Zero Trust Access with Qualys Platform

Ashish Kar
Director, Product Management
Qualys

Qualys®

Enterprise TruRisk™ Platform

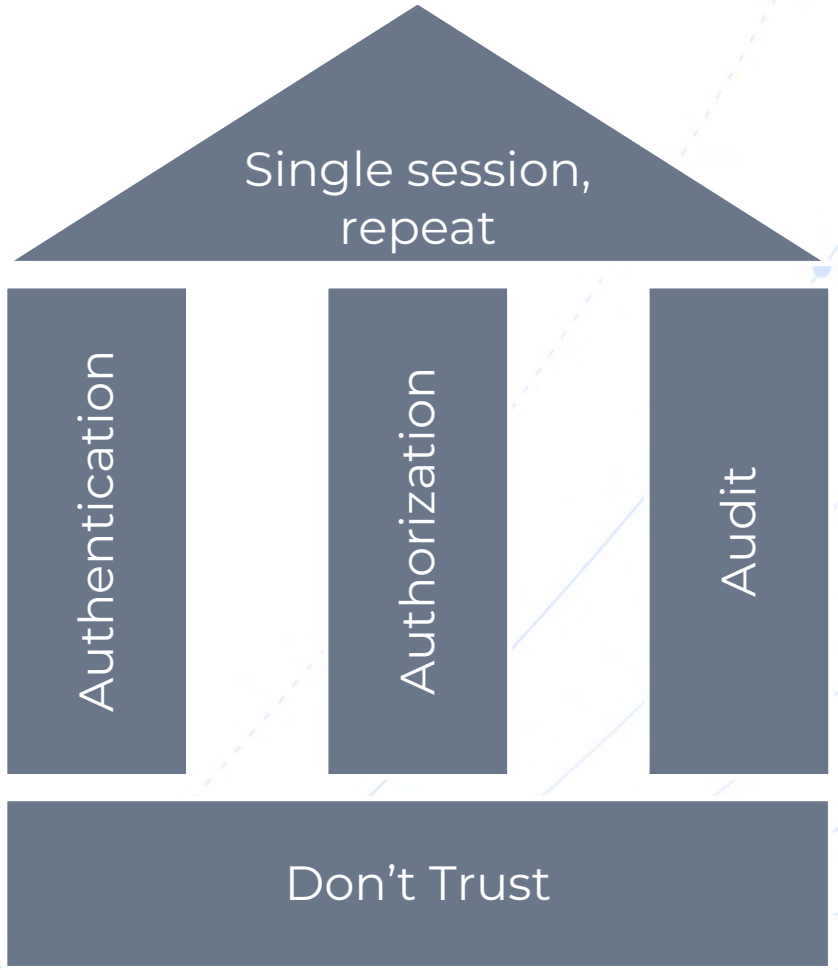
Measure, communicate, and eliminate cyber risk.

De-risk your business.

