BCNET CONNECT

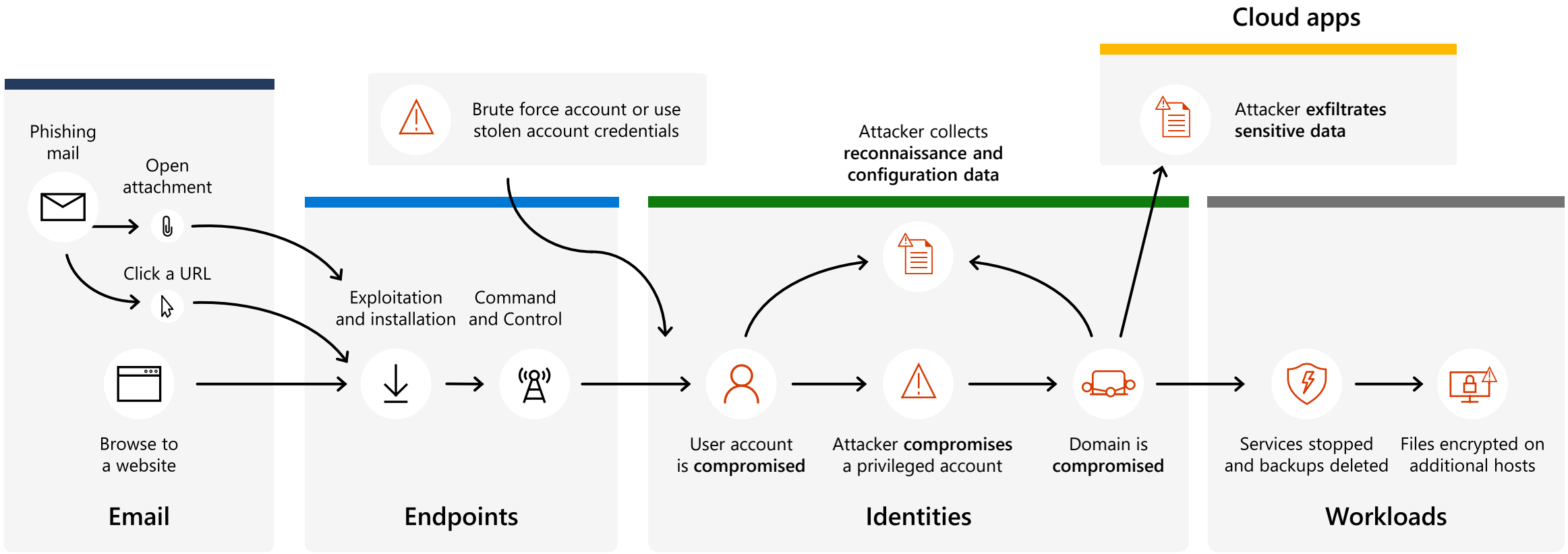
HIGHER ED & RESEARCH TECH SUMMIT

Reduce Complexity & Increase Security with XDR + SIEM

Why is defense so difficult?

