External Attack Surface Summary Report

GENERATED FOR Acme Corporation

Powered By

Qualys.

01

Qualys External Attack Surface Discovery

EASM Discovery Process

02

View Your Attack Surface

EASM Summary
Top Organizations with Internet-facing assets
Internet-Facing Cloud and Hosting Provider Instances

03

Know Your Risk On Internet facing Assets

Internet-Facing Assets with Risk
Cloud Instances with Risk
Top Risky Domains and Subdomains
Risky Open Ports On Your Internet-Facing Assets
Database Open Ports on your internet-facing assets
Top Open Ports
Top Vulnerabilities On Internet-facing Assets

04

Prioritize Your Risk

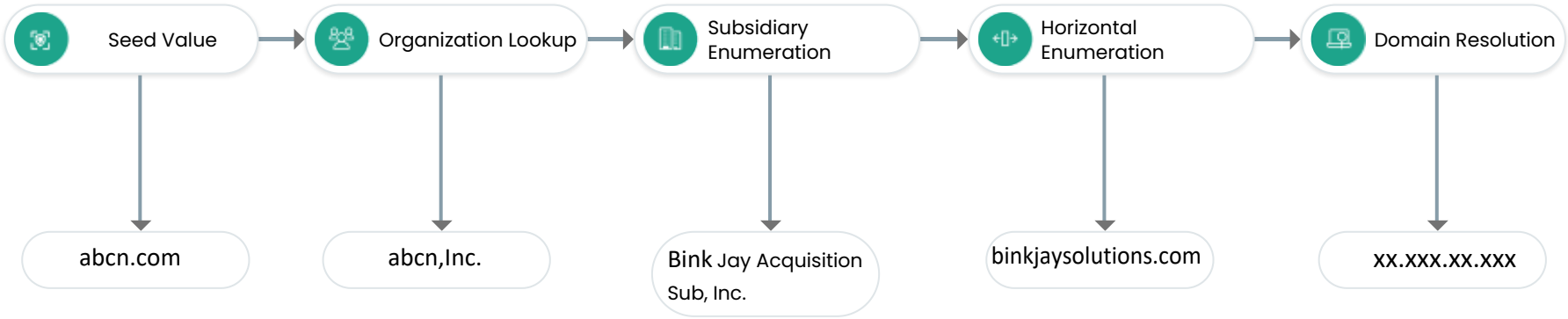
Prioritize Your Risk
Use The Power Of Qualys VMDR And WAS
Continuously discover and monitor your entire attack surface

Qualys **EASM Discovery**

External Attack Surface Discovery Process

The EASM configuration considers seed values like Organization, Domain, Netblock, or Cert subject and starts discovering your Internet-facing assets. **It finds your subsidiaries, domains, and sub domains through various enumeration processes and correlates WHOIS and DNS records to attribute assets to your organization in an accurate manner.** Also, it periodically monitors changes, such as new open ports and services, certificates due for expiration, or vulnerabilities.

An example of how your assets are discovered through EASM enumeration process:



External Attack Surface Summary

2.78K
Total Internet-facing Assets

2.78K
Assets missing in VMDR

8
Organization/Subsidiaries

66
Domains

1.55K
Subdomains

2
Databases

1.09K
Web Servers

Top Organizations with Internet-facing assets

2.8k Total Internet-Facing Assets

Showing top **8** Of 8 total organizations

Hooli, Inc.	2.78K Assets
Assets Missing in VMDR	2.78K
Domain	66
Subdomains	1.55K

Bink Jay Acquisition Sub, Inc.	94 Assets
Assets Missing in VMDR	94
Domain	6
Subdomains	52

SSQ Labs	22 Assets
Assets Missing in VMDR	22
Domain	1
Subdomains	40

Globex Corp.	17 Assets
Assets Missing in VMDR	17
Domain	1
Subdomains	5

Second Front Systems	11 Assets
Assets Missing in VMDR	11
Domain	1
Subdomains	3

Bink Hexa	10 Assets
Assets Missing in VMDR	10
Domain	1
Subdomains	7

Adyua, Inc	1 Assets
Assets Missing in VMDR	1
Domain	1
Subdomains	1

Yoo Insight, Inc.	1 Assets
Assets Missing in VMDR	1
Domain	36
Subdomains	9

Internet-Facing Cloud Provider Instances

2.8k Total Internet-Facing Assets

aws			
35	**6**	**3**	**27**
AWS Hosted Instances	**GCP** Hosted Instances	**AZURE** Hosted Instances	**ORACLE** Hosted Instances