Qualys®

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

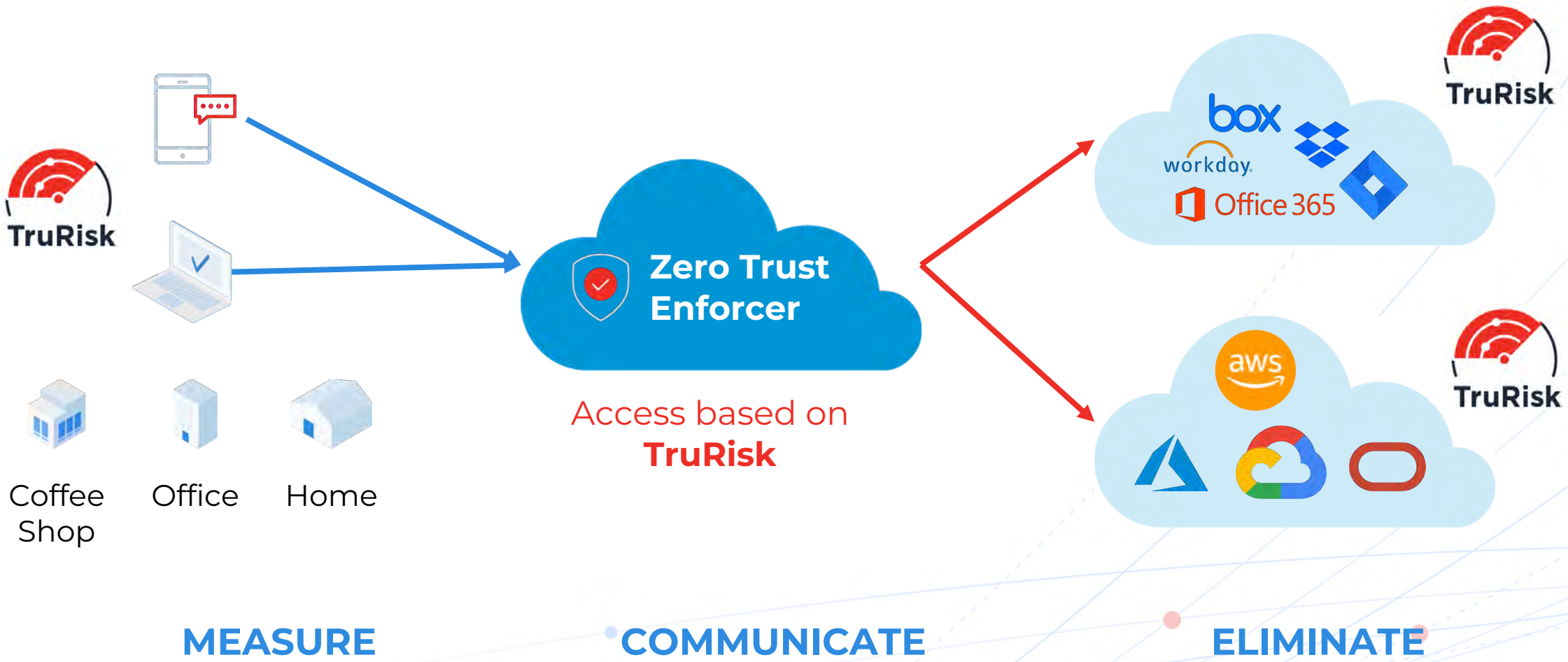
Why Zero Trust is hard to implement

- 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.

Photo by Matthew Henry on Unsplash

Qualys Risk-based Zero Trust Access



MEASURE **COMMUNICATE** **ELIMINATE**

Qualys.

SaaS Endpoint Data Protection

Compliance Risk
Inventory Risk
Unauthorized SW Risk
Vulnerability Risk
Malware Risk

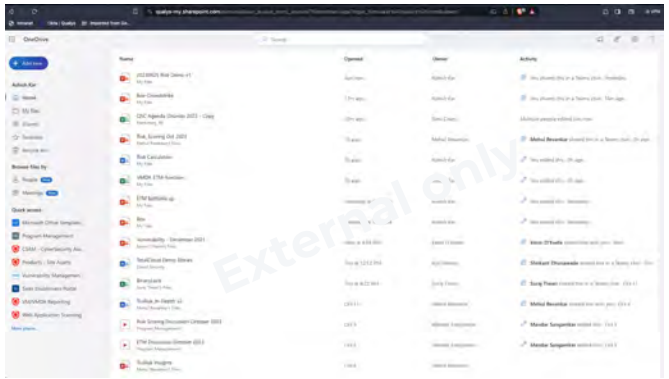
- **Measure:** TruRisk for Endpoint and Service
- **Communicate:** Risk to Security team and user
- **Eliminate:** Risk by giving endpoint limited or no access to service

Qualys.

