tenable.ad

#ADSEC

>_Harden. Detect. Respond.

tenable.ad

Active Directory (AD) has become the primary target of attackers who stealthily raid companies' most vital assets.

The industry incorrectly models advanced attacks as flows that begin outside your organization, then fly through networks and endpoints to eventually reach your data and vital assets.

Unfortunately, this ignores the ubiquitous, all-powerful overseer that orchestrates everything in your IT infrastructure: Active Directory. Which receives too little attention from IT security specialists, and far too much attention from hackers.

95% >_ Fortune 1000 is using Active Directory

100M >_ security decisions are processed each day by large directory infrastructures

85% >_ of admins acknowledge they have difficulty managing AD's security models

10% >_ of a company's annual turnover is the average cost of a remediation plan—and it keeps growing

80% >_ global enterprises audited

25 >_ had critical misconfigurations in place

95% >_ had a vulnerable AD

WHY IT MATTERS

Active Directory infrastructures are the focal point of your entire company security. User credentials, inboxes, corporate and financial data: they are all ruled by the directory infrastructure that acts as the master key holder for your company.

But AD's design makes it easily accessible and exposed to attackers seeking to reach your corporate network. It only takes one single compromise to jeopardize the entire organization.

>_ Magellan Health
April 2020

>_ Cognizant
April 2020

>_ World Health Organization
March 2020

>_ United Nations
Jan 2020

>_ Baltimore
June 2019

>_ Norsk Hydro
March 2019

>_ SingHealth
Oct 2018

WHY CURRENT DEFENSE SOLUTIONS ARE FAILING

- Most security tools focus on detecting attacks, but none improve the inner resilience of your AD architecture or actually prevent attacks in the first place.
- AD infrastructure is complex and constantly evolving. With thousands of concurrent security rules, a seemingly unimportant misconfiguration can cascade into several major vulnerabilities in a matter of minutes.

TENABLE.AD REINVENTS AD SECURITY

Tenable.ad hardens your directory infrastructure, enriches your SOC capabilities with AD threat detection, and empowers your incident response and threat hunter teams to investigate AD-related threats. All with no agents and no privileges.

FIND & FIX EXISTING WEAKNESSES

>_ Immediately discover, map, and score existing weaknesses

>_ Follow our step-by-step remediation tactics and prevent attacks

UNCOVER ATTACK PATHWAYS

>_ Instantly detect new weaknesses and misconfigurations

>_ Break attack pathways and keep your threat exposure in check

DETECT ATTACKS IN REAL TIME

>_ Get real-time alerts and actionable remediation plans on AD attacks

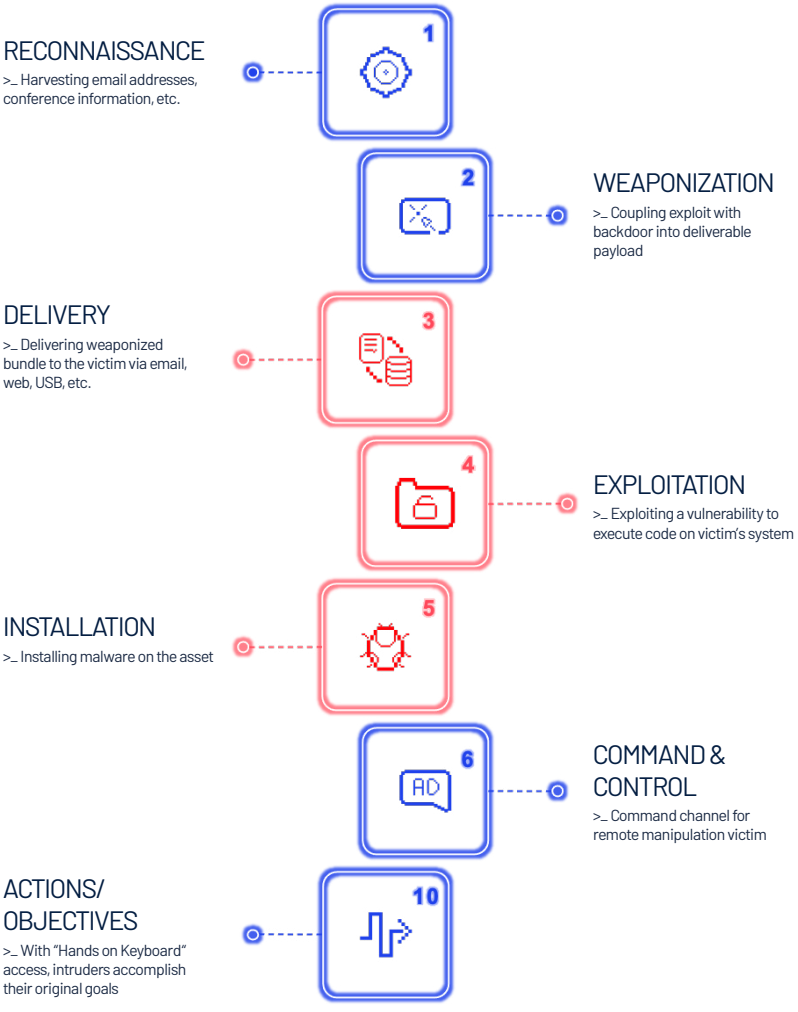
>_ Visualize notifications and trigger responses in your SIEM / SOAR / SOC

