

Qualys Ransomware Risk Assessment Playbook

January 2024

Table of Content

Introduction to Qualys Ransomware Risk Assessment Solution

What I Get with Ransomware Solution (RAS) Enabled?

What will I see in my subscription?

- About the Ransomware Prevention Dashboard
 - Advantages of using this dashboard
 - How do I access this dashboard?
 - How do I view this dashboard?
- Let's Get Started
 - <u> Step 1 Build your Inventory</u>
 - Step 2 Detect at-risk Assets and Applications
 - Step 3 Prioritize Vulnerabilities
 - <u>Step 4 Deploy Patches</u>
 - Assess Misconfigurations



Introduction to Qualys Risk Assessment Solution

To gain a foothold in an environment, attackers often exploit a known vulnerability. In many cases, organizations are unable to deal with such initial breaches in a timely manner. Also, ransomware players use the same techniques against different organizations to exploit ransomware-related vulnerabilities. As a result of not patching those vulnerabilities - even after being exploited - ransomware players will exploit the same vulnerability against the same organization running a new ransomware campaign!

Qualys Ransomware Risk Prevention Solution helps organizations operationalize government guidelines, providing a specific ransomware heatmap to shrink their attack surface and eliminate risk areas. It features a dynamic dashboard for risk management, aligns with CISA's cybersecurity requirements, and uses extensive research to offer a proactive, actionable plan against ransomware threats.

Read the Blog about Qualys Ransomware Solution

Strategies for Protecting Your Business from Ransomware Attacks

Refer to Qualys Documentation and Qualys Videos to set up and configure Qualys capabilities, as required.



What I Get with Ransomware Solution (RAS) Enabled

When the Ransomware (RAS) is enabled, you can:

- Identify and prioritize ransomware vulnerabilities in line with CISA guidelines in your interactive **3 Tips For Ransomware Prevention** dashboard.
- Get prioritized, actionable insights for missing patches required to remediate your prioritized ransomware vulnerabilities.
- Deploy prioritized patches, utilizing automation wherever applicable. Ensure out-of-the-box support for internet-facing applications, including browsers, readers, and more, via the Qualys Patch Management application.





You will start seeing the following in your subscription based on your customer type:

Existing Customers

- After you import the dashboard in the Unified Dashboard module, the new dashboard will be available in your library for your ransomware risk assessment and remediation. Data based on agents that are enabled for the campaign is displayed in the widgets.
- Best Practice Controls for Malware/Ransomware Prevention policy in Policy Compliance.

(Only if you have CSAM enabled in your subscription) Default authorization rules, 'Software Elevating Cybersecurity Risk for Data Center Assets' or 'Most Common Ransomware Attack Vectors' to receive alerts on potential threats. <u>Configure Authorization Rule</u>.

New Customers

You will import the dashboard in the Unified Dashboard module, which will be provisioned in your subscription, along with other Qualys modules. The new dashboard will be available in your library for your ransomware risk assessment and remediation. Data based on agents that are enabled for the campaign is displayed in the widgets.

Trail Users

Once the trial is enabled, you can start using the Qualys Cloud capabilities provisioned in your subscription immediately to start assessing and mitigating your ransomware risk exposure. For more information, you can contact your TAM.



About the Ransomware Prevention Dashboard

Qualys enables organizations to quickly identify and locate vulnerabilities in their infrastructure.

The **3 Tips For Ransomware Prevention** dashboard displays the most critical vulnerabilities that are commonly exploited by ransomware groups. Ransomware vulnerabilities are automatically prioritized by Qualys Detection Score (QDS). This allows organizations to quickly identify and address critical ransomware vulnerabilities before they become problematic. The dashboard also allows you to patch vulnerabilities with a single click, if you have the Patch Management module enabled in your subscription.



Security leaders need this dashboard to ANALYZE the security posture of their infrastructure and what actions they can take to PREVENT a ransomware attack.



