

Zero Trust Access with Qualys Platform



Ashish Kar Director, Product Management Qualys



Enterprise TruRisk[™] Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.



What is Zero Trust?

- Don't trust any device, user, or app
- Access is granted only after Authentication and Authorization
- Authorization is determined by dynamic policy
- Every access is Audited
- Access is granted on a session basis





Source: NIST SP 800-27 Tenets of Zero Trust

Why Zero Trust is hard to implement



- Enterprise Infrastructure is incredibly complex.
- Leads to business continuity risk if policies are not defined properly.
- Risk-based **prioritization** is missing in most cases.



Qualys Risk-based Zero Trust Access



SaaS Endpoint Data Protection



Compliance Risk Inventory Risk Unauthorized SW Risk Vulnerability Risk Malware Risk

- Measure: TruRisk for Endpoint and Service
- Communicate: Risk to Security team and user
- Eliminate: Risk by giving endpoint limited or no access to service



Easy workflow for the security team

Policy in Qualys Platform

- TruRisk>500 no access to internal document
- TruRisk>700 no network access

OveDrive		test .			4897
+ 44000		- Cymraet	-	A.0.45	
Adult for	PETRONY Not Designed 1	Large-	April da	# mineriterat	and the second
5 mm	Discountries	Disc appoint	ingmide day	# manufactures	and the last
C M fee	CDC Agenda Disivita 2023 - Char Textures, II	10- MP	in Dec	Matrice preside edited in	
to have	Bod, Scorreg God 2021	These lines	Addust Dimension	P Mathal Recording ()-	and a local de la companya
The second second	Instantion	6.44	Amilda	1 marine	
1. 1. 00	MON 1754 Function	hee		- Dimminia	
2 therein C	Distance of			O manifest and	-
Elinait Otra lington	0- In-		and the	2 months in the	-
Columbia	De Manufactor Desiman 2011			a married	in the second second
Products - Ent Asams	Marking large large	have the second	ALC: NO.	C Senart Duranale	multiple dampile in
Vaninginity Management	Displant	hy a strait.	Juniy Course	C day best incom	
Statutes Reporting	Dializa in Ferrit si	CHIEF.	control interesting	C Metal Bearing on	and the second second
With Application Sciences	Pair Strang Documer Officer (001) Property Management	- 200	-	a Martin Graperton	and some Yest Y
	(a) 174 (a)	1444		P Manta Sequeira	100 K
	a talange	1000	-		

Malware Infected Endpoint

- Malware activity TruRisk 800
- Network access blocked





Risky Endpoint

- Running risky software TruRisk 535
- Only external documents are visible









THANK YOU



Why Zero Trust is a game changer



- Enterprise Infrastructure is

 allowing attackers to hide in plain sight
- Zero Trust assumes that the your environment
- Reduce Risk by preventing lateral movements and data breaches.



Demo Flow for #1

Approve or Deny Access to SaaS or network based on the TruRisk Score of the Endpoint

- The analyst also applies a policy that if (1) TruRisk is >500, then there is no access to O365 internal data – as a preventive measure in the future, (2) if TruRisk>700, then quarantine network access
- The next day, the analyst discovers an endpoint with unsanctioned SW TruRisk is 500+
- The access to O365 is only limited to public docs, no internal sensitive doc is visible.
- The next day, the analyst discovers an endpoint with malware TruRisk is high
- The malware cannot get to O365 sensitive data due to policy, the malware cannot exfil data as the network is locked down.
- The analyst fixes the malware issue, and now O365 access is restored
- Key points (1) Auto-remediate config issues, (2) Put preventive policies commensurate with risk – like removing sensitive data access, or blocking all egress, (3) Once the issue is fixed, the operation is restored.



Screen 1

Admin

Enable TruRisk Scoring for EDR product

OPTIONAL

EDR UI

Toggle on TruRisk Scoring



Screen 2 - Create Rules in Qualys SaaS-DR to

Q serreds .

box ADMAN

... Insights

Content Reports

Governance

K. Relay

Platform III Apps

Rule 1 – TruRisk >550, Limit access to internal files, only show external files.

Rule 2 – TruRisk>700, Limit access to O365, network on endpoint is quarantined.

EDR \rightarrow O365 rule

There is a page in Qualys SaaS DR that allows the user to configure rules between EDR score and a SaaS Application.

> Define Risk Level and **Remediation Step**



Admin



Screen 3 – TruRisk score 500

User downloads risky software and her TruRisk is 550. Now she is not able to view internal sensitive docs in her O365.

Put 2 screenshots of the O365 folder -

- 1) with both internal and external files and
- 2) with external files only.

We can show once her risk got high, her view changed from 1 to 2. Also, got a message to delete the software or contact the IT/Sec team.