Easy workflow for the security team

Policy in Qualys Platform

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

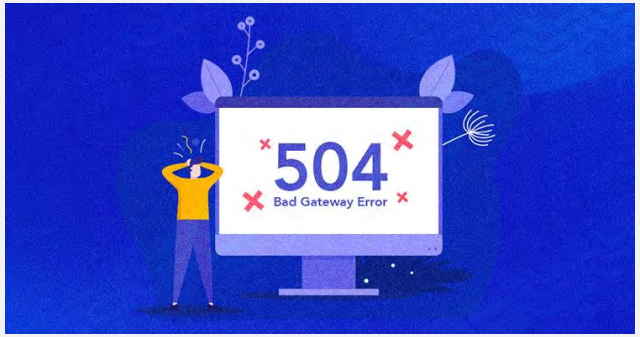


Malware Infected Endpoint

- Malware activity – TruRisk 800
- Network access blocked

Risky Endpoint

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



Qualys.

Demo

Qualys.

THANK YOU

Why Zero Trust is a game changer

- Enterprise Infrastructure is incredibly complex – allowing attackers to hide in plain sight
- Zero Trust assumes that the attacker is already in your environment
- Reduce Risk by preventing lateral movements and data breaches.

Qualys.

Photo by Matthew Henry on Unsplash

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

Qualys.

Screen 2 - Create Rules in Qualys SaaS-DR to

Admin

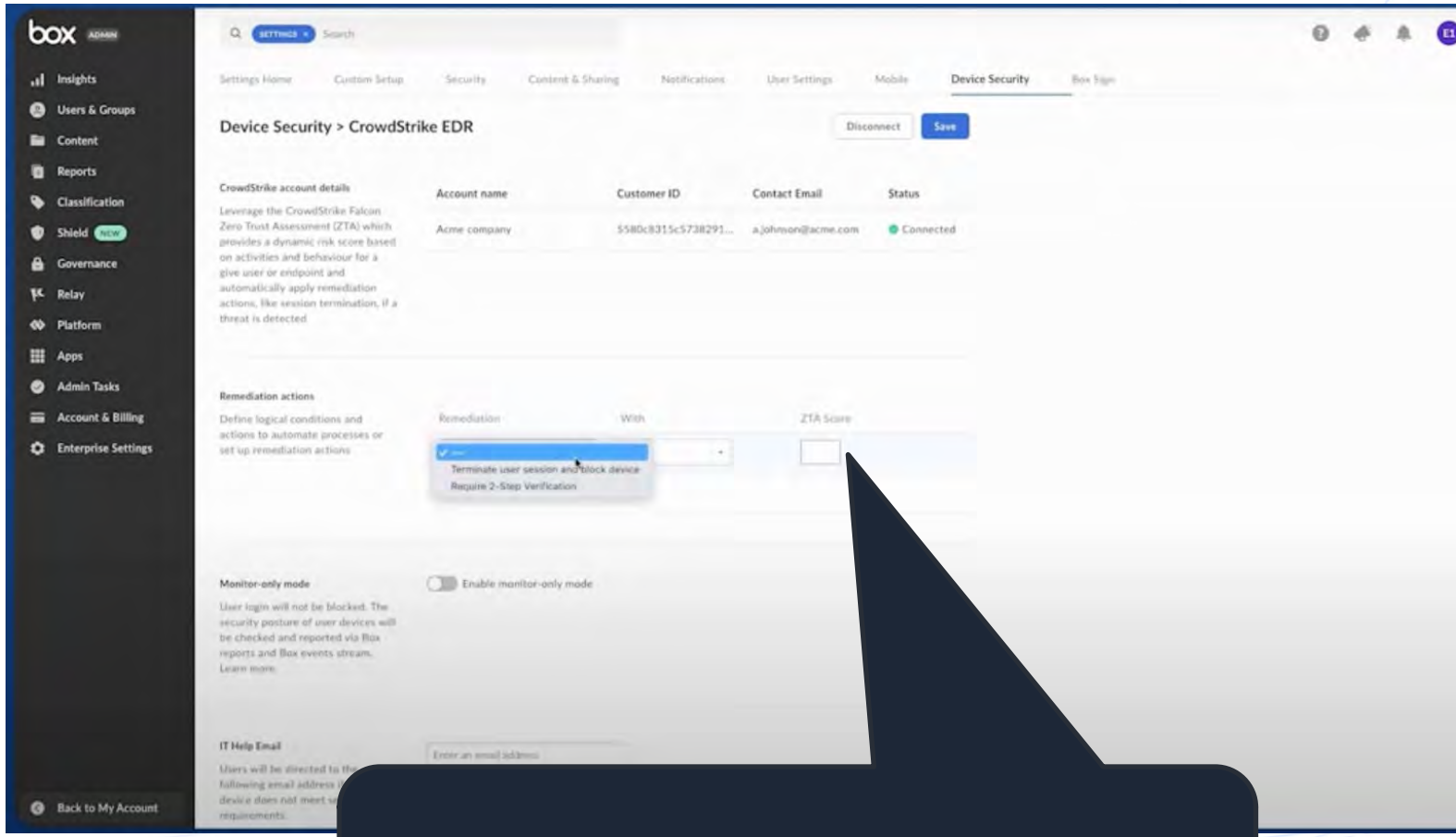
Rule 1 – TruRisk >550, Limit access to internal files, only show external files.