Advantages of using this dashboard

You can use this dashboard to:

Track	 Overall potential true risk based on our "TruRisk Score" Vulnerabilities in VMDR based on Ransomware RTIs Ransomware-related vulnerabilities, which are automatically prioritized by Qualys Detection Score (QDS) Vulnerabilities that can be patched
Patch	 Patch based on Ransomware RTI. You can use our Patch Management module or leverage your existing tools Patching on assets that operate software for processing internet data, such as web browsers, browser plugins, and document readers 3rd party apps - focused on web browsers and Adobe reader Create RTI-based automated patch jobs via our Patch Management module

With <u>Trending</u> enabled for dashboard widgets, you can keep track of vulnerability trends and ransomware-related compliance controls in your environment.





How do I access the dashboard?

Your subscription does not include this dashboard by default.

To access this dashboard

- 1. Click <u>here</u> to download the JSON file. If you need any help, you can reach out to your TAM.
- 2. <u>Import</u> the JSON file into the Unified Dashboard module.
- 3. Open the **3 Tips For Ransomware Prevention** dashboard in the **Dashboard** tab.

Note: Qualys Patch Management or a similar patch management tool is required for patching vulnerabilities.

CloudView V	DASHBOARD RESOURCES	MONITOR POLICIES REPORTS CONFIGURATION
AWS 🗸		
Last 90 Days		
RESOURCE DISTRIBUTION E	BY TYPE	FAILURES BY CONTROL CRITICALITY
450		Total Failures
350		2256
300		HIGH 1259
200		MEDIUM 974
150		
100		
0		
Internet Route Security Gate Table Group	r Instance 53 VPC EBS Subnet IAM P Bucket Volume User	ACL
TOP 5 ACCOUNTS BY FAILE	D CONTROLS	TOP 5 FAILED CONTROLS
ACCOUNT	CONTROLS FAILED	CONTROL RESOURCES FAILED
383031258652	52	Ensure database Instance snapshot is encrypted 602
883273722338	50	Criticality MEDIUM
		Ensure IAM policies are attached only to groups or 207 Criticality, Definition
		Ensure anness key1 is rotated every 90 days or less 105
		Criticality HIGH
		Ensure access keys unused for 90 days or greater 97
		Criticality HIGH
SECURITY POSTURE BY REC	SIONS	
		All Regions 600
	16	Total Resources 400
108 26	-31.	1619 200
	108	Inte_ Rou_ Loa_ Sec.InstancAut_ S3_ VPCSubneEBSNet
	40	Total Failures
+	31 17	2252 HIGH 1259
		MEDIUM 970



To view the Ransomware Prevention Dashboard

In the **Dashboard** tab, click the **Dashboard Picker** and then select the dashboard. The dashboard is added to your list of available dashboards, and you can start viewing ransomware-related data in your widgets.

82	3 Tips For Ra	nsomware Prevention			
Dash	boards			+	<u>نې</u>
3 tips					×
All Da	ashboards (1)	Frequently Used (458)	Favorites (0)		
	3 Tips fo All Assets p Created On:	r Ransomware Prevention art of the qualys patch POC Nov 30, 2023 04:07 AM		습	:



Let's Get Started

The most important step to start protecting your organization from ransomware threats is having an extensive, thorough, and up-to-date inventory.

With an in-depth IT asset inventory, you can:

- Identify dangerous blind spots in advance
- Adequately understand your environment to prioritize assets and risks
- Plan further visibility and protective measures.





Step 1 – Build your Inventory

CyberSecurity Asset Management (CSAM) helps you discover and inventory assets and accurately assess complex IT infrastructure so you can quickly identify and remediate risk.

Note: This step is for customers with CSAM enabled in their subscription. You can contact your TAM to enable CSAM for your subscription.