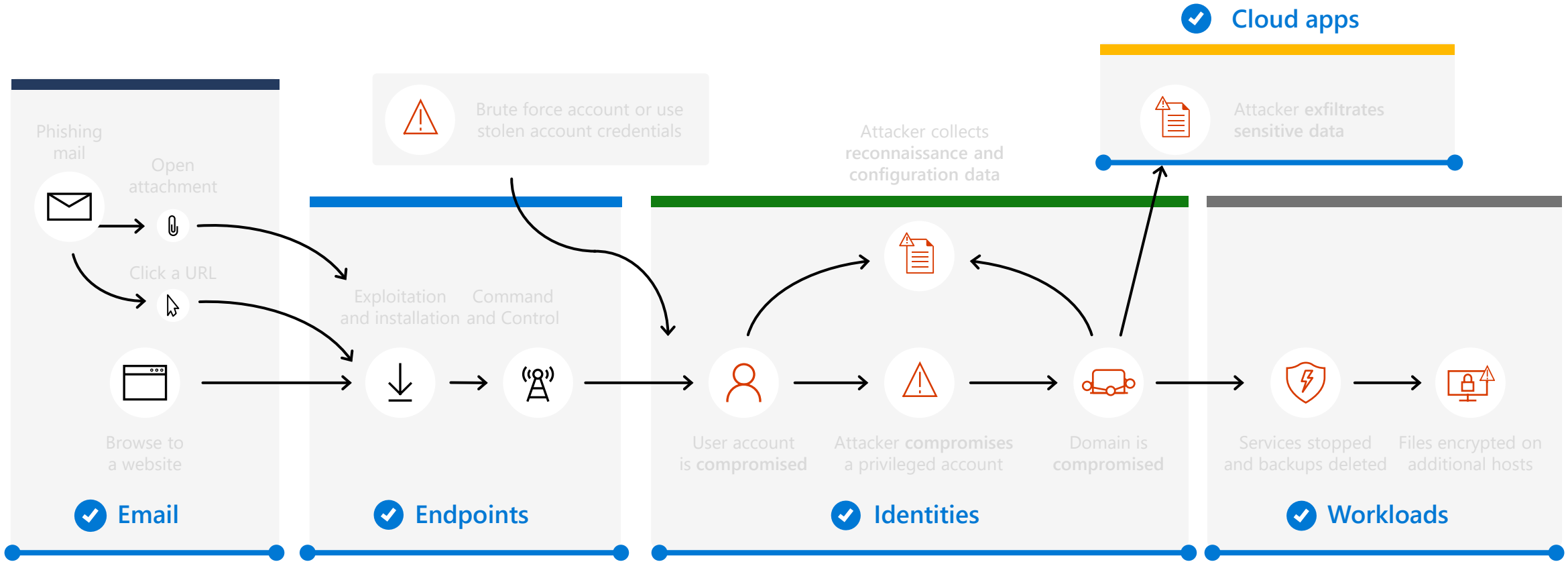
Attacks are crossing modalities

Typical human-operated ransomware campaign



Protection across the entire kill chain

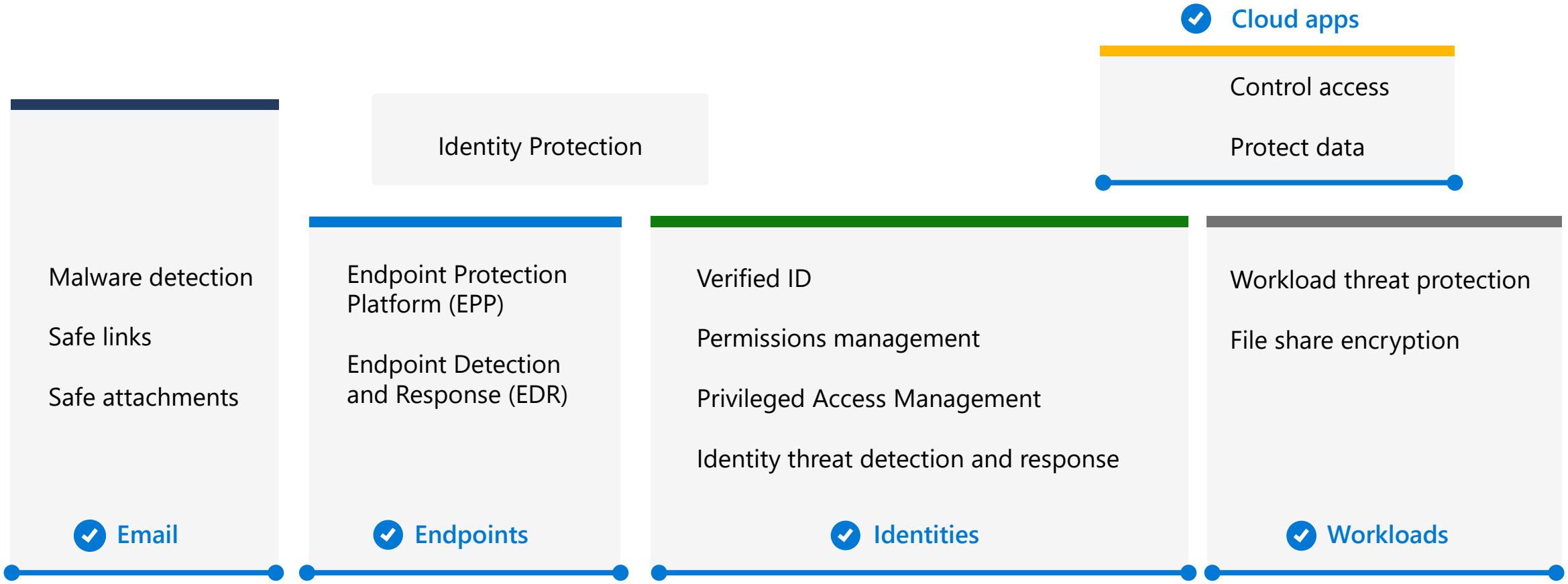
With Microsoft SIEM and XDR



Uncover the attack end to end and take action to completely evict the attacker.

Protection across the entire kill chain

With Microsoft SIEM and XDR



Uncover the attack end to end and take action to completely evict the attacker.