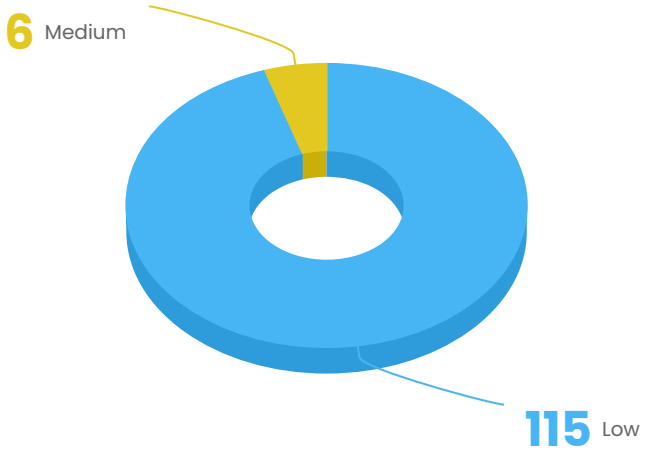
Internet-Facing Hosting Provider Instances

CDN Hosted Instances	**747** Assets
Akamai Technologies, Inc.	**343**
Akamai International B.V.	**277**
Amazon.com, Inc.	**35**

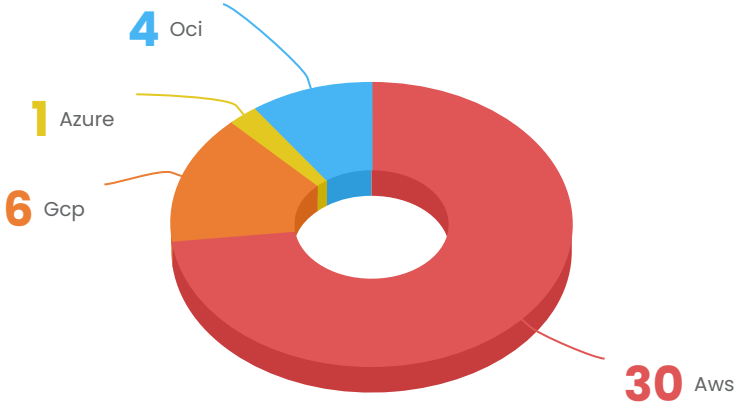
Other Hosted Instances	**1.93K** Assets
Oracle Corporation	**502**
QUALYS, Inc.	**502**
Microsoft Corporation	**7**

