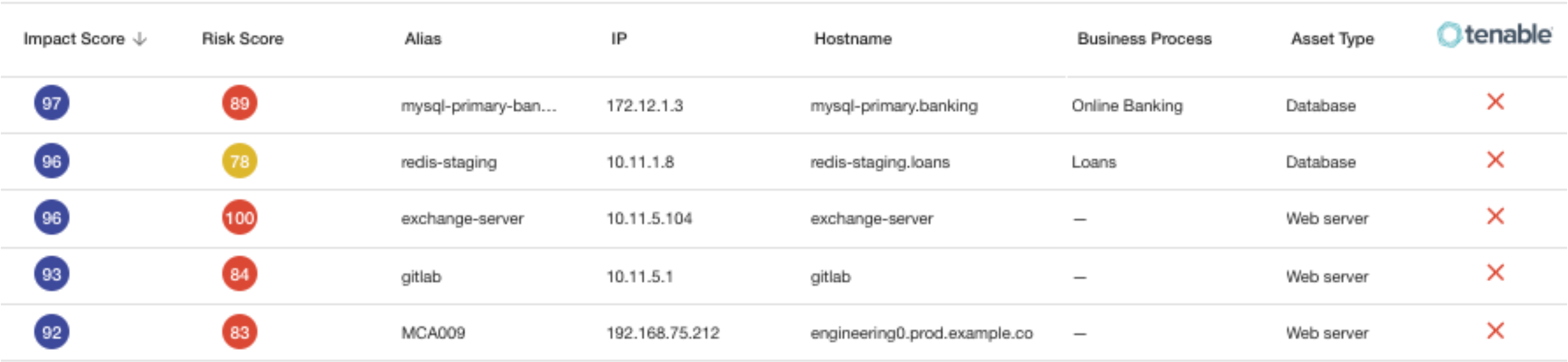


Vulnerability Name	ID	Severity	High Impact Assets
Adobe Flash Player Use-After-Free Vulnerability	NIST CVE-2018-4878	9.8 Critical	4
Microsoft Windows SMBv1 Remote Code Execution Vulnerability	NIST CVE-2021-38508	8.1 High	4
Apache Log4j2 Remote Code Execution Vulnerability	NIST CVE-2021-44228	10.0 Critical	3
Apache Struts Jakarta Multipart parser exception handling vulnerability	NIST CVE-2017-5638	9.8 Critical	3
Microsoft Exchange Server Key Validation Vulnerability	NIST CVE-2020-0688	8.8 High	3

The full list of these vulnerabilities is available as a spreadsheet in Appendix B.

High Priority Coverage Gaps to Remediate:
Missing Vulnerability Scanner Coverage

These are your top high-impact assets that are missing vulnerability scanner coverage. These are the highest priority for coverage remediation.

