



# Active Directory Attack Surface Risk Management

**Lavish Jhamb**

Senior Product Manager  
Compliance Solutions



---

# **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

# 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



# 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 **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

### Active Directory Attack Surface Risk Management

- 1 Discover Active Directory Servers
- 2 Enable Active Directory Risk Assessment

#### Identify Active Directory Servers in Your Environment

In this step, Active Directory servers within your environment are discovered and assigned a dynamic asset tag, named 'AD\_Server'

Discover

5

Total Active Directory Servers

AD\_Server

Dynamic tag assigned to AD Servers

Cancel

Next



# 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

QID	TITLE	QDS	SEVERITY	LAST DETECTED
51001450	Check for number of administrator accounts above the baseline <b>Active</b>	100	■■■■■	Nov 6, 2023
51001451	Admin count check <b>Active</b>	95	■■■■■	Nov 6, 2023
51001452	Check domain functional level <b>Active</b>	100	■■■■■	Nov 6, 2023
51001453	Dangerous SID history check <b>Active</b>	100	■■■■■	Nov 6, 2023
51001454	Detect weak cryptography algorithms in AD PKI <b>Active</b>	100	■■■■■	Nov 6, 2023
51001455	Identify members of privileged groups in AD <b>Active</b>	95	■■■■■	Nov 6, 2023
51001456	LAPS password policy check <b>Active</b>	96	■■■■■	Nov 6, 2023
51001457	SYSVOL replication service check <b>Active</b>	100	■■■■■	Nov 6, 2023
51001458	Inactive Account Analyzer in AD <b>Active</b>	96	■■■■■	Nov 6, 2023
51001459	Identify accounts with non-expiring passwords in AD <b>Active</b>	100	■■■■■	Nov 6, 2023
51001460	Pre Win2000 compatible access check <b>Active</b>	96	■■■■■	Nov 6, 2023

# 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

The screenshot shows the 'Create Reporting Schedule: AD Security Assessment' interface in the Qualys Cloud Platform. The page has a blue header with the Qualys logo and the text 'Qualys Cloud Platform'. Below the header, there is a navigation bar with a back arrow and the title 'Create Reporting Schedule: AD Security Assessment'. The main content area is divided into several sections:

- Report Details:** A section with the heading 'Report Details' and a sub-heading 'Configure details, schedule and email recipients for this dashboard.' It contains a 'Report Name' field with a help icon, containing the text 'AD Assessment Report'.
- Report Format:** A section with the heading 'Report Format' and two radio button options: 'PDF (Portrait)' (selected) and 'PDF (Landscape)'.
- Schedule Report:** A section with the heading 'Schedule Report' and three radio button options: 'Run Now' (selected), 'Single Occurrence', and 'Recurring'. Below this, it says 'Summary as below: Run now only once.'
- Recipients:** A section with the heading 'Recipients' and a sub-heading 'Enter recipient(s) email address(es)'. It contains a 'To' field with a help icon, containing the email address 'lhamg@qualys.com'.
- Subject:** A section with the heading 'Subject' and a help icon, containing the text 'Daily AD Assessment'.

At the bottom of the form, there are two buttons: 'Cancel' and 'Create'.

# 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

The screenshot displays the Qualys Cloud Platform interface, specifically the 'Library' section for 'Active Directory Remediation'. The page shows a total of 84 scripts. A list of 15 scripts is visible, each with a title, version, and last updated date. All scripts have a checked checkbox in the left margin, indicating they are selected for action.

TITLE	ASSET TYPE	LAST UPDATED
<input checked="" type="checkbox"/> Remove User Account Certificate Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Assign LAPS Password Policy On Local Administrator Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Set Domain Functional Level Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Remove Disabled Accounts In Privileged Groups Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Remove AdminCount Attribute Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Remove user or computer from AD groups Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Remediate password spray attack on AD Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Disable user accounts in AD Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Restrict Group Creation Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Remediate weak cryptography algorithms in AD PKI Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Secure Service Accounts Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Set Minimum Password Length Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Set Enforce Password History Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM
<input checked="" type="checkbox"/> Set Audit account logon events Version 3	Custom Scripts Response	Oct 28, 2023 02:02 AM

# Demo

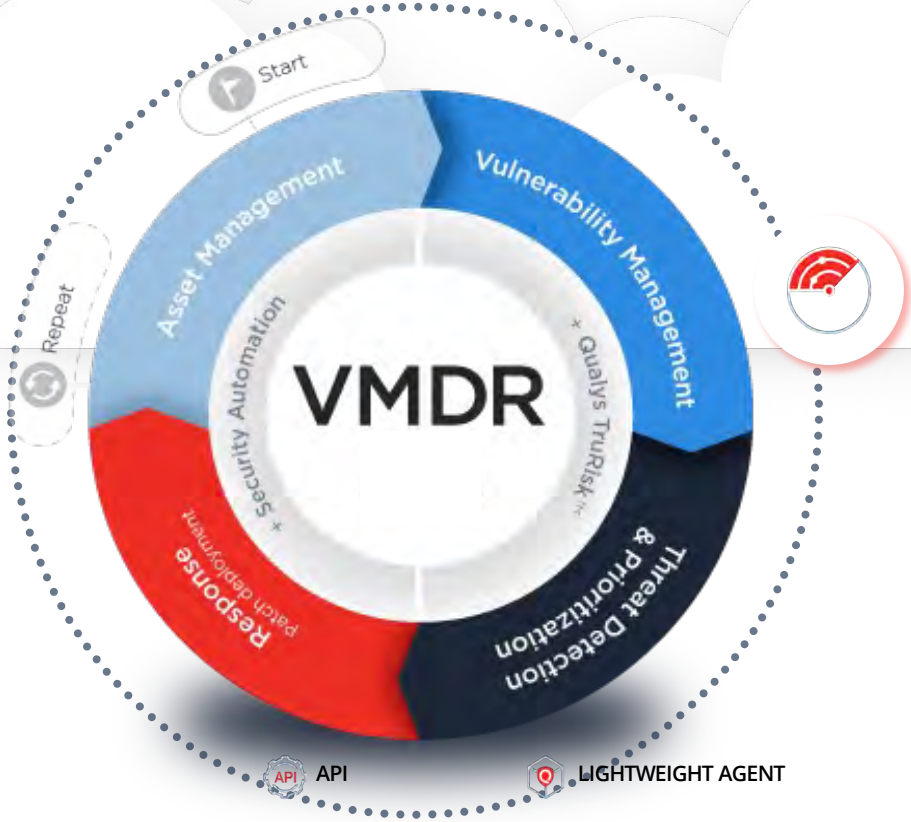


# One place to manage your Active Directory Risk

## 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



- APPLICATIONS: workday, Office 365, SAP
- OPERATING SYSTEMS: Windows, Linux, Apple
- CLOUD / CONTAINERS / VMs: aws, Google Cloud, Azure
- IT / WORKSTATIONS / SERVERS: server rack, laptop
- IOT: gear, smartphone, wireless signal
- EXTERNAL DEVICES: printer, scanner, tablet

