CYBERSECURITY INSIGHTS

Is EDR Alone Enough? Why Do We Need XDR?



EDR · XDR · Defense in Depth

TODAY'S AGENDA

Four questions in ten minutes

01
What does EDR do?

02
Is EDR alone enough?

03
Why do we need XDR?

04
How does it all fit together?

01 · ENDPOINT DETECTION AND RESPONSE

What EDR does

A lightweight agent on each laptop, desktop, server and mobile device sends security telemetry to a central console.

Monitor

Processes, files, network connections and system events

Detect

Suspicious behavior and malware execution

Respond

Isolate devices, stop processes, investigate

DEPLOYMENT MODELS

On-premises or cloud-based?

On-premises EDR

Servers in your own office or data center. Remote devices usually need a VPN.

+ Direct control over data and infrastructure

− You run hardware, patching and backups

Cloud-based EDR

Platform hosted by the vendor. Devices connect securely over the internet.

+ Less overhead, easier scaling

− Subscriptions, data residency, compliance

02 · IS EDR ALONE ENOUGH?

No.

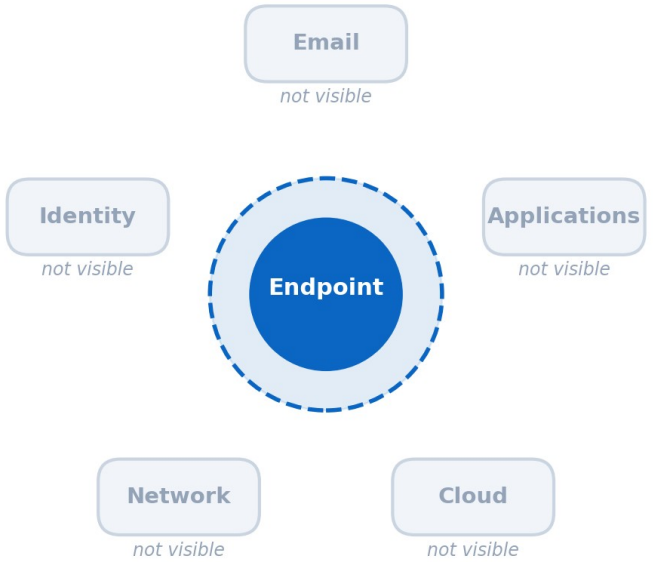
EDR sees the endpoint. Attacks move across email, identities, networks and the cloud.

What a security team cannot see, it cannot defend.

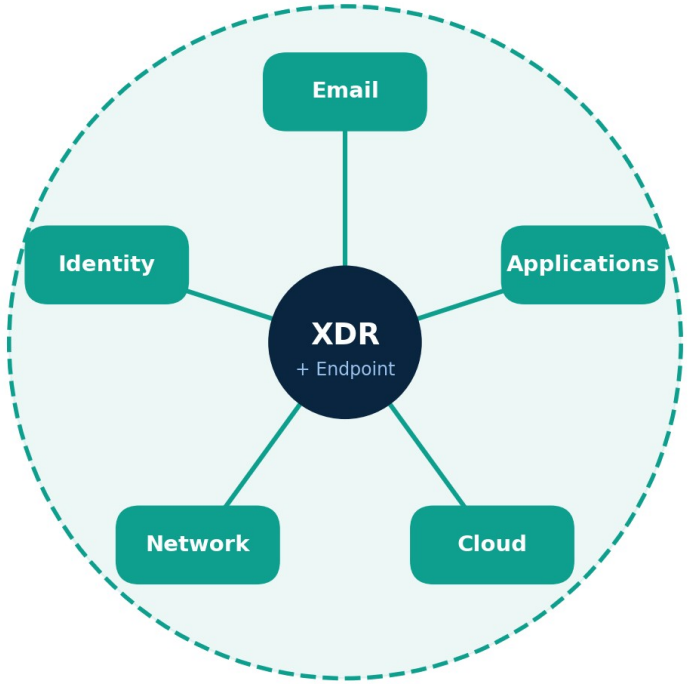
THE VISIBILITY GAP

EDR sees one piece. XDR connects the story.

