

## IDENTITY SECURITY AND XDR

# How XDR Connects the Signals Behind Identity Attacks

Stolen credentials can make malicious activity look like normal user or application access. Extended Detection and Response (XDR) brings those signals together, helping teams trace the attack and coordinate containment.

## The Identity Attack Surface Is Growing

**32%**

is the increase in identity-based attacks Microsoft reported during the first half of 2025

**75%**

of organizations report growth in identities such as service accounts and API keys<sup>1</sup>

**73%**

of organizations use agentic AI or other automations that require credentials<sup>2</sup>

Employees and administrators now sit alongside applications, workloads, service accounts, API keys, and AI agents. Some non-human identities remain active around the clock or hold broad permissions, increasing the potential impact of exposed credentials.

## One Identity Attack Can Leave Signals Across the Environment

With the right integrations in place, XDR links activity involving the same account, device, application, or workload and reconstructs the sequence for investigation.

| STAGE | WHAT HAPPENS                                                                                                | COMMONLY RECORDED IN  |
|-------|-------------------------------------------------------------------------------------------------------------|-----------------------|
| 1     | <b>INITIAL ACCESS</b><br>An attacker signs in with a stolen credential, such as a password or session token | Identity Platform     |
| 2     | <b>EMAIL CHANGE</b><br>The attacker changes email rules within the compromised account                      | Email Security        |
| 3     | <b>PERMISSION CHANGE</b><br>The account grants a new application permission                                 | Cloud Application     |
| 4     | <b>DATA ACCESS</b><br>The account downloads an unusual volume of data                                       | SaaS or Cloud Service |
| 5     | <b>MOVEMENT</b><br>The attacker uses the account to reach another device or business system                 | Endpoint or Network   |

## Containment Must Follow Detection Quickly

The time between detection and containment gives attackers more opportunity to gain privileges or reach sensitive information.

**68%**

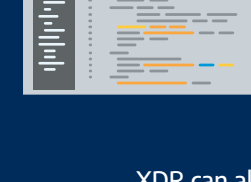
**55%**

of organizations detect an identity attack within 24 hours<sup>3</sup>

of organizations contain the attack within that same 24-hour window<sup>3</sup>

## XDR Connects Detection with Coordinated Response

Once a team confirms an incident, XDR can coordinate actions across connected tools. The response should reflect the identity involved.



### Compromised Employee Identity

- Reset the account
- Revoke active sessions



### Compromised Application or Service Identity

- Disable access
- Replace exposed credentials
- Investigate every system it contacted

XDR can also isolate affected devices, block malicious messages, and restrict cloud access. Teams can require analyst approval before any action that may interrupt legitimate work.

## XDR Supports Existing Identity Controls

Access controls, multifactor authentication, privileged account protection, and regular access reviews reduce the likelihood of identity misuse. XDR helps detect and contain attacks when credentials are stolen, preventive controls are bypassed, or legitimate access is abused.

**85%**

of organizations have deployed identity threat detection and response tools<sup>4</sup>

**55%**

of organizations experienced an identity-related breach in the previous 12 months<sup>5</sup>

## Six Questions to Ask When Comparing XDR Platforms

**1**

### Which Identity Systems Can It Monitor?

Confirm support for the directories, identity providers, SaaS applications, and cloud environments you use.

**2**

### How Much Visibility Does Each Integration Provide?

Check which events each connector can collect and which response actions the platform can perform.

**3**

### Can It Monitor Non-human Identities?

Look for coverage of service accounts, applications, API credentials, workloads, and AI agents.

**4**

### How Are Response Actions Controlled?

Determine which actions can run automatically, which require approval, and how the platform records them.

**5**

### What Will Implementation Require?

Consider data volumes, retention and privacy requirements, staff training, and ongoing maintenance.

**6**

### What Is the Complete Cost?

Account for licenses, connectors, data storage, implementation, and staffing, including where existing tools will remain necessary.

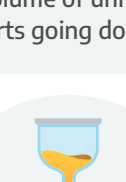
## Track XDR's Impact on Your Security Operations

These four indicators show whether the platform improves coverage and helps teams respond faster.



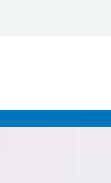
### Coverage Across Critical Systems

Are the right identity sources connected?



### Unnecessary Alerts Reaching Analysts

Is the volume of unnecessary alerts going down?



### Investigation Time

Is the team resolving incidents faster?



### Containment Time

Is containment keeping pace with detection?

## Bring Identity Signals Into the Broader Security Strategy

Connection's Security Technology Integration services can help organizations connect and improve existing investments across identity and access management, [endpoint security](#), advanced threat protection, and SIEM and log management.

## Explore Our Solutions and Services

[Security Technology Integration](#)

[Extended Detection and Response \(XDR\)](#)

Contact a Connection Account Manager to learn more.

**1.800.998.0019**