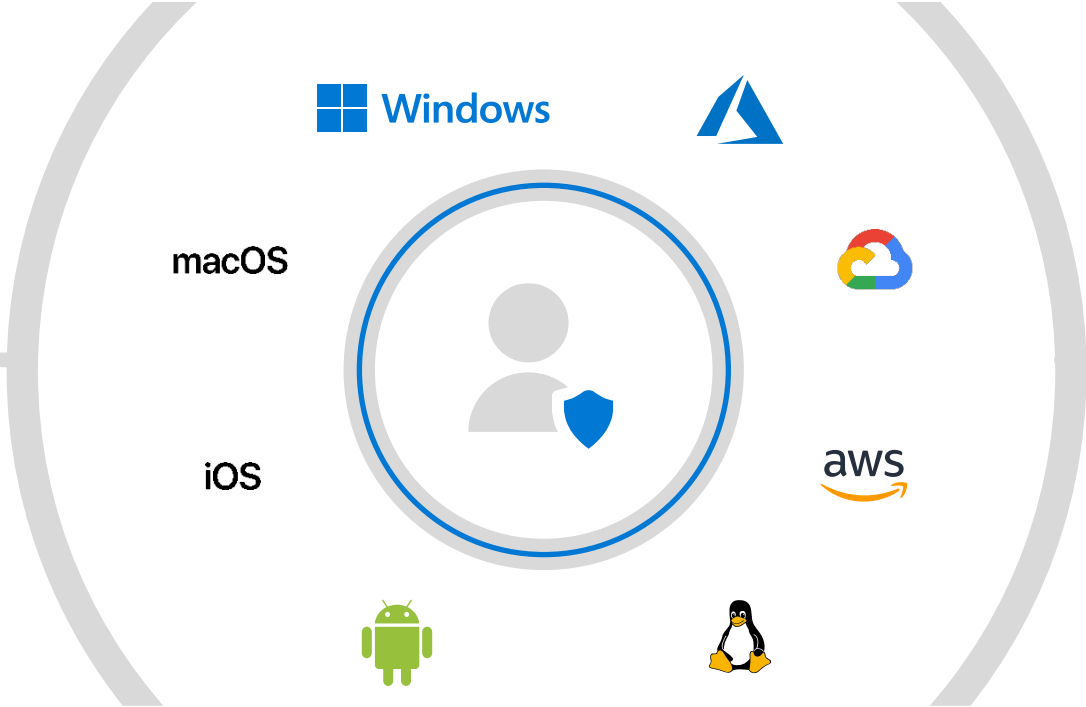
Microsoft's Defenders

Holistic protection from internal and external threats

SIEM

Microsoft Sentinel

Visibility across your entire organization



Existing security portfolio

Microsoft ecosystem

Microsoft 365 Defender

Secure your end users

Microsoft Defender for Cloud

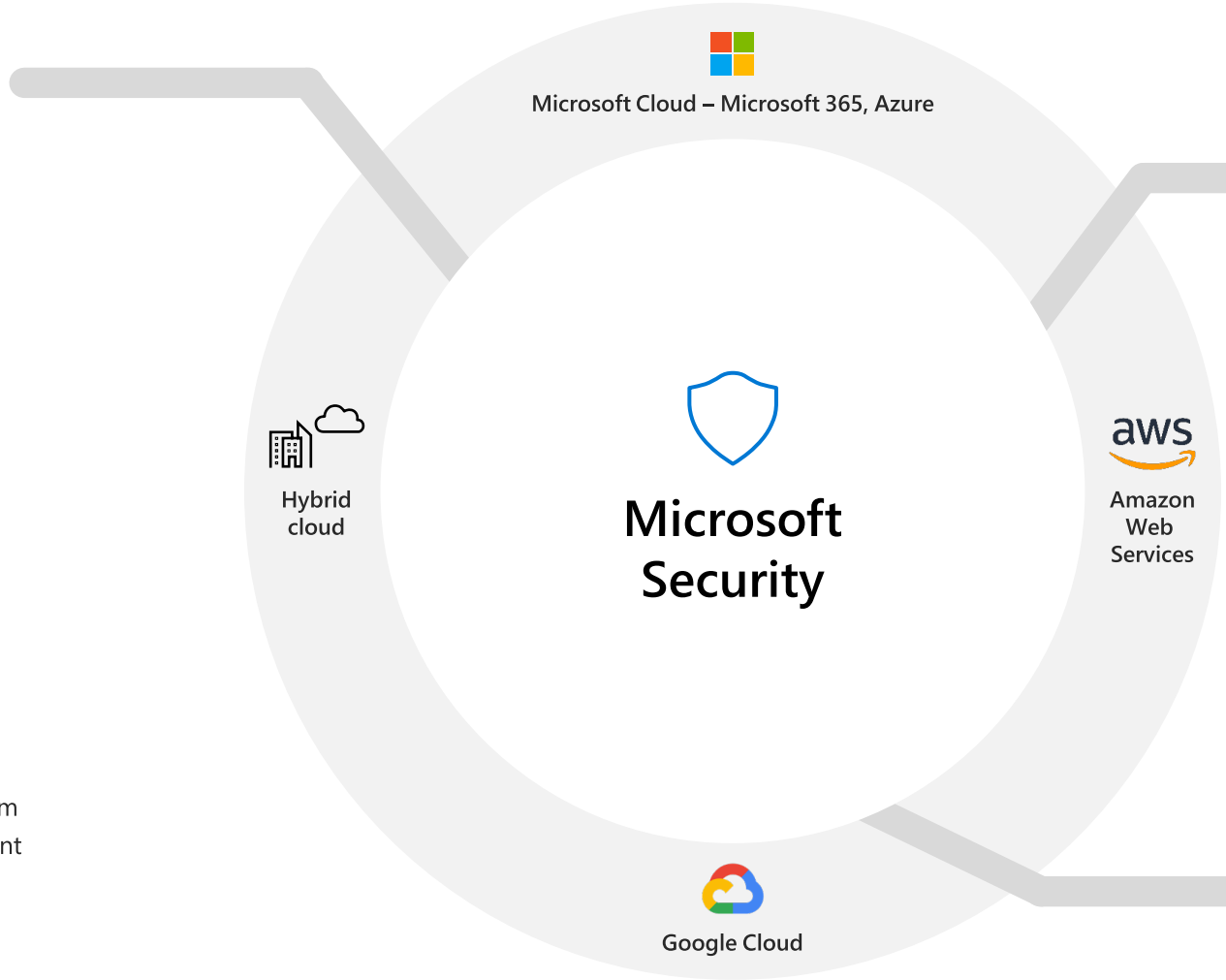
Secure your infrastructure

XDR

Microsoft's end-to-end security

Integrate over 40 categories

Endpoint detection and response
Endpoint protection platform
Forensic tools
Intrusion prevention system
Threat vulnerability management
Anti-phishing
User and entity behavior analytics
Threat intelligence feeds
App and browser isolation
Attachment sandboxing
Application control
End-user training
Network firewall (URL detonation)
Host firewall
Secure email gateway
Security assessment
SIEM
SOAR
Cloud access security broker
Cloud workload protection platform
Cloud security posture management
Incident response services
DDOS protection
IoT protection