INVESTIGATE INCIDENTS & THREATS

>_ Drill down into the most comprehensive security tracker for AD

>_ Search and correlate AD changes at object and attribute levels

PREVENTING THE APT KILL CHAIN WITH TENABLE.AD



DELIVERY

Prevent - Tenable.ad identifies exploitable delivery methods and notifies SOC teams in real time for preemptive fixing.

Detect - Tenable.ad detects ongoing deliveries in real time and allows for immediate mitigation and remediation.

Respond - Tenable.ad's curated alerts and metrics empower IR teams to uncover root causes and to guide post-exposure responses and hardening processes.

EXPLOITATION & INSTALLATION

Prevent - Whether for misconfigurations or software vulnerabilities, Tenable.ad guides SOC teams through the process of hardening their AD and preventing exploitations.

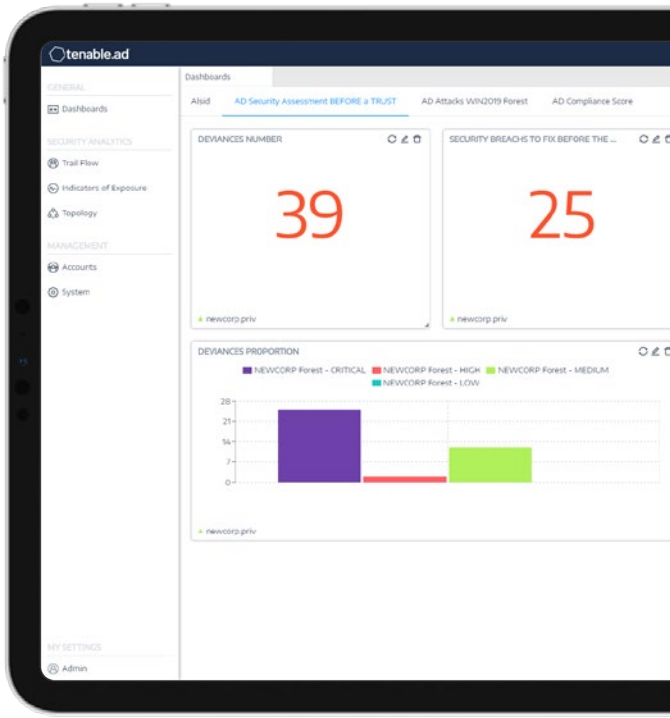
Detect - With the largest detection surface on the market, Tenable.ad spots ongoing exploitations and triggers remediations at machine-speed.

Respond - Tenable.ad's detailed recommendations walk AD admins through the (otherwise complex) process of managing compromised objects and non-compliant servers, and toward hardening their infrastructure as a whole.

tenable.ad

INTEGRATED PLATFORM

- Unified, dashboard-oriented admin console
- Centralized platform to manage multiple Active Directory infrastructures simultaneously
- Strong authentication mechanism thanks to MFA and isolated authentication database
- Corporate, process-oriented outputs with built-in Excel to JSON export features



CUSTOMERS TRUST TENABLE.AD

"Tenable.ad's integration was not only accomplished in a day, but it also provided efficient security monitoring on atomic infrastructures without any impact on the workload of security teams."

Thierry Augier
Deputy CIO & CISO, Lagardère

"Tenable.ad's solution freed us from Active Directory security concerns so that we could focus on new business incorporation."

Dominique Tessaro
CIO, VINCI Energies

"Tenable.ad is the answer to the two questions every CISO should be constantly asking – Are my domains adequately secured? And how can I independently prove it?"

Jamie Rossato
VP Information Technology & Cyber Security, Orica

ABOUT TENABLE.AD

Tenable.ad is specialized in defending the common denominator of most attacks: Active Directory (AD) infrastructures. The Tenable.ad solution provides users with step-by-step, custom recommendations for hardening their AD, a real-time attack detection engine, and tailored investigation and remediation capabilities. All with no agents and no privileges.

Today, Tenable.ad protects more than 6 million users worldwide against advanced attacks.

Contact us: tenable.com/products/tenable-ad

6100 Merriweather Drive
12th Floor
Columbia, MD 21044

North America +1 (410) 872-0555

www.tenable.com

primo-infection is a lost battle

Lateral movement is the new front