Start building your inventory by installing cloud agents. With our lightweight agents, you'll get continuous network security updates through the cloud. As soon as changes are discovered on your hosts, they'll be assessed, and you'll know about new ransomware threats right away.

Qualys. Cloud P	atform																			
CyberSecurity Asse	t Mana	agement 🗸	ном	E DASHBOARD INVENTORY	TAGS NETWORK	RULES RESPONSES REPORT	S	80 🗠												
Managed	~	Assets Software																		
		X NOT software:(category2:[`Antivirus`,	Endpoint Protecti	ion'])			(Last 30 Days 🗸 📃												
90		TOP HARDWARE CATEGORIES			TOP OPERATING	SYSTEMS CATEGORIES														
Total Assets		0 Virtualized	Unidentified	Computers		Linux Win	dows Mac	Unidentified												
MANUFACTURER	25	Actions (0) V Group Assets by V					1 - 50 (of 90 🔇 🔈 🕹 🖒 🖬 🛞												
Google	22	ASSET	CRITICALITY (1)	OPERATING SYSTEM	HARDWARE	LAST USER	SOURCE	TAGS												
VMware Apple 1 more 👻	20 20 2	ip-192-168-0-185.ec2.internal 192.168.0.185 06:96:b1:af:b5:be	4 😴	Amazon Web Services Amazon L 2.0	- Virtual Machine	reboot	QAGENT Updated: Sep 30, 2021	192.168.0.0/16 21 more												
TAGS Cloud Agent	90	demo-gcp-uc1-vm1.c.gcp-qualy 10.128.15.234,fe80:0:0:0:4001:aff:fe80 42:01:0a:80:0f:ea	4 Δ	Debian Project Debian GNU/Linu 10.2	Google Compute Engine Cloud Instance	reboot	QAGENT Updated: Sep 30, 2021	Data Center 20 more												
All Assets OS: Windows 8.1 Scanned in 180-D	90 90 87 86	90 90 87 86	90 90 87 86	90 90 87 86	90 90 87 86	90 90 87 86	90 90 87 86	90 90 87 86	90 90 87 86	90 90 87 86	90 90 87 86	90 90 87 86	90 90 87 86	ip-172-31-36-198.us-east-2.co 3.134.103.36,172.31.36.198 0a:dd:14.87:b8:ae	2 🕲	Canonical Ubuntu Bionic Beaver 18.04 LTS 18.04.5 LTS	Amazon Web Services Amazon EC2 T3 t3.micro Cloud Instance	reboot	QAGENT Updated: Sep 30, 2021	OS: Ubuntu xx 16 more
45 more ⊌		WIN-890BLRMESC6 10.115.67.165 00:50:56:AA:1F:01	5	Microsoft Windows Server 2012 Standard6.3 64-Bit	VMware VMware Virtual Platform Virtual Machine	exchange.local\Administrator	QAGENT Updated: Sep 30, 2021	Crash_TCP_Unknown 32 more												
		demo-gcp-uw2-redhat-6-public 10.0.0.139,fe80.0.0.0.4001.aff.fe00.8b 42:01:0A:00:00:88	4 Δ	Red Hat Enterprise Linux Server 6 6.10	Google Compute Engine Cloud Instance	reboot	QAGENT Updated: Sep 30, 2021	GCP-Public-Instance												
					1	/	/	/												

Install Qualys Cloud Agents | Cloud Agent Getting Started Guide | Cloud Agent Onboarding Videos

You can have cloud agents on private clouds, public clouds, on-premises, and endpoints to continuously discover your IT assets, providing 100% real-time visibility.

CSAM Quick Start Guide | CSAM Onboarding Videos | CSAM Online Help



© 2 0 2 4 Qualys. All rights reserved.

Step 2 (a) – Detect at-risk Assets and Applications

CSAM enriches your asset inventory with in-context, relevant information to help you detect at-risk assets and applications. You can identify and set alerts for assets that are running unauthorized software or are not using anti-virus/endpoint security tools.