Data discovery
Data classification
Data loss prevention
Insider risk management
Data retention
Data deletion
Records management
eDiscovery
Audit
Risk assessment
Privileged access management
Compliance management
Information and messaging encryption

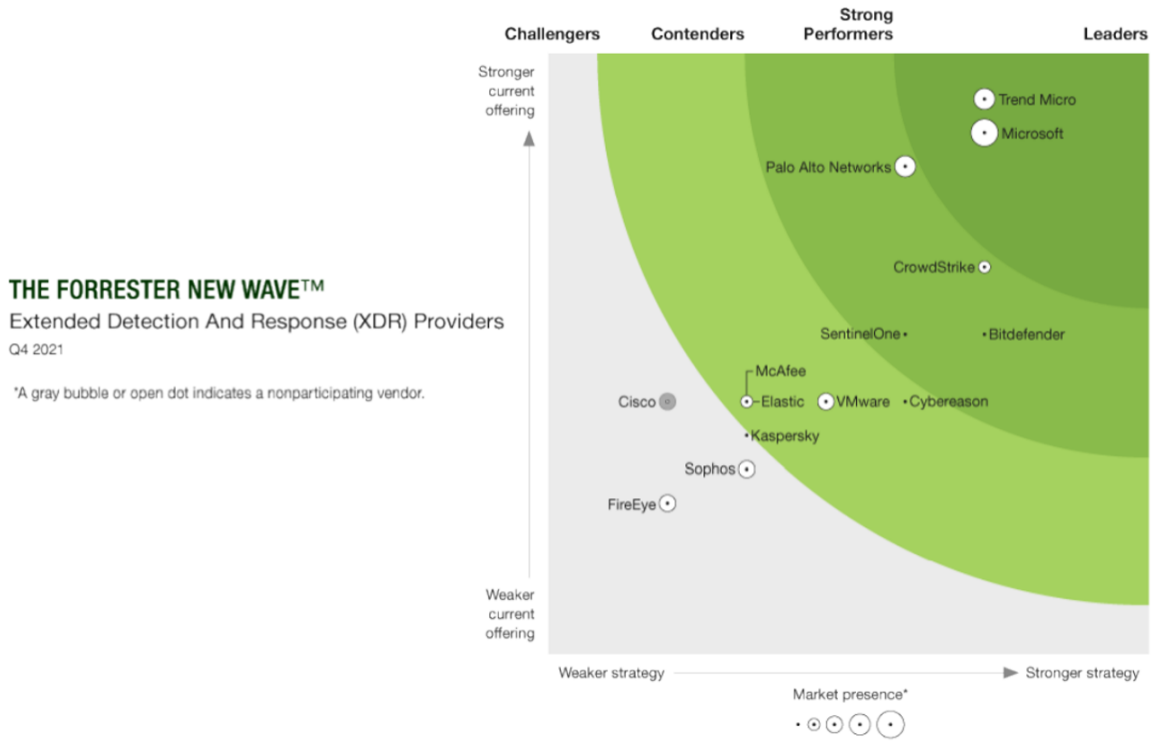
Identity and access management
Single sign-on
User provisioning
Multi-factor authentication
Passwordless authentication
Risk-based conditional access
Identity protection
Self-service password reset
Identity governance
Priviledged identity management
Endpoint management
Mobile application management
Mobile device management