	Name T	Created >>	Created By	Modified ~	Modified By
	1.QSC Orlando Storyboard Template.docx	Yesterday at 8:44 PM	Utpal Desei	3 hours and	Vinicial liver
	AI-ML.docx	Yesterday at 8:57 PM	Visual lyer	Yesterday at 9:05 PM	Vinud lyes
	Data Driven Risk Prioritization.docx	s hours ago	Abhishek Singh	5 minutes ago	Abhishek Singh
	Endpoint Security.docx	Yeslerday at 9115 PM	Vinod liver	Yesterday at 10:25 PM	Andrew Morrisett
	Risk Reduction .docx	Yestenday at 8117 PM	Vinind liyer	15 minutes ago	Efán Livne
	TotalCloud .docx	10 hours and	Viend lyer	10 Rours alto	Vinco Iver
	WAS.docx	4 hours ago	John Dobrotheon	4 bears ann	John Delamdena
	All Fi	les are	e visik	ole	
- N	All Fi w ~ ↑ Upload ~ ⊞ Edit in grid view	les are	e visik	E All Documents	- 7 0
- N	All Fi w ✓ ↑ Upload ← I Edit in grid view nents → Conferences ● QSC → QSC U	ee Share که Copy ISA 2023 > Decks f	e visik	DIE = Ali Documents	7.0
- Ni cum	ew ~ ↑ Upload ~ 目 Edit in grid view hents > Conferences + QSC > QSC U	Ies are Share @ Copy ISA 2023 > Decks f Created ~	e visit	E All Documents	 ∇ .Q Modified By ~
- Ni	MIFi w	Les are Les share @ Copy ISA 2023 > Decks f Created ~ About an Nouthago	e visit	E All Documents Modified ~ About an hour ago.	- 7 O Modified By ~ Abhishek Singh
cun	W V T Upload V Edit in grid view T T Conferences V C V C Name V V C S Conferences V C C V C V C V C V C C C C C C C C C	IES are Share & Copy ISA 2023 > Decks f Created ~ About an houl upo Tuesday at 10/21 AM	e visit	All Documents Modified About an hour apo Tuesday at 10 21 AM	 √ Q Modified By ~ Abhshek Singh Vinod Iyer
cup	All Fi w Tupload Plant Edit in grid view hents Conferences QSC QSC Conferences QSC QSC Conferences QSC QSC Conferences QSC Conferences QSC Conferences QSC Conferences Conferences	Ies are Share Copy ISA 2023 > Decks f Created ~ About an houff ago Tuesday at 10/21 AM	Ink Created By ~ Abmsnek Singn visiod Iyer	All Documents Modified ~ About an hour age ruesday at 10 '21 AM	Modified By ~ Abhshek Singh Vinod Iyer
cun	All Fi w T Upload T Upload Edit in grid view nents Conferences QSC QSC Name C Name C QSC Corlando Silde Template.pptx C C C C C C C C C C C C C	Les are Le Share @ Copy ISA 2023 > Decks f Created ~ Acout an Noull ago Tuesday at 10/21 AM	e visit	All Documents Modified Tuesday at 10 '21 AM	- T O Modified By ~ Abrishek Singh Vinod Iyer



Screen 4 – Admin gets an alert Can take remediation steps

Admin gets an alert - Access denied to "Internal O365 files" due to risky SW on the endpoint.

The actions she can take are

- Contact user
- Remediate
- File Jira
- Ignore



Admin workflow



OLD VERSION





Zero Trust Access with Qualys Platform

October 2023

What is Zero Trust?

- Don't trust any device, user, or app
- Access is granted only after Authentication and Authorization
- Authorization is determined by dynamic policy
- Every access is Audited
- Access is granted on a session basis





Source: NIST SP 800-27 Tenets of Zero Trust

Why Zero Trust is a game changer



- Enterprise Infrastructure is

 allowing attackers to hide in plain sight
- Zero Trust assumes that the your environment
- Reduce Risk by preventing lateral movements and data breaches.





SaaS Endpoint Data Protection



EDR

Qualys Zero Trust Access

Office 365

SaaS-DR

- Endpoint has Qualys EDR with TruRisk turned on
- Continuous risk-based authorization
- Action can be taken on the endpoint or SaaS product



Easy workflow for the security team

Policy in Qualys Platform

- TruRisk>500 no access to internal document
- TruRisk>700 no network access

	and free lat.				
DieDive		2 Sec.			4.8.9.7
	Ser.	Operand	-	Adves	
Adulto	PLINED Replace.et	here.	Same day	# mineters	Nov (SA. Salada
in such	Bar Constitutes	1 Pro appoint	ingenity day	# manufactures	Same and Barlage.
D M fai	CC Agenda Doorino 2021 - Cany Sectore, IV	10 mm	See Dans	Address oversite edited	1. Ta
the later	Ban, Ausereg Get 2001	These States	Adda Disarrige	P Matul Brownia ()	Additional advertised
2 hours and	Ban Castadenia-	6.6	Amitie	I manine	-
à tun 🚥	WOI 114 factor	Sec. 1		2 marine	÷
Station Contractor	Diff lamon of			2 marine m	-
atimath Otta Longian	0- In-		and the	a second doctor	
CSM - Operation Am	De Landrage (Sectores 201)	Se Containing		a lass 27ada	in the second
Products - Day Austra	Di Malina Despines	Nov # 1212 Int.	ALC: NO.	C Senart Durana	a most into a change but the
Vaningshity Managemen	De Braylant Jacq Teacy Frain	hypertrai-	Juniy Course	C they bear incom	
S viewicz mpartog	Di Balia in Secti di	CHIEF-	control dimension	C Metal Baratha	and the same part of the
😸 Welt Application Forming Man pain.	Anis Servery December Officer (01) Property Nampusar	- 2013	allowed the state of the	al Manta Langarita	and the York Y
	(E) (Printer (in)	Tank .		P Martin Sergeria	and the other states of the local diversity of the local dintersity of the local diversity of the local diversity
	Distances	1004			

Malware Infected Endpoint

- Malware activity TruRisk 800
- Network access blocked



Risky Endpoint

- Running risky software TruRisk 535
- Only external documents are visible





Demo Time





Enterprise TruRisk[™] Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.



Screen 5 – TruRisk score 800

Another user, clicks on a link and has malware on his endpoint – trurisk is > 700. His laptop is quarantined.

Analyst gets an alert and can send a remediation action to remove the malware and restore network access.



You might have an infected machine. Contact your admin.



Screen 6 – Admin gets an alert Can take remediation steps

Admin gets an alert - Network Quarantined due to malware on the endpoint.

The actions she can take are

- Contact user
- Remediate
- File Jira



Admin workflow







Thank you