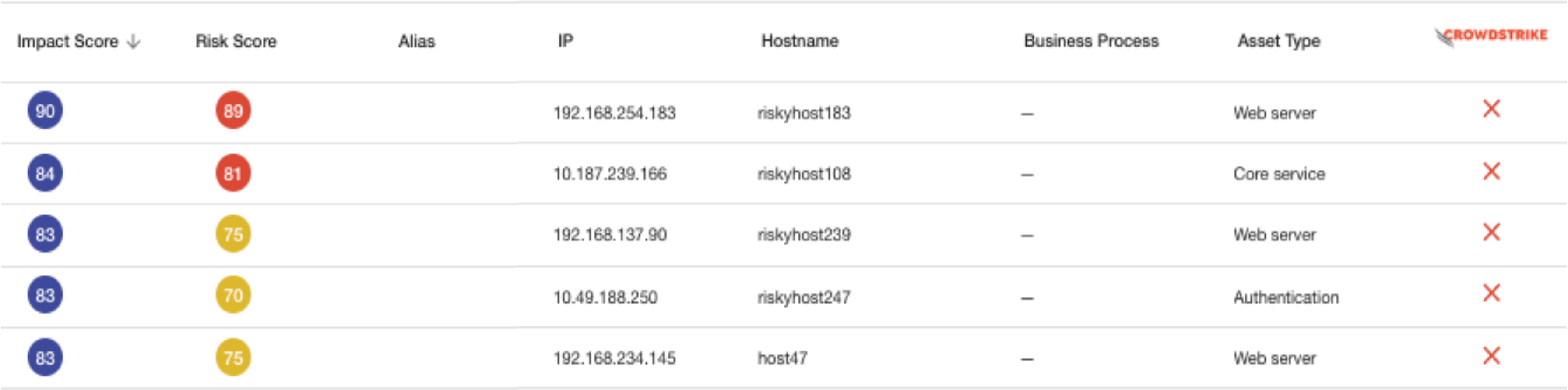


Impact Score ↓	Risk Score	Alias	IP	Hostname	Business Process	Asset Type	tenable
97	89	mysql-primary-ban...	172.12.1.3	mysql-primary.banking	Online Banking	Database	✗
96	78	redis-staging	10.11.1.8	redis-staging.loans	Loans	Database	✗
96	100	exchange-server	10.11.5.104	exchange-server	–	Web server	✗
93	84	gitlab	10.11.5.1	gitlab	–	Web server	✗
92	83	MCA009	192.168.75.212	engineering0.prod.example.co	–	Web server	✗

The full list of these assets is available as a spreadsheet in Appendix C.

High Priority Coverage Gaps to Remediate:
Missing EDR Coverage

These are your top high-impact assets that are missing endpoint detection & response (EDR) coverage. These are the second highest priority for coverage remediation.



Impact Score ↓	Risk Score	Alias	IP	Hostname	Business Process	Asset Type	CROWDSTRIKE
90	89		192.168.254.183	riskyhost183	–	Web server	✗
84	81		10.187.239.166	riskyhost108	–	Core service	✗
83	75		192.168.137.90	riskyhost239	–	Web server	✗
83	70		10.49.188.250	riskyhost247	–	Authentication	✗
83	75		192.168.234.145	host47	–	Web server	✗

The full list of these assets is available as a spreadsheet in Appendix D.

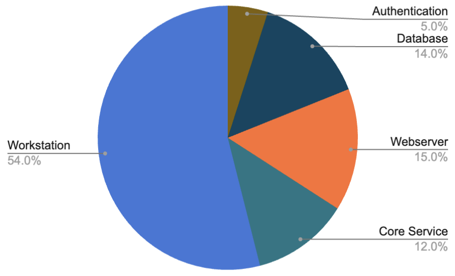
Executive Summary

Every chart is presented for both your full environment and your high-impact assets only.

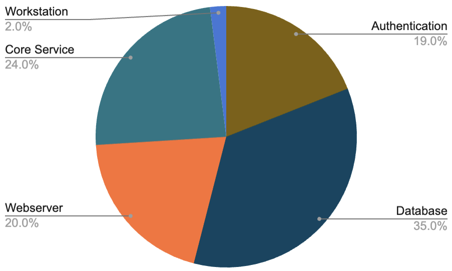
Your Cyber Asset Inventory

This is a summary of the cyber assets discovered in your environment. A cyber assets is defined as a network-addressable instance of compute.

All Assets		High-Impact Assets
17,358	Total Number of Assets	314
86	Total Number of Subnets	32