Unauthorized software should be removed to quickly reduce unnecessary attack vectors. With CSAM, you can easily define rules to monitor unauthorized software installations.

Use CSAM to identify assets that are missing required security software, such as Antivirus and Endpoint Protection. Navigate to the Inventory tab and form queries to search for desired results.



CSAM Quick Start Guide | CSAM Onboarding Videos | CSAM Online Help



Step 2 (b) – Detect at-risk Assets and Applications

You can also identify End-Of-Life/End-Of-Support software, which can be used as ransomware attack vectors. End-of-Support software is one of the first things hackers look to exploit because they are aware that the publishers are no longer providing security updates and patches.

Configure tags so you can apply them to assets in your subscription. This helps you to organize your assets and to manage user access to them. Let's say you create a tag "RDP Asset" to find all assets with Remote Desktop Protocol (RDP) service enabled, then all assets with RDP service enabled will be grouped along with any new hosts that get added to the environment. <u>How to configure tags?</u>

Example of CSAM Ransomware Dashboard





Step 2 (c) – Detect at-risk Assets and Applications

Configure Authorization Rules

Configure rules to monitor critical events that satisfy the conditions specified in a rule and send you alert messages if events/incidents matching the conditions are detected.

You can enable the default authorization rules, 'Software Elevating Cybersecurity Risk for Data Center Assets' or 'Most Common Ransomware Attack Vectors', to receive alerts on potential threats.

Navigate to **Rules > Software Rules** and choose a rule. Then, from the **Quick Actions** menu, click **Enable**.

You can also create your own rules. Know more about Creating Software Rules.

	U	U	U	U	
_					
	_				
				_	
ш					
			/		
	-	/			





Step 3 (a) – Prioritize Vulnerabilities

Now that your inventory is in place use VMDR to assess, prioritize, and remediate the vulnerabilities and misconfigurations on your assets.

VMDR helps you automatically detect and prioritize the specially researched vulnerabilities, and the threat feed helps you understand your asset exposure to highprofile exploited vulnerabilities.

Navigate to VMDR and use the tags to identify and analyze the vulnerability information of your ransomware-scoped assets. We will prioritize the risk against specially researched CVEs and generate a report.

Now that hosts with the "RDP" service are identified by the tag you created; you want to detect which of these assets have flagged this vulnerability. VMDR automatically detects new vulnerabilities like Windows RDP, Exchange Server vulnerability, and more based on the updated Knowledgebase. You can see all your impacted hosts for this vulnerability tagged with the 'Ransomware asset tag in the vulnerabilities view by using this QQL query:

