



XDR in Action: The Blueprint for Holistic Visibility & Automated Response





MEET OUR PRESENTERS



Ben Wilcox

Managing Director of Cybersecurity & Compliance
Chief Technology Officer

bwilcox@proarch.com
[Linkedin.com/in/ben-wilcox/](https://www.linkedin.com/in/ben-wilcox/)



Michael Wurz

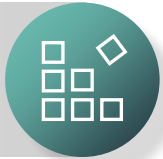
VP of Cybersecurity Solutions

mwurz@proarch.com
[Linkedin.com/in/mwurz/](https://www.linkedin.com/in/mwurz/)

Defending against cyberattacks has never been harder...



Growing frequency, speed, and targeting of threats



Security gaps from fragmented tools



Alert fatigue and SOC burnout

...and the security team's work is endless

How do I investigate more effectively?



How do I prioritize?

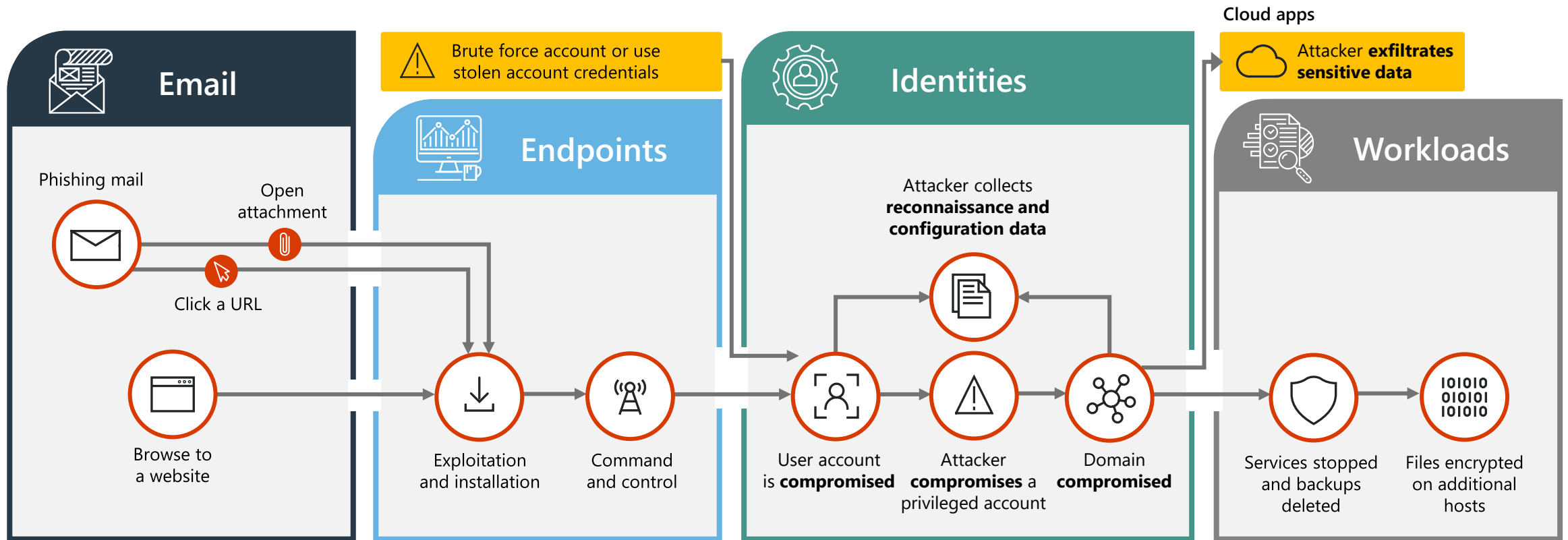


How do I prevent and stop attacks quickly?



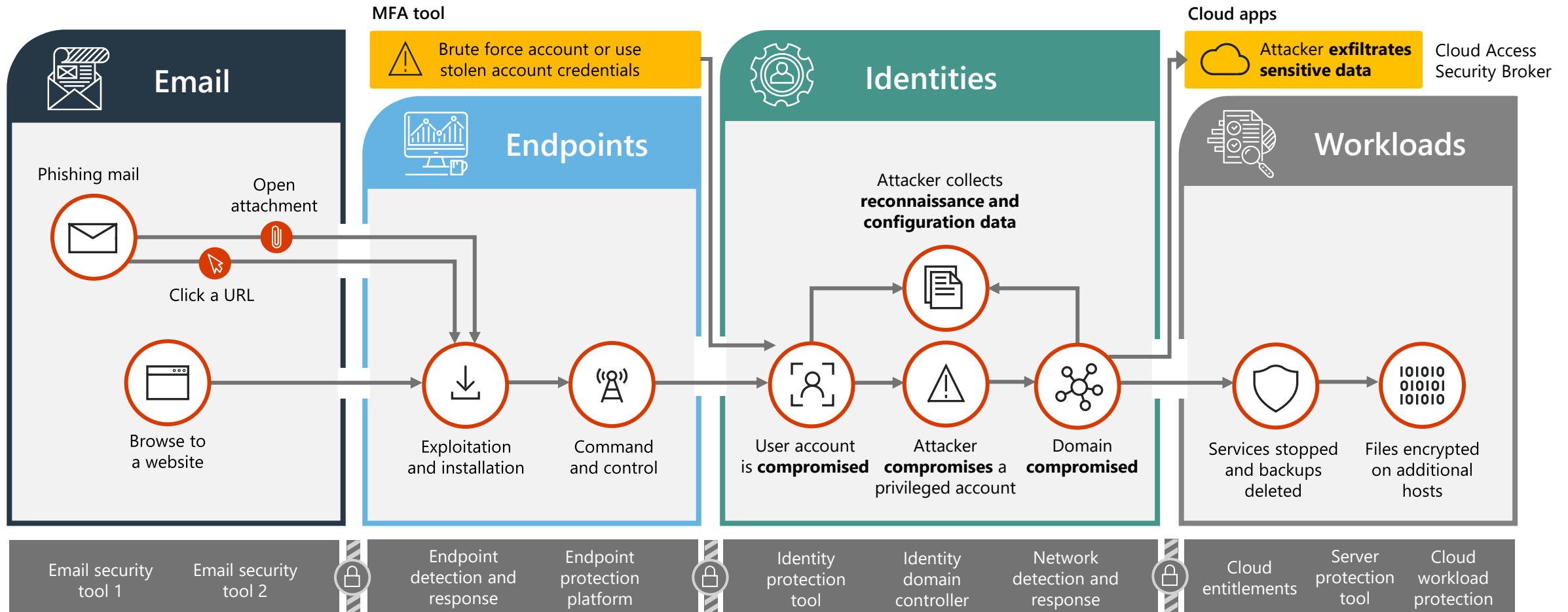
Why is defense so difficult today?