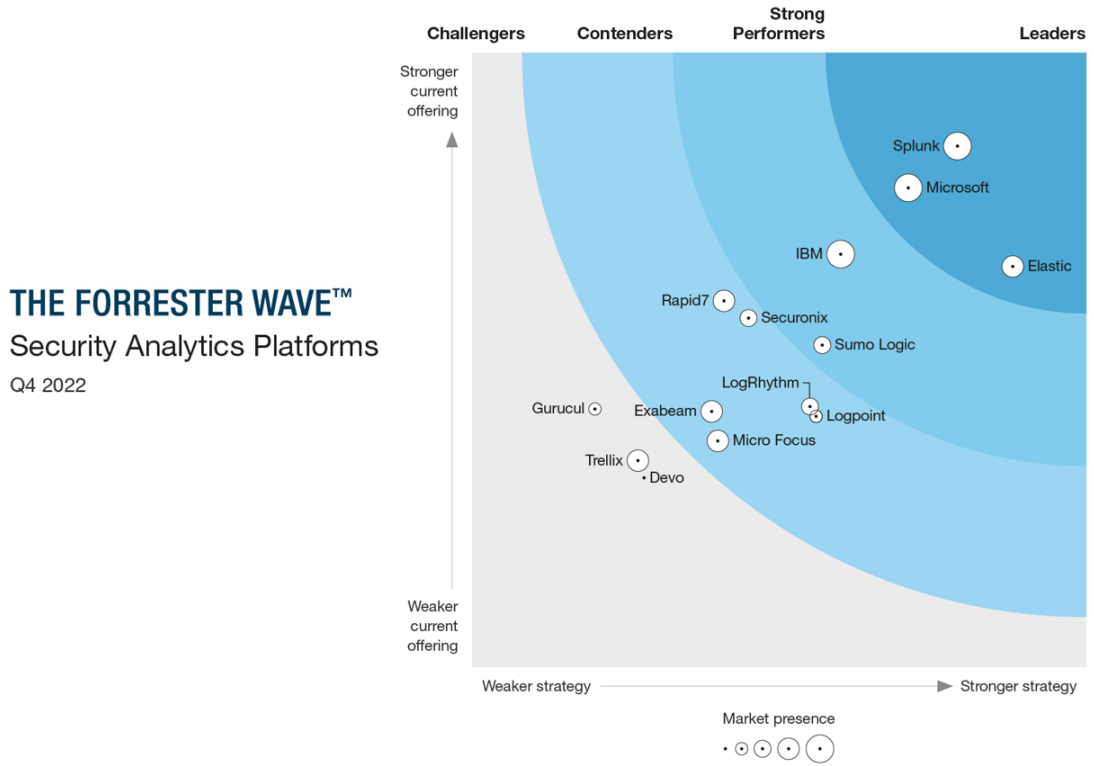
Don’t take our word for it…

Endpoint Protection Platforms

Magic Quadrant for Security Information and Event Management

Don’t take our word for it…

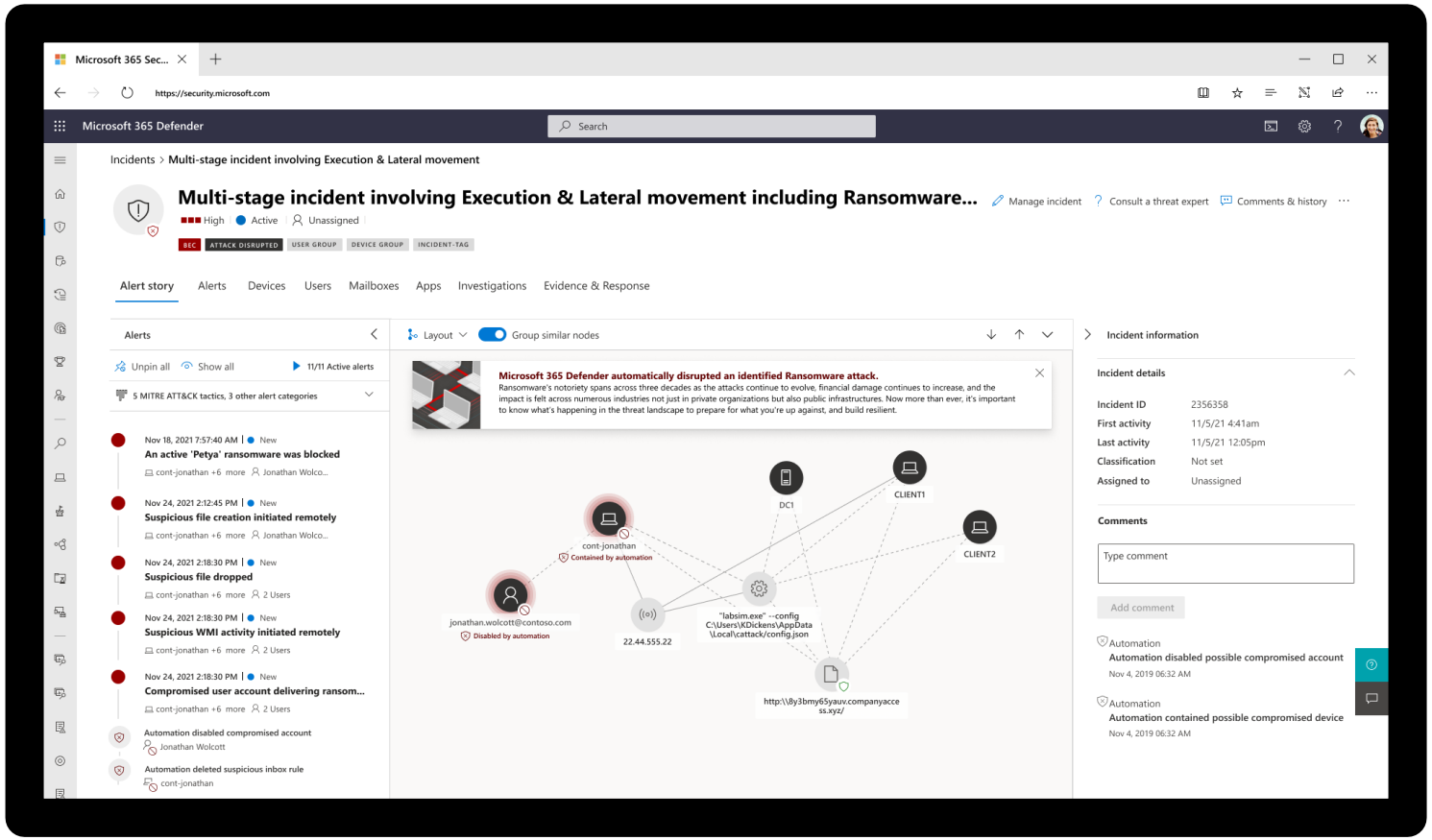




Automatic attack disruption - At machine speed

Automated response actions aimed to quickly contain an attack in progress, based on high-confidence, cross-workload signals.

- **Correlates signals** across endpoints, identity, email, documents, cloud apps
- **Automatically suspends compromised accounts and isolates infected devices** used to spread ransomware payloads
- **Reduces the overall cost of an attack** by stopping attacks from spreading laterally
- **Leaves your SOC team in full control** of investigating, remediating, and bringing assets back online



Microsoft 365 Sec...

https://security.microsoft.com

Microsoft 365 Defender

Search