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

EDR → 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



This is how BOX recently did it with Crowdstrike

Qualys.

Screen 3 – TruRisk score 500

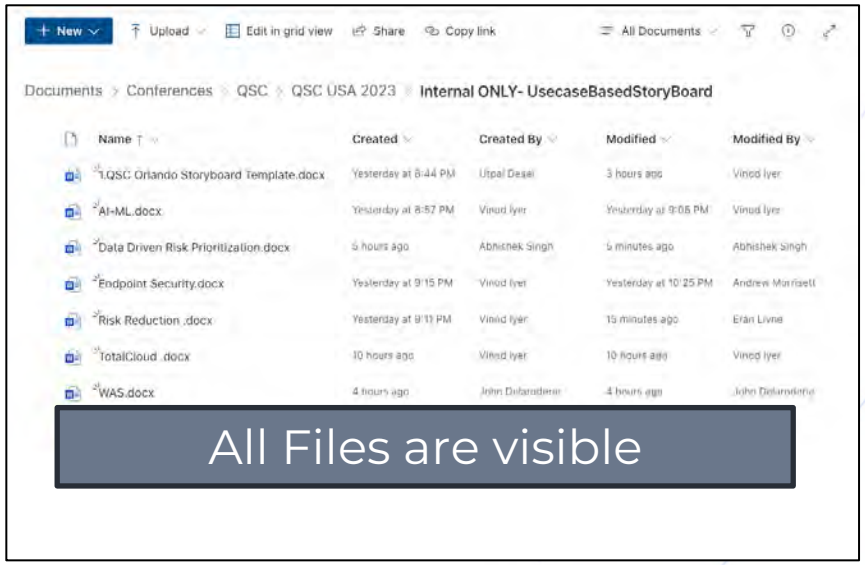
User

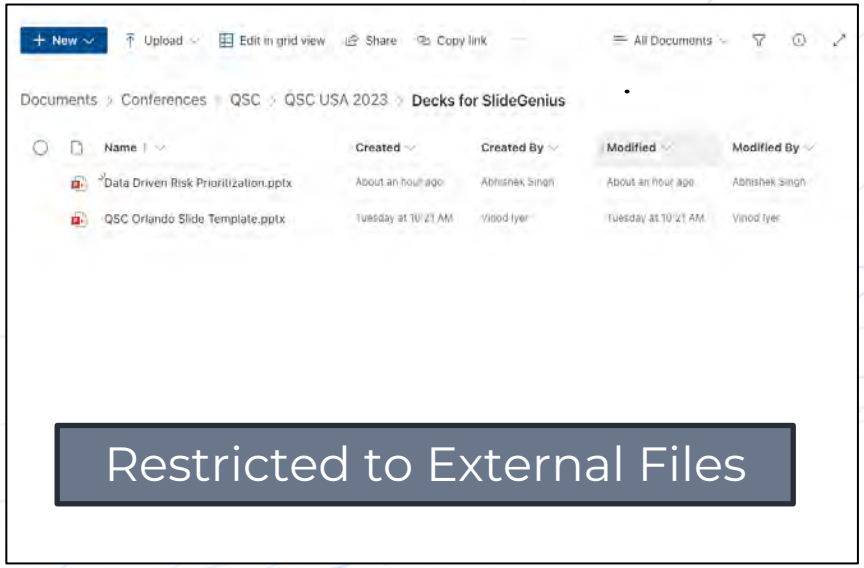
User downloads risky software and her TruRisk is 550. Now she is not able to view internal sensitive docs in her O365.