EDR: Endpoint visibility only

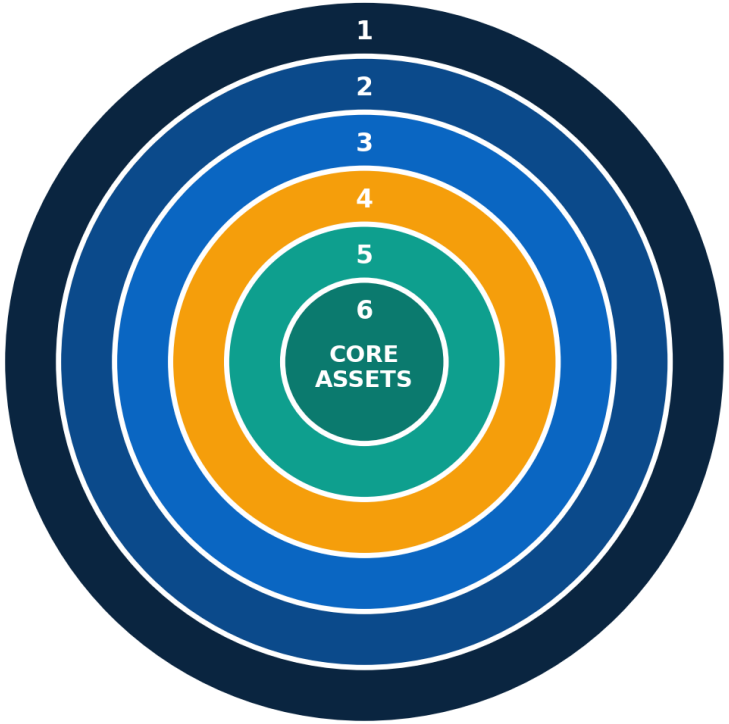


XDR: Correlated, cross-domain visibility



DEFENSE IN DEPTH

Security works in layers, like an onion



1 **Layer 1: Policies & People**
Policies, training, awareness

2 **Layer 2: Perimeter Security**
Firewalls, IDS/IPS, gateways

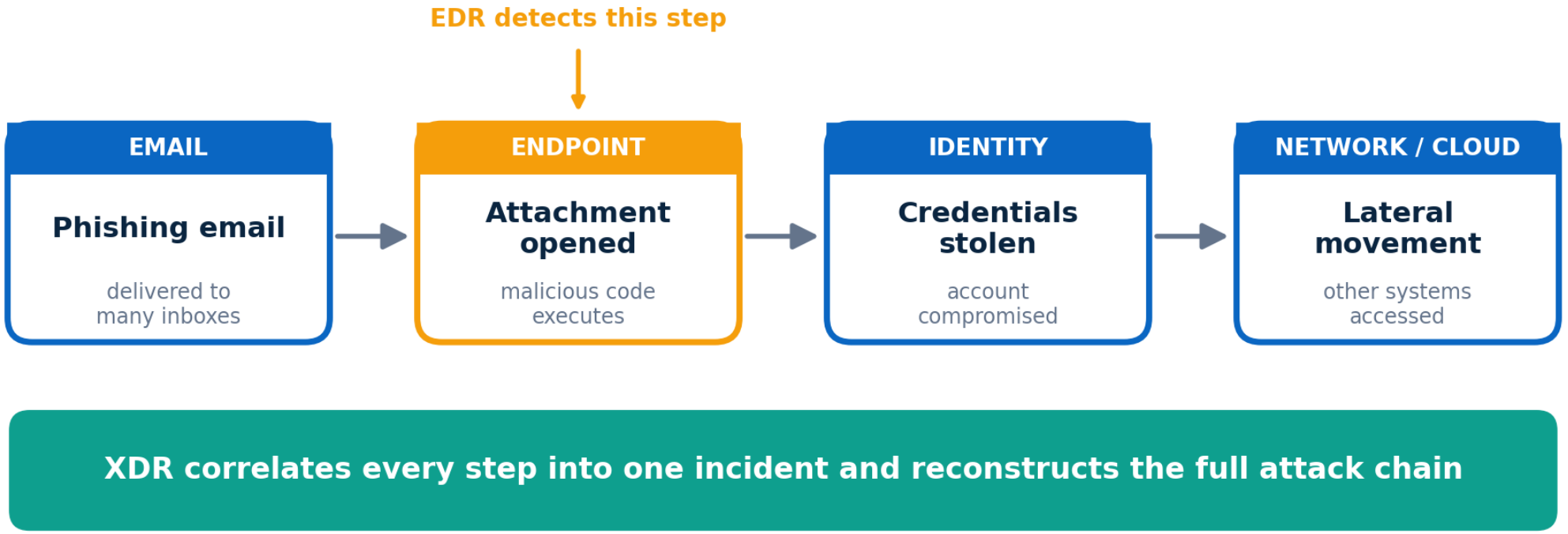
3 **Layer 3: Internal Network**
Segmentation, NAC, Zero Trust

4 **Layer 4: Endpoint Security**
EDR's core role — EDR

5 **Layer 5: Application Security**
Secure coding, testing, WAF

6 **Layer 6: Data Security**
Encryption, DLP, FIM, backups

A phishing attack, seen two ways



WHAT XDR ADDS

Four key benefits of XDR

Cross-layer visibility

One view across endpoint, email, identity, network and cloud

Event correlation

Related alerts become one incident, not many

Automated response

Isolate devices or disable accounts faster, if tuned carefully

Less complexity

Fewer consoles to switch between during an incident

TRADE-OFFS

XDR has challenges too

Vendor lock-in

Easy inside one ecosystem, harder to leave. Check portability and exit terms.

Integration limits

Third-party tools may share limited data. Verify before you buy.

Cost and licensing

Tiers, data limits and add-ons. Judge total cost of ownership.

A BURMESE PROVERB

“A snail that tries to imitate a frog’s leap may end up stranded in the pond.”

Don’t follow security trends blindly. Decide based on your own risks, priorities and resources.

04 · BRINGING IT TOGETHER

Real security needs all three

Technology

EDR, XDR and layered controls

+

People

Skilled engineers and analysts

+

Strategy

Defense in Depth, based on risk

Cybersecurity can't be bought off the shelf. Neither EDR nor XDR is a complete solution on its own.

Thank you

Questions and discussion

[Presenter name] · [LinkedIn / contact]