Active Directory Attack Surface Risk Management

Lavish Jhamb
Senior Product Manager
Compliance Solutions

Qualys®

Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.

Why do we need Active Directory (AD) Security

Active Directory Exploits on the Rise

90% Global Fortune 1000 companies use Active Directory (AD)

50% Businesses Experienced an AD Attack in last 1-2 years

40% AD attacks were successful

Source: 2021 EMA Research Report

Avenues to compromise your Active Directory

Most Common AD Security Issues

1. Too Many Administrators
2. Short and Simple Passwords
3. Leaving Inactive Accounts
4. Service accounts with elevated privileges

Image courtesy: medium.com

Challenges

How do we measure and communicate Active Directory Risk

Lack of visibility into the AD environment

Finding misconfigurations and weak policies

81% of data breaches involved weak, default or stolen passwords

Identifying Indicators of Risk

87% Riskiest threat vector: Domain accounts with too many permissions and escalated privileges

Consolidation of all datapoints to know actual risk

The Solution

Qualys.

Qualys VMDR

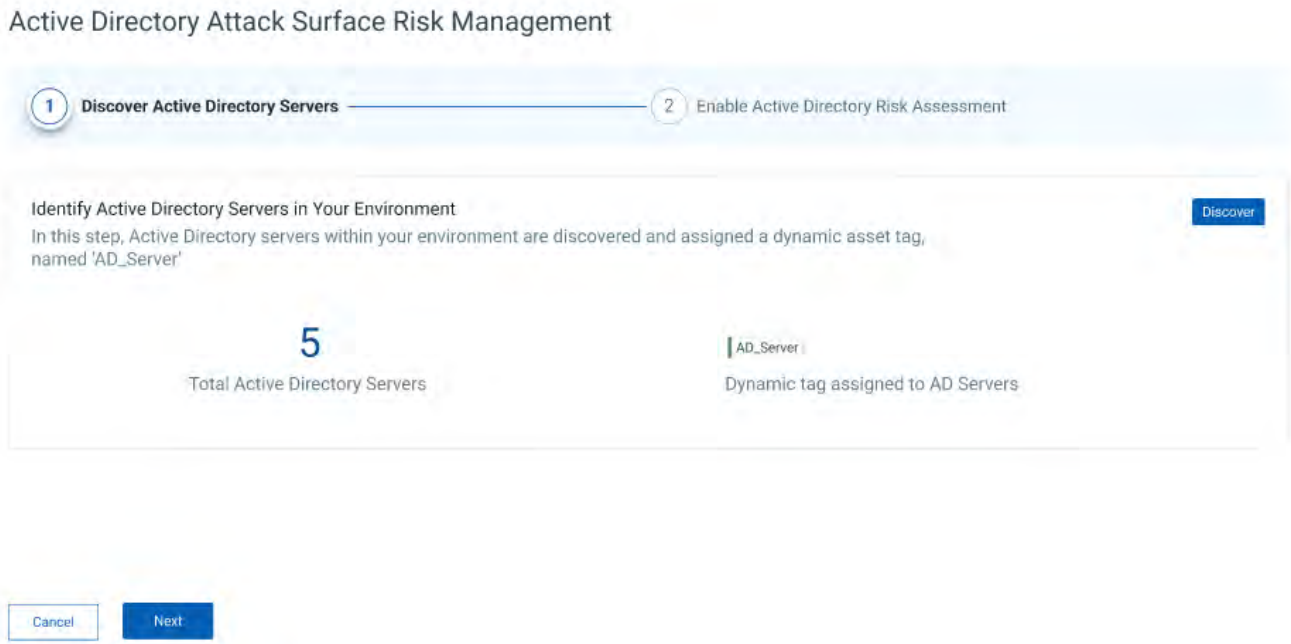
now extends to offer

AD Attack Surface Risk Management

Active Directory (AD) Servers

Step 0 – Measuring the AD Risk

1. Easily **identify** AD Servers in your inventory
2. **Classify** AD Servers exposed to Shodan
3. Find AD Servers with **EOL/EOS** software



Qualys.