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.





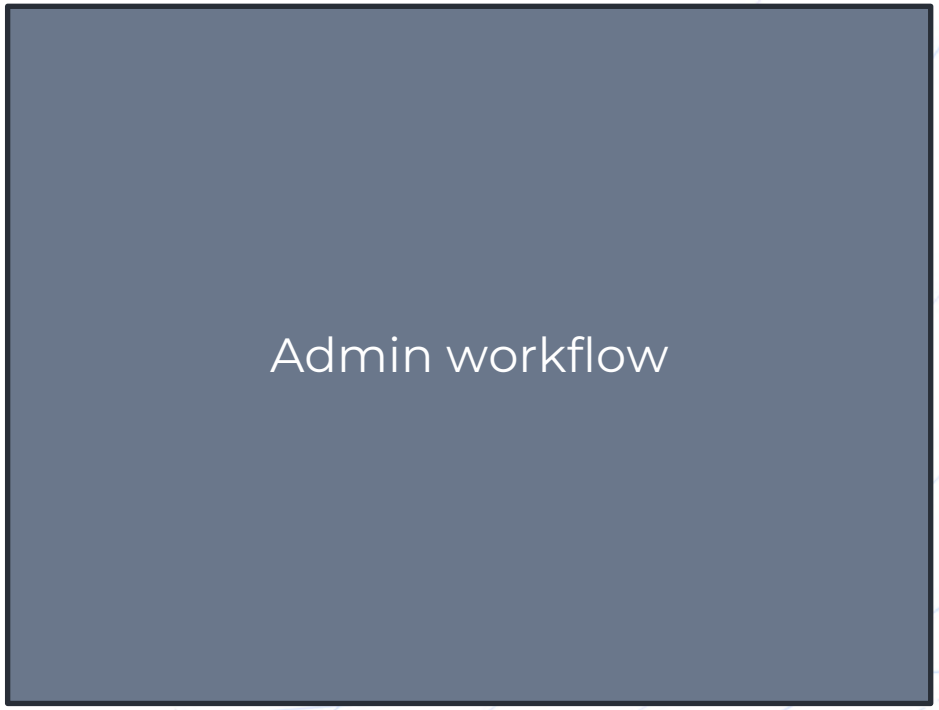
Qualys.

Screen 4 – Admin gets an alert
Can take remediation steps

Admin

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



Qualys.

