EDR vs. ITDR vs. MDR vs. XDR

Detection response tools can be acronym overload. Think of EDR as the "core" offering, with various additional layers adding their own benefits.

EDR
Endpoint Detection & Response

Coverage
Endpoint devices like desktops, laptops, servers

Handles
Endpoint threats like malware, ransomware

Ownership
Typically internal IT

Pros
Baseline need
Lowest cost
Easy to scale

Cons
Typically can't remediate
Can overload small team
Narrow scope

You need identity protection for users...

ITDR
Identity Threat Detection & Response

Coverage
User activity and access management

Handles
Identity threats like compromised credentials

Ownership
Typically internal IT

Pros
Critical need
Adds additional layer

Cons
Increased cost
Narrowest scope

If remediation overwhelms your team...

MDR
Managed Detection & Response

Coverage
Endpoint devices like desktops, laptops, servers

Handles
Endpoint threats like malware, ransomware

Ownership
Managed by third party

Pros
Offload management
Enhanced governance

Cons
Increased cost
Still limited EDR scope

If you need unified visibility and reports...

XDR
Extended Detection & Response

Coverage
Cross-layer security ecosystem: endpoints, network, cloud, identities

Handles
Threat detection, investigation, and response across ecosystem

Ownership
Typically managed by third party, often a SOC

Pros
Holistic approach
Correlated reporting

Cons
Priciest option
Overkill for some orgs

Integris.

integrisit.com