Know your Active Directory Attack Surface

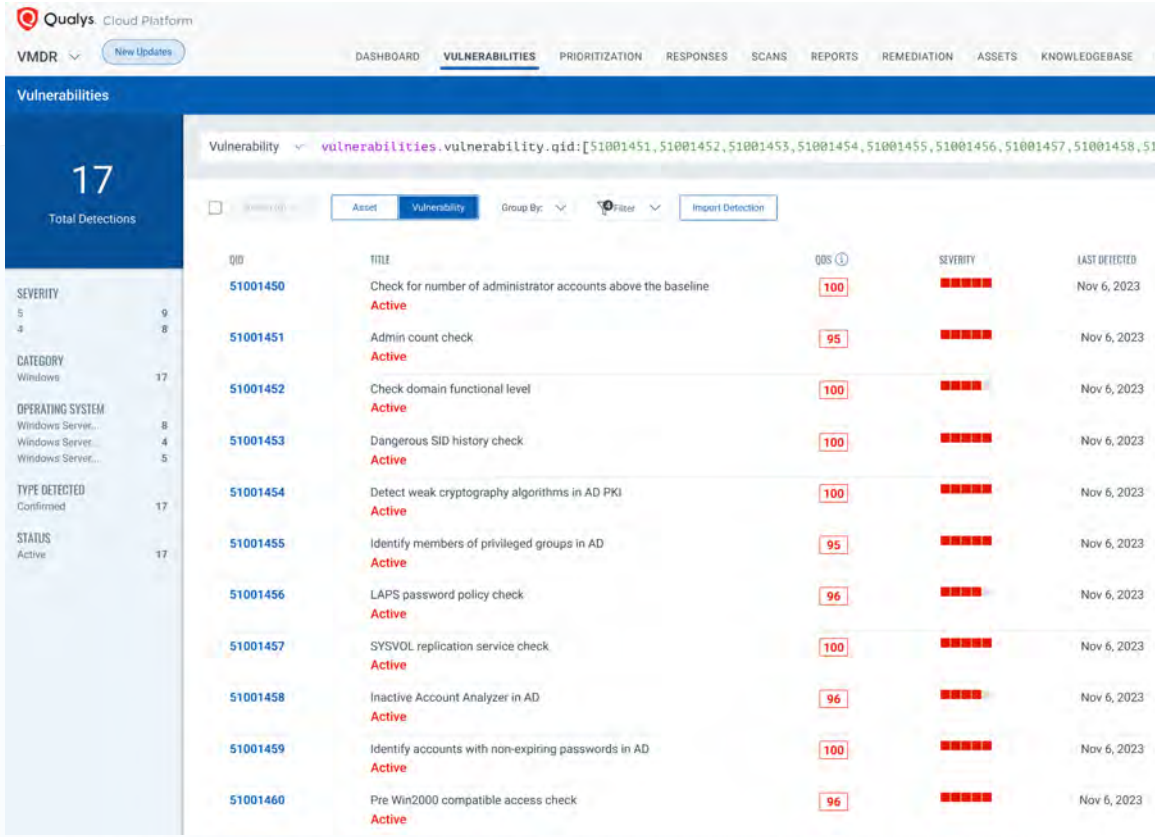
Measuring the AD Risk

1 Step 1 – Detect vulnerabilities and Indicators of Risk (IOR)

- Scan for known CVEs
- Scan for IOR using pre-defined package of scripts, imported as custom QIDs for AD Security

