VECTRA AI

2026 STATE OF THREAT EXPOSURE MANAGEMENT REPORT

The Modern Exposure Reality

Exposure management is no longer a simple vulnerability management problem. It is a problem of continuously understanding what is operating, communicating, and creating exposed attack paths across dynamic environments.

Vectra AI analyzed customer environments to understand asset change, unmanaged devices, AI-agent presence, and attacker-relevant exposure conditions.

Observation #1 — Asset change was universal across observed environments

100%

of analyzed environments experienced newly observed hosts in just 14 days.

Modern enterprise environments are continuously changing faster than static inventories can accurately track.

14-DAY ASSET CHANGE OBSERVATION

249 Median newly observed hosts per environment	**90%** Environments with new host roles	**83%** Environments with new device types
7 Median new device types per environment	**44** 90th percentile, new device types	**399** Maximum new device types observed

WHAT THIS MEANS

Environments are continuously introducing *new* assets and device types, creating persistent uncertainty around ownership, *role*, management status, coverage, segmentation, communication behavior, and whether new assets create paths attackers could use.

Observation #2 — EDR visibility does not extend to the entire environment

>30%

of devices are unmanaged on average.

These assets can operate outside agent-based visibility.

WHAT THIS MEANS

Organizations cannot assume endpoint tools provide complete visibility. Many assets remain outside agent-based coverage, creating blind spots that leave potential attack paths unmonitored.

Observation #3 — AI-agents and non-human actors are already material

96:1

maximum observed AI-agent to device ratio.

In some environments, AI agents and non-human actors already outnumber traditional devices at a massive scale.

90-DAY AI-AGENT OBSERVATION

1.17:1 Median agent-to-device ratio	**0.15:1** Minimum agent-to-device ratio

WHAT THIS MEANS

Security teams need visibility beyond users and devices. AI agents, service accounts, automation pipelines, APIs, and other non-human identities are now active operational actors that create new access paths, communication flows, and potential attack paths.

Observation #4 — Attacker-relevant exposure conditions remain widespread

98%

of analyzed environments had at least one attacker-relevant exposure condition present.

Legacy protocols, weak cryptography, credential exposure, and risky services remain widespread across modern environments.

MOST COMMONLY OBSERVED EXPOSURE CONDITIONS · PAST 30 DAYS

Deprecated TLS client	96%
Expired certificates	91%
NetBIOS	86%
Plaintext passwords	85%
Deprecated TLS server	82%
Certificates expiring soon	82%
Credential files in SMB	81%
FTP	73%
SMBv1 server	61%
Telnet	57%
SMBv1 client	55%
Exposed RDP	46%

These conditions can help attackers gain access, move laterally, steal credentials, weaken encryption, or expand control once inside an environment.

WHAT THIS MEANS

Attacker-relevant exposure is widespread, but not all conditions carry equal risk. Security teams need context to understand which conditions are merely present, which ones create exploitable attack paths, and which ones should be remediated first.

WHERE EXPOSURE MANAGEMENT GOES NEXT

The future of security exposure management

Modern environments are dynamic, interconnected, and expanding faster than traditional security models can track. Exposure management must become continuous, contextual, and operational so that teams can identify and reduce exposed attack paths before attackers use them.

01
Continuous Visibility
Understand what is operating, how it's communicating, and what has changed.

02
Context + Prioritization
Focus on exposure conditions that create or extend exposed attack paths.

03
Action + Remediation
Address issues across assets, identities, and environments with operational context.

04
Validate + Reduce Risk
Continuously validate that exposure has been reduced and risk is meaningfully lowered.

Read the full report

Source: Vectra AI's "2026 State of Threat Exposure Management Report"