vulnerabilities.vulnerability.ransomware.name:Cerber

Qualys. Clou	d Platform														
VMDR 🗸		DASHBOARD	VULNERABILITIES	RESPONSES	PRIORITIZATION	SCANS	REPORTS	REMEDIATION	ASSETS	THRE	AT INTELLIGEN	ICE KNOWL	EDGEBASE U	ISERS	2 @
Vulnerabilities															
		Vulnerability 🗸	vulnerabilities.	vulnerability.	.ransomware.nam	e:Cerber									× ⊞ ⑦
385	5	 Qualys Insights co 	nsolidates data to get a	n enhanced view o	of the security posture	e.									View Qualys Insight
Total Detection	ons	Actions (0) V Assel	Vulnersbility	Group by 🗸	S [®] Fil	lers 🗸	Import Detections						1 - 50 of 385 🔇	D & C M
EVERITY		QID	TITLE						SOURCE	QDS 🕓	SEVERITY	LAST DETECTED	↓ FIRST DETECTED	ASSET	TAGS (BETA)
	287	91355	Microsoft Win Active	ndows Security	Update April 2017	,			Qualys	100		12/12/2023	09/06/2023	SHAREPOINT2 335575105	Critical Vuln 1 more
TEGORY	98	124185	Google Chron Active	ne Prior to 46.0.	.2490.80 Adobe F	lash Player U	Ipdate		Qualys	100		12/12/2023	02/11/2023	WNSRV2012-2 739736722	Critical Vuln
indows cal	244 60	91355	Microsoft Win Active	ndows Security	Update April 2017	,			Qualys	100		12/12/2023	. 12/10/2021	w2k8r2es2012 417398791	Critical Vuln
ernet Explorer	39 28	91355	Microsoft Win Active	ndows Security	Update April 2017	,			Qualys	100		12/12/2023	12/10/2021	vsdynamics20 417412952	Critical Vuln
SI SI	6	91355	Microsoft Wir Active	ndows Security	Update April 2017	,			Qualys	100		12/12/2023	. 14/10/2021	dyn365v9-1p.v 418650263	Critical Vuln
PERATING SYSTEM		100217	Microsoft Win Active	ndows Update fo	or Vulnerabilities i	in Adobe Flas	sh Player in I	internet Ex	Qualys	100		12/12/2023	12/10/2021	vs-lyncsrv201 417422031	Critical Vuln 1 more
indows Server Indows Server	51 37	124154	Adobe Flash Active	Player Security	Update (APSB15-	27)			Qualys	100		12/12/2023	12/10/2021	vs-lyncsrv201 417422031	Critical Vuln
indows Server Indows 8.1 Ent.,	36 24	100261	Microsoft Win	ndows Update fo	or Vulnerabilities i	in Adobe Flas	sh Player in I	Internet Ex	Qualys	100		12/12/2023	12/10/2021	vs-lyncsrv201	Critical Vuln

VMDR Onboarding Videos | VMDR Getting Started Guide | VMDR Online Help



Step 3 (b) – Prioritize Vulnerabilities

From a prioritization perspective, TruRisk scores can be further combined with additional attributes using QQL to refine the prioritization process. Here's an example:

Vulnerabilities.vulnerabilities.threatIntel.ransomware:true and vulnerabilities.detectionScore>80 and vulnerabilities.typeDetected:'Confirmed'

Generate a <u>VMDR Prioritization Report</u> to detect which vulnerabilities to remediate first, identify the most critical threats, and prioritize patching.

Using the prioritization report, the ransomware vulnerabilities can be easily prioritized using "Ransomware" Real-Time Threat Intelligence.







© 2 0 2 4 Qualys. All rights reserved.

Step 3 (c) – Prioritize Vulnerabilities

VMDR also enables you to stay on top of these threats proactively via the 'live threat feed' provided for threat prioritization. With the 'live feed' updated for all emerging high and medium risks, you can clearly see the impacted hosts against threats. Simply click on the impacted assets for the "Ransomware" feeds to see the vulnerability and impacted host details.

Introduction to VMDR Videos Best Scanning Strategy Videos

VMDR ~	DASHBOARD VULNERABILITIES RES	SPONSES PRIORITIZATION SCANS REPO	ORTS REMEDIATION ASSETS
Prioritization Repo	orts Threat Feed		
contents:ranspmware			
р			
Any All			
HIGH RATED FEED 31		MEDIUM / LOW RATED FEED 8	
High	10/11/2023 公 三	Medium	16/05/2023
SysAid On-Premise Server Vulner	ability and Active Exploitation by Ransomwa	PoC Exploit available for CVE-2020-14	/2
Live mneat Intelligence Feed SysAid, a la recently issued a critical advisory. The n their on-premise server software, which	ading IT Service Management (ITSM) solutions provider, ofice reveals a previously undisclosed vulnerability in Is currently being exploited in the wild. This escalation	An exploit for CVE-2020-1472 is now available 374028, 375010, 91668, 178231, 373486, 2570 373569, 198077, 174081, 280446, 91680, 1740	rrom cisa-alerts. Qualys has added QID(43, 373557, 198030, 91688, 198031, 286 71, 174072, 174069, 174070, 238937, 35
	0		87
	Impacted Assem		limpacted
High	18/09/2023 合 三	Medium	08/09/2022
CISA Added Cisco Adaptive Secu	urity Appliance Software Vulnerability to its	PoC Exploit available for CVE-2021-34	527
Live Threat Intelligence Feed CISA has a Software and Firepower Threat Defense The addition of the vulnerability to CISA	dded a vulnerability in Cisco Adaptive Security Appliance Software to its Known Exploited Vulnerabilities Catalo g . KEV is the acknowledgment of active exploitation of the	An exploit for CVE-2021-34527 is now available 91785 to detect this issue in your environment. ASSETS WITH PUBLIC EXPLOIT AVAILABLE or	from clsa-alerts. Qualys has added QID Please check your ThreatPROTECT das search for
	2 Impacted Assets		34 Impacted
High	12/04/2023 🏠 🚞	Medium	10/02/2022
	023 Security Update Review	PoC Exploit available for CVE-2017-01	44
Microsoft Patch Tuesday April 20			