2.8k Total Internet-Facing Assets

Internet-Facing Assets with Risk



Cloud Instances with Risk



Cloud & Hosting provider Instances missing in your VM program

71/71

Total Internet-Facing **Cloud Provider** Instances missing in VMDR

747/747

Total Internet-Facing **CDN** hosted Instances missing in VMDR

1.93K/1.93K

Total Internet-Facing **Other** hosted Instances missing in VMDR

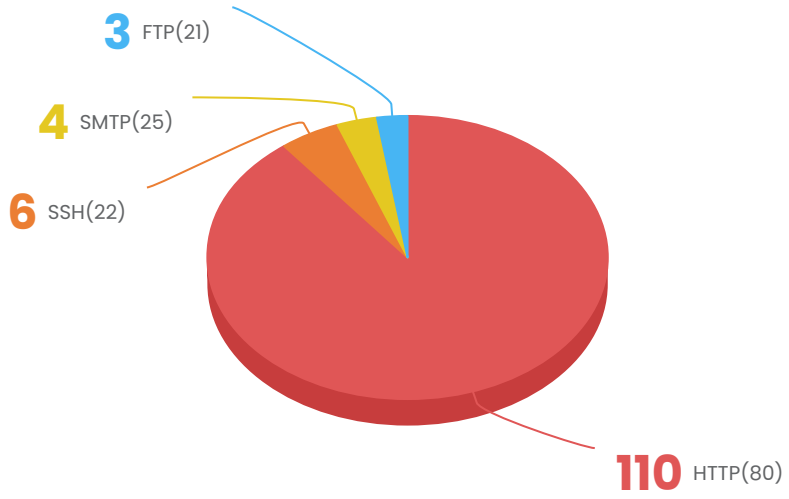
Top Risky **Domains**

ASSET DOMAIN	ORGANIZATION NAME	ASSET COUNT
hooli.io	hooli, Inc.	4
trustworthyinternet.com	Hooli, Inc	4
trustworthyinternet.org	Hooli, Inc	4
trustworthyinternetmovement.com	Hooli, Inc	4
trustworthyinternetmovement.org	Hooli, Inc	4
cio-ciso-interchange.org	Hooli, Inc.	3
cio-cisointerchange.org	Hooli, Inc.	3
ciointerchange.org	Hooli, Inc.	3
csointerchange.com	Hooli, Inc.	3
csointerchange.org	Hooli, Inc.	3

Top Risky **Subdomains**

ASSET SUBDOMAIN	ORGANIZATION NAME	ASSET COUNT
event.qualys.com	Hooli, Inc.	5
go.binkhexa.ai	Bink Hexa	5
go.secondfront.com	Second Front Systems	5
info.binkhexa. ai	Bink Hexa	5
info.binkjaysolutions.com	Bink Jay Acquisition Sub, Inc.	5
lps.hooli.com	Hooli, Inc.	5
app.hooli.io	Hooli, Inc.	4
assets.hooli.com	Hooli, Inc	4
autodiscover.binkjaysolutions.com	Bink Jay Acquisition Sub, Inc.	4
dev.cio-ciso-interchange.org	Hooli, Inc.	4

Risky Open Ports On Your Internet-Facing Assets



DNS (53)
DNS stands for Domain Name System. It is both a TCP and UDP port used for transfers and queries respectively. One common exploit on the DNS ports is the Distributed Denial of Service (DDoS) attack.

Telnet (23)
The Telnet protocol is a TCP protocol that enables a user to connect to remote computers over the internet. The Telnet port has long been replaced by SSH, but it is still used by some websites today. It is outdated, insecure, and vulnerable to malware. Telnet is vulnerable to spoofing, credential sniffing, and credential brute-forcing.

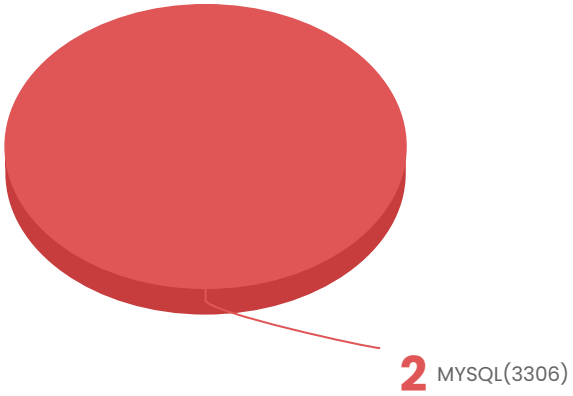
FTP (20, 21)
FTP stands for File Transfer Protocol. Port 20 and 21 are solely TCP ports used to allow users to send and to receive files from a server to their personal computers. The FTP port is insecure and outdated and can be exploited using: 1. Anonymous authentication. You can log into the FTP port with both username and password set to "anonymous".2. Cross-Site Scripting.3. Brute-forcing passwords.4. Directory traversal attacks.

SSH (22)
SSH stands for Secure Shell. It is a TCP port used to ensure secure remote access to servers. You can exploit the SSH port by brute-forcing SSH credentials or using a private key to gain access to the target system.

TFTP (69)
TFTP stands for Trivial File Transfer Protocol. It's a UDP port used to send and receive files between a user and a server over a network. TFTP is a simplified version of the file transfer protocol. Because it is a UDP port, it does not require authentication, which makes it faster yet less secure.

RDP (3389)
Remote Desktop Protocol (RDP) is a Microsoft protocol which enables administrators to access desktop computers. RDP is now the single most common attack vector used by cyber-criminals – particularly ransomware gangs.