2 Step 2 – Detect AD Misconfigurations

Configuration assessment based on system hardening guidelines

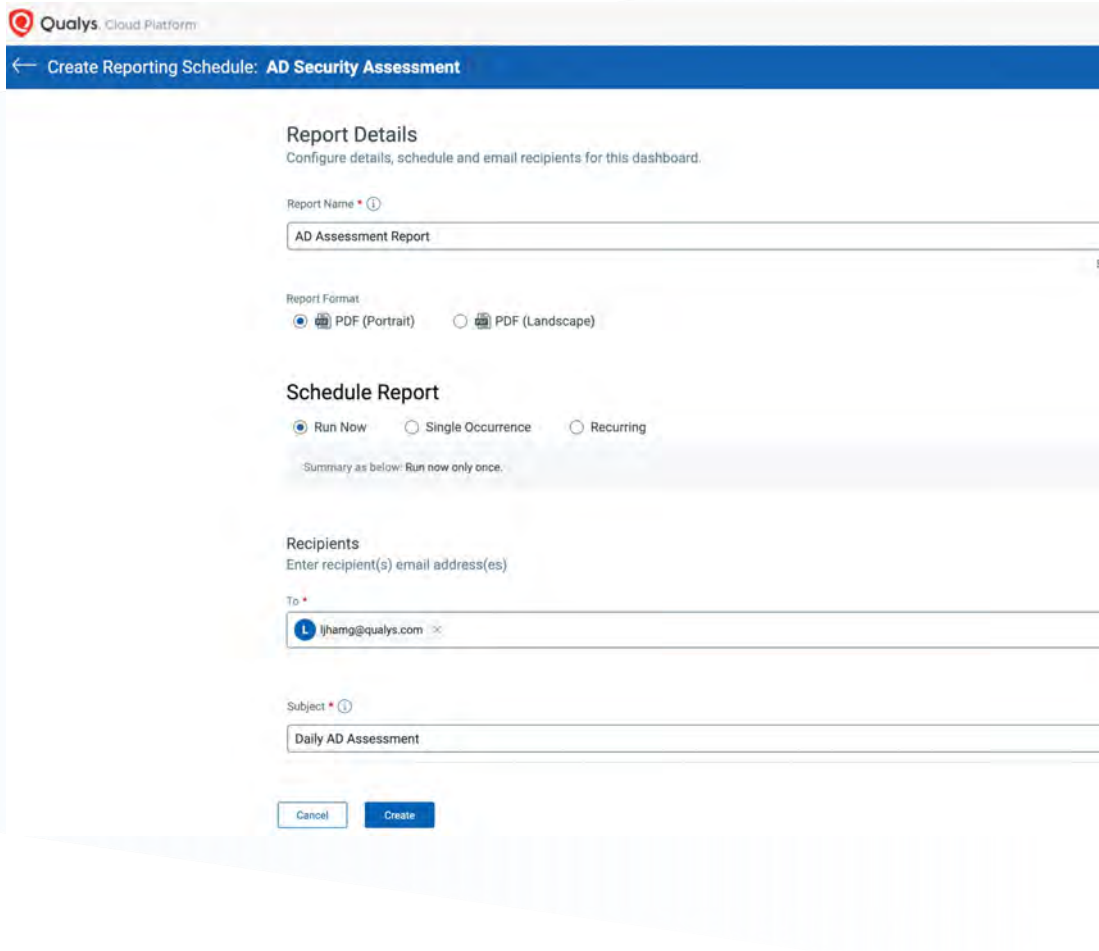


Simplified, Consolidated Risk View

Communicating the AD Risk at multiple levels

Schedule automated **reports** for communicating

1. **Executives** with TruRisk of AD Servers
2. **Security teams** with a holistic view of vulnerabilities and Indicators of risk
3. **Compliance analysts** with AD misconfiguration findings
4. **IT teams** with visibility into AD environment, exposed servers and Remediation measures to reduce risk



Qualys.