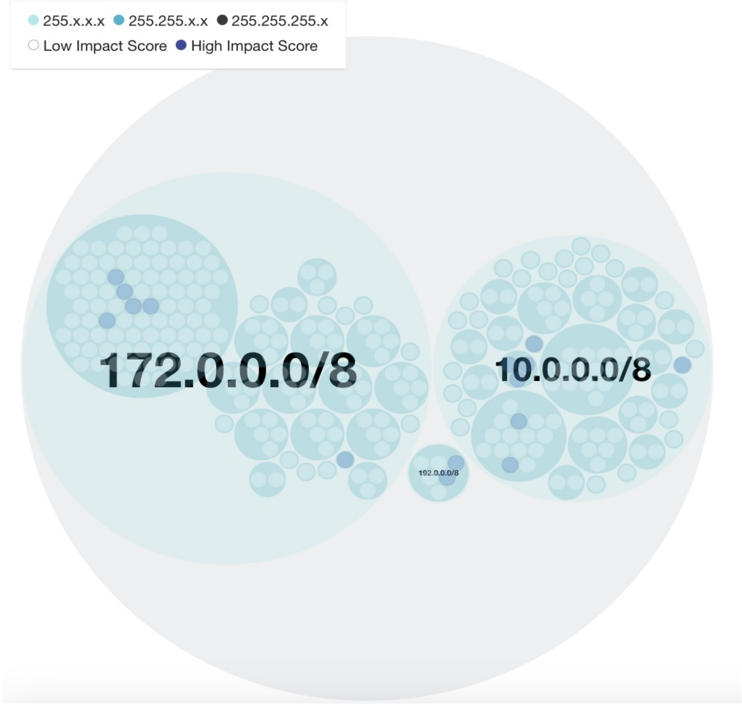
Asset Types



The full inventory, sorted by impact score, is available as a spreadsheet in Appendix E.

Your Cyber Asset Map

This map shows the subnets discovered in your environment. The subnets in blue contain one or more high-impact assets. This visualization can be used to identify areas to apply your zero trust initiatives.

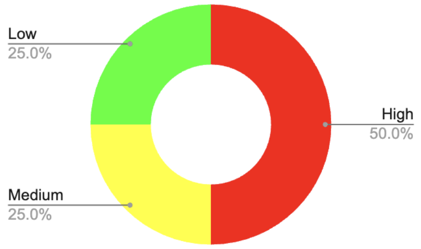


The full list of subnets with high-impact asset is available as a spreadsheet in [Appendix F](#).

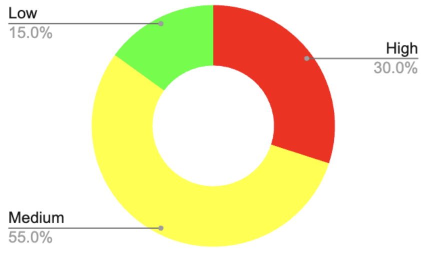
Your Risk Posture

For every cyber asset in your environment, KeyCaliber computes a Risk Score (0 to 100) which incorporates the Impact Score, vulnerabilities, vulnerability exploitability/severity, open ports, distance from the Internet, and a variety of additional factors. High: > 80, Medium: 40-80, Low: < 40

All Assets		High-Impact Assets
87	Average Risk Score	68
592	Number of High-Risk Assets	132



Risk Breakdown

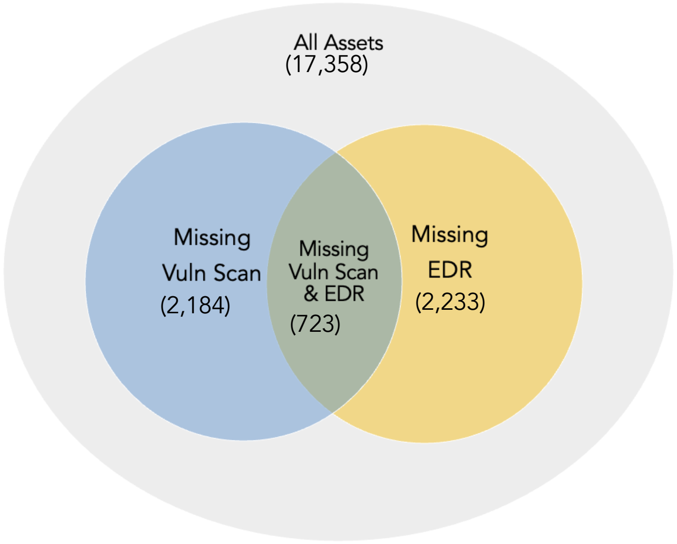


The full list of high-risk assets is available as a spreadsheet in Appendix G.