OLD VERSION

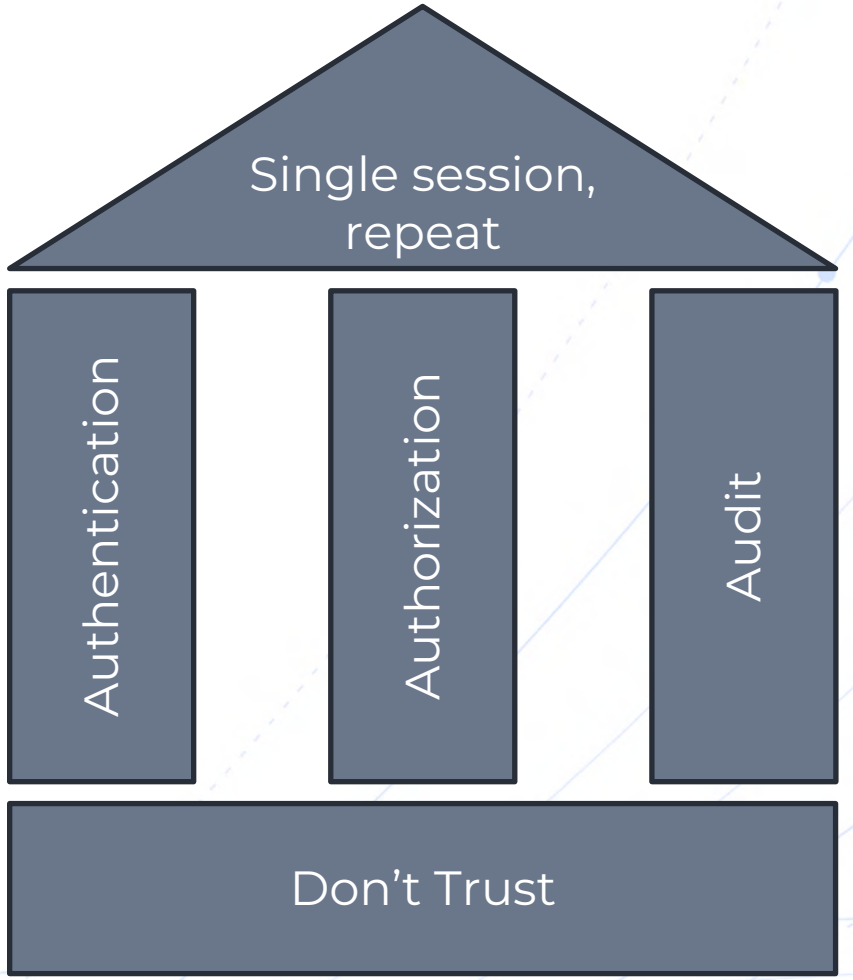
Qualys®

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

Qualys.