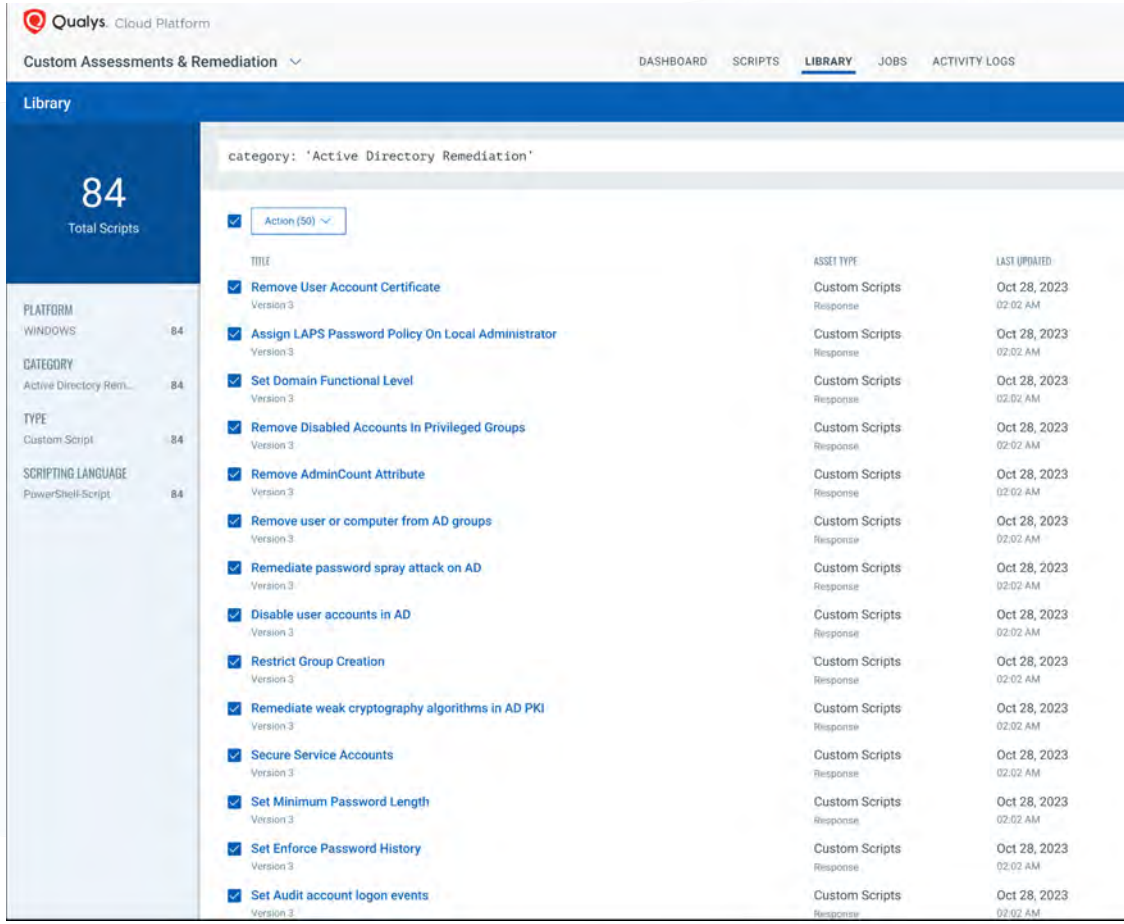
Remediate your AD Servers

Eliminating the AD Risk

1. **Prioritize and patch** AD vulnerabilities

2. **80+ AD Remediation Scripts** in Library to fix misconfigurations and Indicators of Risk (IOR)

3. Start **real time monitoring** for critical files and registry objects of AD for any changes if patch or remediation script can not be applied

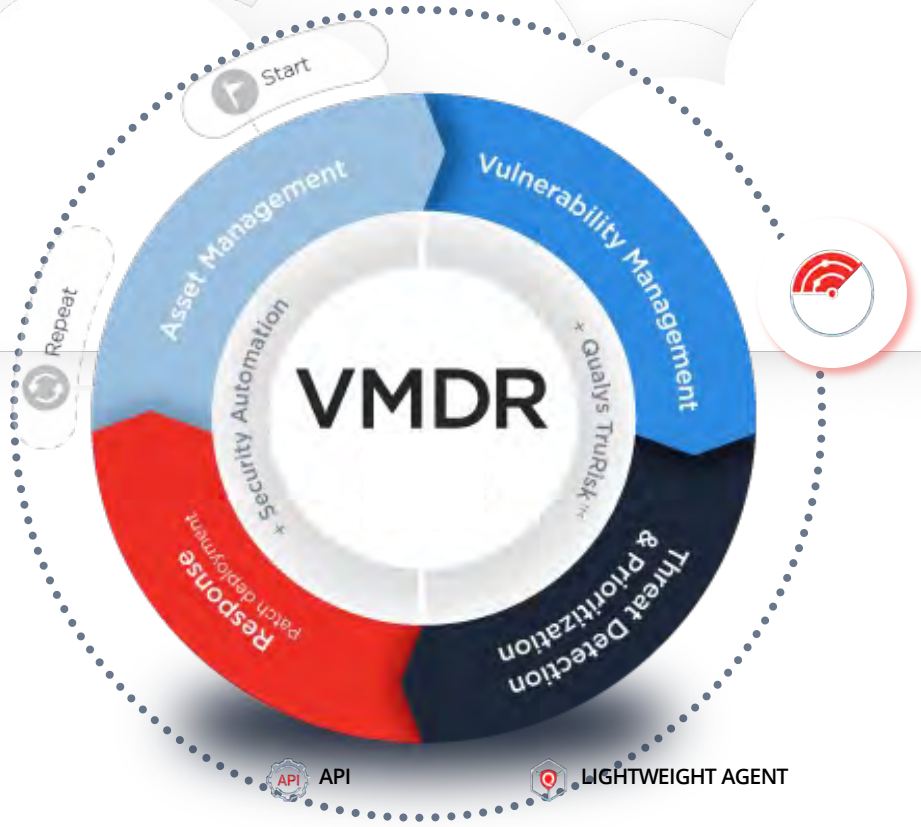


Qualys.

Demo

Qualys.

One place to manage your Active Directory Risk



Extending VMDR for Active Directory Security

Measure, communicate and eliminate your AD risk as part of Enterprise TruRisk Management from Qualys

Start AD Security Assessment (Beta) Q4 2023 / early Q1 2024

SENSORS

APPLICATIONS

OPERATING SYSTEMS

CLOUD / CONTAINERS / VMs

IT / WORKSTATIONS / SERVERS

IOT

EXTERNAL DEVICES


SC
23