Read more about the vulnerability threat landscape here:

An In-Depth Look at the Latest Vulnerability Threat Landscape

An In-Depth Look at the Latest Vulnerability Threat Landscape (Attackers' Edition)



Step 4 – Deploy Patches

Ensure that all assets, system components, and software are protected from known vulnerabilities by deploying curated ransomware patches.

You can quickly identify all missing patches from your VMDR prioritization report. Use the method described above to filter only ransomware-related vulnerabilities. Select the vulnerabilities you would like to remediate and add them to a new job. Qualys will automatically map all the selected vulnerabilities to the patches that remediate those vulnerabilities and are relevant to your environment. Only the latest patches will be included, saving the need to deploy old patches that have been superseded. Configure the patch job and deploy the patches to your vulnerable assets. You may also use our zero-touch patching capability to intelligently identify and automatically deploy the proper patches required for remediating vulnerabilities.



Deploying Patch Jobs on Assets | Patch Management Getting Started Guide | Patch Management Videos



Assess Misconfigurations

The Policy Compliance (PC) and Security Configuration Assessment (SCA) help organizations evaluate research-driven configuration policies for ransomware to identify, assess and remediate misconfigurations exploited by ransomware. Configuration management adds context to your overall vulnerability management.

Qualys Policy Compliance provides Best Practice Controls for Malware/Ransomware Prevention policy that contains the critical controls mapped to MITRE ATT&CK mitigations and tactics recommended by CISA.

Posture						
		Controls V X policy.name	Best Practice Controls for Malware/Ransomware P	revention		: : :
15.8 Total Control In:	stances	overall compliance Compliance 31.74%	Total Passed Total Failed	FAILURE BY CRITICAL 6/K	ITY TICAL SERIOUS	URGENT MEDIUM MINIMAL
OSTURE	10.8K	Controls Assets Group by :	Control Category $ imes imes$			1-7 of 7 🤇 📐 🕹 🖒
ASS	5.02K	CONTROL CATEGORY	ASSET COUNT	ASSET INSTANCE COUNT	CONTROL COUNT	CONTROL INSTANCE COUNT COMPLIANCE SCORE
ERROR 1	1	OS Security Settings	70	70	111	8.13K — 16.3
RITICAL	6.15K 4.71K	Access Control Requirements	70	71	88	6.25K 52.4
RGENT	3.63K 1.22K	Integrity and Availability	69	69	5	410
MINIMAL 110 Exception status	Anti-Virus/Malware	70	70	б	39459.	
		Encryption	70	70	б	38622.
			[Entire] Network Setting	69	69	2
		Services	70	70	1	85

Navigate to the **Policy Compliance > Dashboard > Posture** tab in your subscription to view all findings returned from the policy.

Security Configuration Assessment Online Help | Policy Compliance Getting Started Guide | Policy Compliance Videos