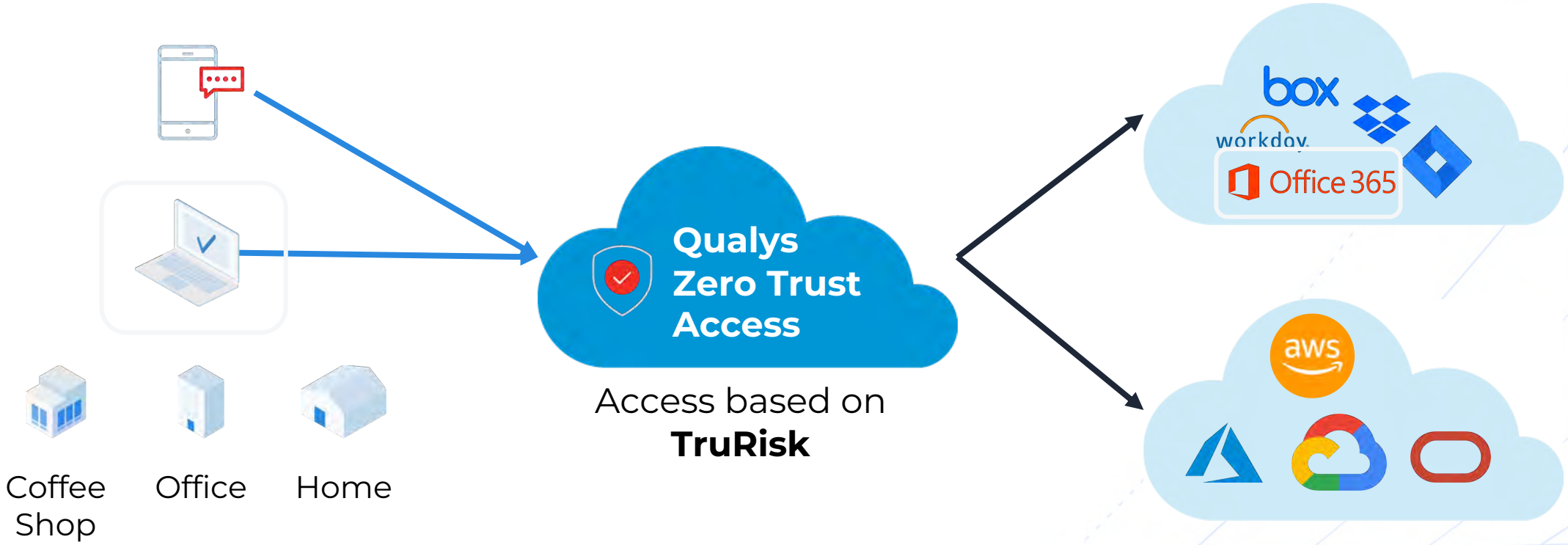
Why Zero Trust is a game changer

- Enterprise Infrastructure is incredibly complex – allowing attackers to hide in plain sight
- Zero Trust assumes that the attacker is already in your environment
- Reduce Risk by preventing lateral movements and data breaches.

Qualys.

Photo by Matthew Henry on Unsplash

Qualys Zero Trust Access



Qualys.

SaaS Endpoint Data Protection

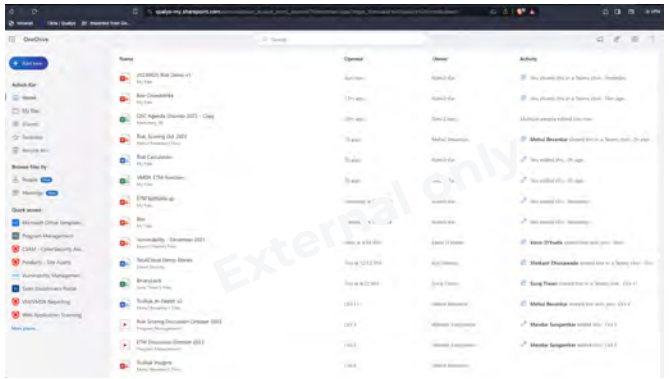
- Endpoint has Qualys EDR with TruRisk turned on
- Continuous risk-based authorization
- Action can be taken on the endpoint or SaaS product

Qualys.

Easy workflow for the security team

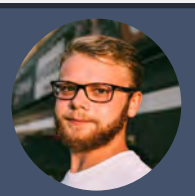
Policy in Qualys Platform

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



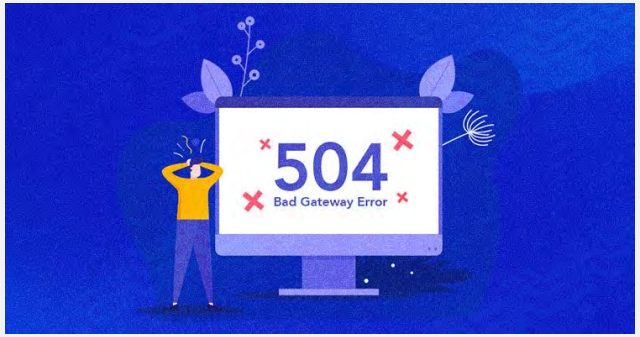
Malware Infected Endpoint

- Malware activity – TruRisk 800
- Network access blocked



Risky Endpoint

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



Qualys.

Demo Time

Qualys®

Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.