Typical human-operated ransomware campaign.



Siloed security leads to gaps in coverage.

Multiple tools providing unequal protection across the attack kill chain.



What is XDR?

WHAT DO YOU THINK!

XDR provides a **holistic view of security activity** by correlating data from various sources.

XDR combines threat detection, investigation, and response **across security domains**, including endpoints, networks, and cloud environments.

XDR Criteria



Centralized data access



Integrates diverse data types and alert sources



Automatic data and alert correlation



Automatic investigation and response



AI and ML

XDR Approach to Defend Against Threats



Identify



Protect and Prevent



Detect and Respond

Email & Collaboration

Exchange Online
Teams
SharePoint
OneDrive
Google Workspace
Google Drive

Endpoints

Servers
Workstations
Mobile Devices
IoT

Identities

On-premises
Cloud
Hybrid

Cloud Apps

SaaS Apps
Custom Apps
Microsoft 365
Apps

Cloud Infrastructure

Azure
AWS
Google Cloud

SIEM/Custom Sources

Multi-cloud
Hybrid
On-prem
Databases
APIs, AI, ML
Logs
OT/ICS



Unified entities
and inventories

Automatically
disrupt attacks

Cross-product
detection engines

Unified threat
intelligence and
analytics

Security Team
support across
domains

XDR





DEMO 

Microsoft Defender XDR

Microsoft Defender XDR

Cross-domain Security



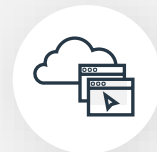
Hybrid identities



Endpoints and IoT



Email and collaboration



SaaS apps



Data



Cloud workloads

Prevent



Reduce attack surface with threat-based configuration recommendations and built-in vulnerability management

Protect



Automatically contain and remediate compromised assets

Detect and respond



Use incidents to respond to cross-workload threats from a single portal



Speed up response with an experience designed for SOC efficiency

Extend




Unified APIs and connectors

XDR Blueprint


DATA SOURCES

ENDPOINT	Servers Workstations Mobile Devices
IDENTITY	On-premises Cloud Hybrid
COMMUNICATION	Email Chat Storage
CLOUD INFRASTRUCTURE	Microsoft Azure Amazon Web Services Google Cloud Platform
CLOUD APPS	Microsoft 365 Apps Third-party Cloud Apps Firewall Traffic
SIEM LOG SOURCES	Endpoints Network Devices Custom Integrations
IoT/OT	OT/ICS General-Purpose IoT Corporate IoT Network

THREAT DETECTION SOURCES

MICROSOFT SIEM 
Microsoft Sentinel



MICROSOFT DEFENDER XDR 
Defender for Endpoint
Defender for Identity
Entra ID Identity Protection
Defender for Office 365
Defender for Cloud
Defender for Cloud Apps
Defender for IOT



RESPONSE, MAINTENANCE, & IMPROVEMENTS

DASHBOARD	Centralized Alert Insights Dashboards & Reporting
SOAR	Event Automation & Orchestration False Positive Tuning Custom Automation Development
THREAT INTELLIGENCE	Threat Intel Briefings Alert Enrichment Client Risk Monitoring
24x7 SECURITY OPERATIONS CENTER	Threat Containment & Remediation Threat Detection Engineering Threat Hunting Incident Response Solution Management
SECURITY STRATEGY	Implement recommendations Keep improving maturity Align with compliance
CICD	Centralized Resource Management Immediate Detection Rule Creation

Next Steps

Address Security Gaps: Focus on improving your security posture across security domains.

Evaluate XDR Vendors: Look for vendors that align with your vision and integrate with your current solutions. Consider the benefits of Microsoft Defender XDR.

Implement XDR: Start planning how to integrate XDR into your existing security infrastructure. Focus on unifying disparate solutions to gain a holistic view of activity.

Consider partnering with ProArch to maximize the benefits of XDR in your organization.

Hunt for Threats

Scan the QR code or email letstalk@proarch.com for 3 complimentary Microsoft 365 Defender threat hunting packages.



Questions?



THANK YOU FOR JOINING US | PROARCH.COM

Ben Wilcox

bwilcox@proarch.com

[Linkedin.com/in/ben-wilcox/](https://www.linkedin.com/in/ben-wilcox/)

Michael Wurz

mwurz@proarch.com

[Linkedin.com/in/mwurz/](https://www.linkedin.com/in/mwurz/)