Database Open Ports on your internet-facing assets



Top **Open Ports**

PORT NUMBER	INTERNET FACING ASSET COUNT
TCP(443)	1078
UDP(123)	779
TCP(80)	110
TCP(8443)	33
UDP(161)	30
TCP(123)	18
TCP(2083)	12
TCP(2087)	11
TCP(10443)	10
TCP(2086)	9

Top Vulnerabilities On Internet-facing Assets

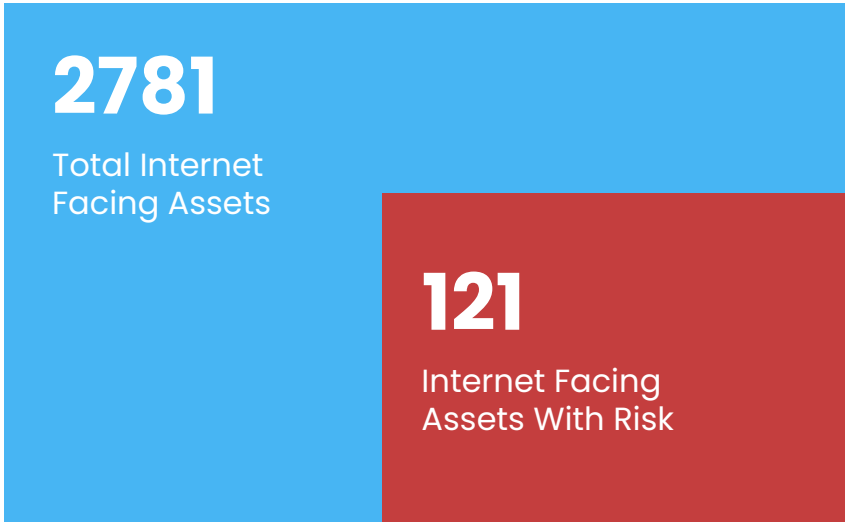
CVE ID	QVS	TYPE	ASSET COUNT
CVE-2019-6110	95	Potential	6
CVE-2018-20685	95	Potential	6
CVE-2019-6111	95	Potential	6
CVE-2019-6109	95	Potential	6
CVE-2020-15778	42	Potential	6
CVE-2018-15473	40	Potential	6
CVE-2017-15906	40	Potential	6
CVE-2016-20012	37	Potential	6
CVE-2021-41617	35	Potential	6
CVE-2018-15919	30	Potential	6

*These vulnerabilities were detected by third-party integration, without active VM/VMDR scan

Rapidly **Prioritize Your Risk**

Once Qualys EASM discovers and categorizes the External facing Assets, it detects risky open ports, Potential Vulnerabilities, Databases exposed to the Internet and more.

Examples of Risk Summary on External assets.



13/121 With Vulnerabilities

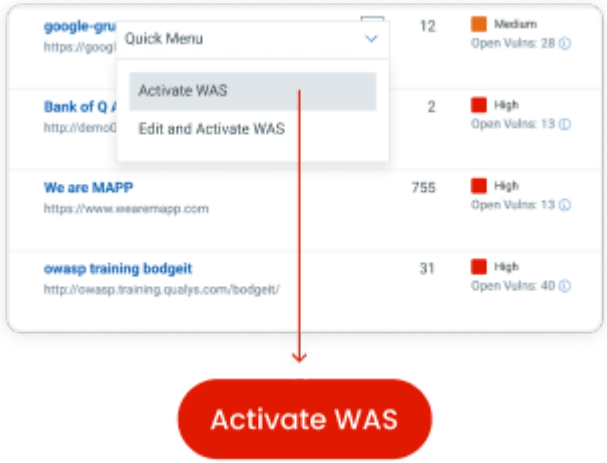
2/121 Open Database Ports

118/121 Open Risky Ports

Use The Power of **Qualys VMDR and WAS to** Secure Your Internet-Facing Assets

Activate Qualys VMDR

The built-in workflow to activate VMDR and/or Web Application Scanning allows you to quickly bring your full attack surface under management through network scans or the Qualys Cloud Agent.



Activate WAS

Qualys Web Application Scanning (WAS) gives organizations the ease of use, centralized management, and integration capabilities to keep attackers at bay and their web applications secure.

Continuously **discover and monitor** your entire attack surface with CSAM

Organizations can continuously gather comprehensive asset inventory data, apply business criticality and risk context, detect security gaps like unauthorized or end-of-life software, and respond with appropriate actions to mitigate risk.

- Full visibility of assets and software in hybrid environments.
- Improve threat prioritization with asset criticality ratings.
- Minimize tech debt with CISA-compliant real-time EOL/EOS software tracking.
- Minimize tech debt with CISA-compliant real-time EOL/EOS software tracking.