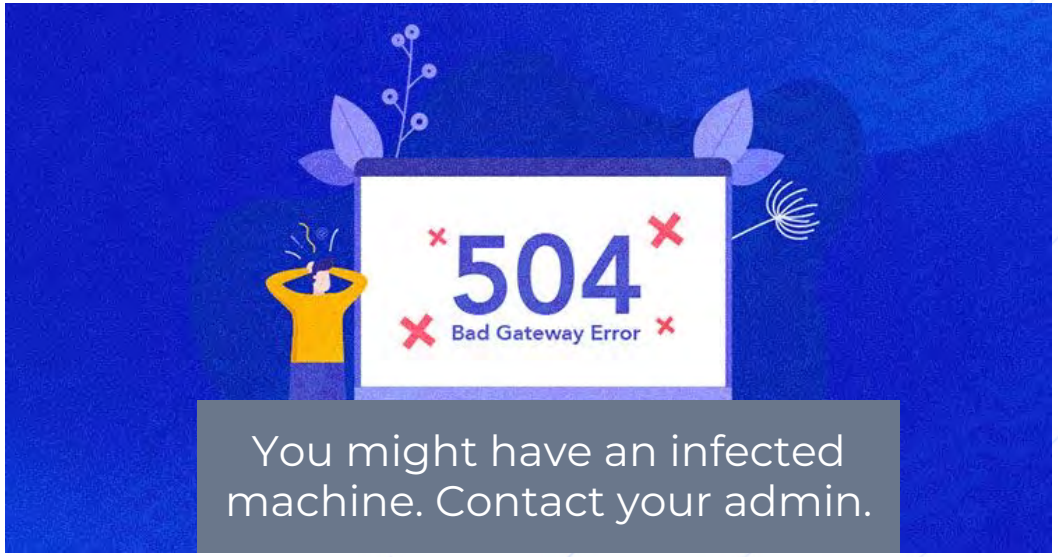
QSC22 | Get More Security

Screen 5 – TruRisk score 800

User

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.



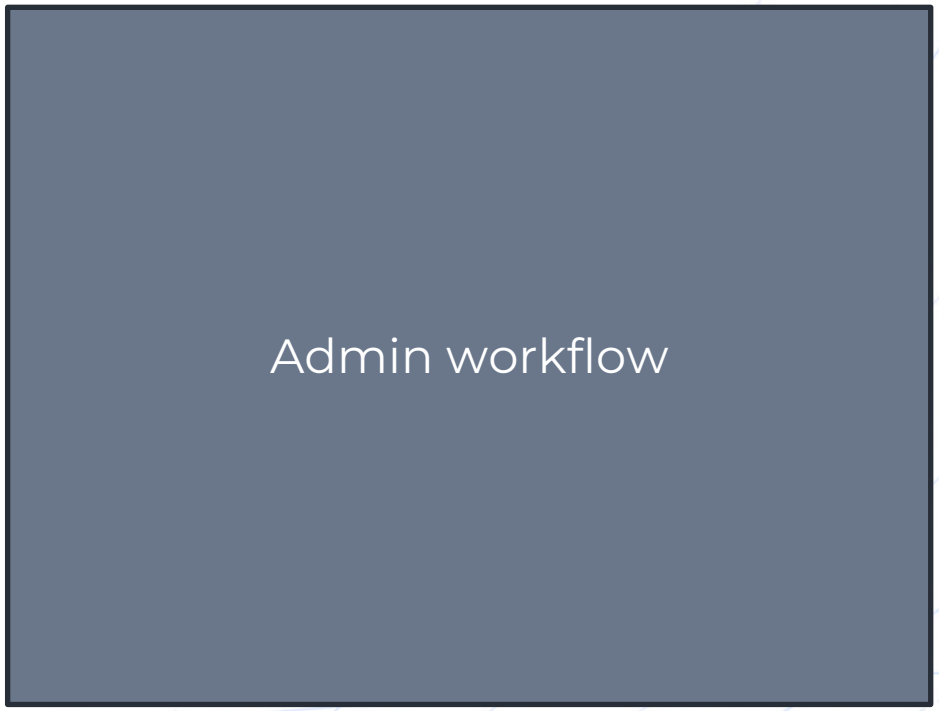
Qualys.

Screen 6 – Admin gets an alert
Can take remediation steps

Admin

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

The actions she can take are
- Contact user
- Remediate
- File Jira



Qualys.

TruRisk

Qualys.

Thank you