Your Security Posture

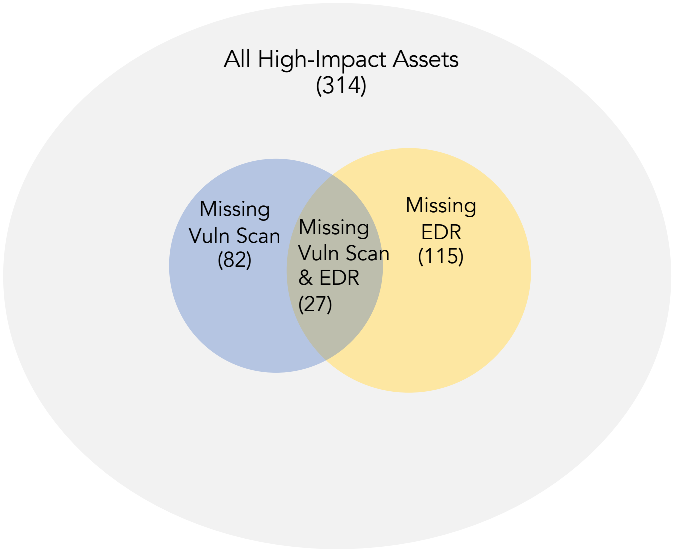
For every cyber asset in your environment, KeyCaliber determines whether the asset is covered by the security tools that were ingested as Data Sources. This is used to show coverage gaps that need to be addressed.

All Assets



Vulnerability Scanner & EDR Coverage Gaps

High-Impact Assets



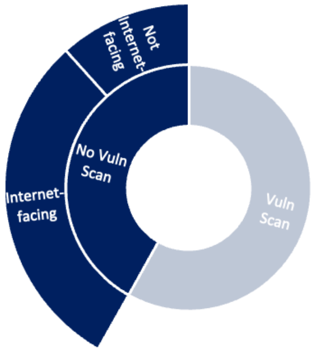
The full list of assets without coverage is available as a spreadsheet in Appendix H.

Your Security Posture

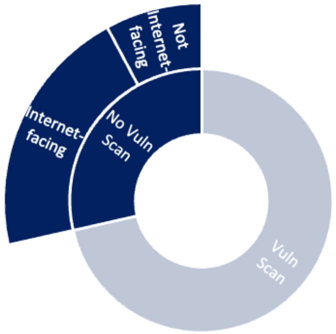
For every cyber asset in your environment, KeyCaliber determines whether the asset is covered by the security tools that were ingested as Data Sources. This is used to show coverage gaps that need to be addressed.

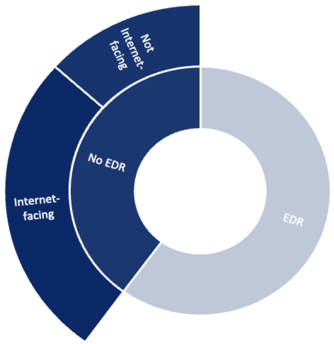
All Assets

High-Impact Assets

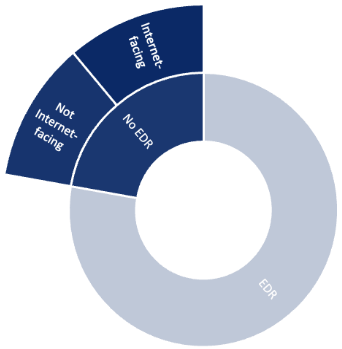


Vulnerability Scanner Coverage





EDR Coverage



The full list of Internet-facing assets without EDR/Vulnerability Scanner coverage is available as a spreadsheet in Appendix I.

Thank You!

To learn more about our continuous assessment/remediation technology or our cybersecurity/risk services, please contact us at hello@keycaliber.com!

KEYCALIBER

www.keycaliber.com