Incidents > Multi-stage incident involving Execution & Lateral movement

Multi-stage incident involving Execution & Lateral movement including Ransomware...

Manage incident | Consult a threat expert | Comments & history

High | Active | Unassigned

RANSOMWARE | ATTACK DISRUPTION

Alert story | Alerts | Devices | Users | Mailboxes | Apps | Investigations | Evidence & Response

Alerts

Unpin all | Show all | 11/11 Active alerts

5 MITRE ATT&CK tactics, 3 other alert categories

Nov 18, 2021 7:57:40 AM | New

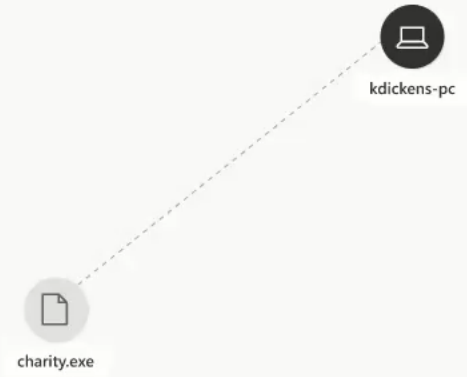
An active 'Petya' ransomware was blocked

kdickens-pc

Layout | Group similar nodes

Microsoft 365 Defender automatically disrupted an identified Ransomware attack

Ransomware's notoriety spans across three decades as the attacks continue to evolve, financial damage continues to increase, and the impact is felt across numerous industries not just in private organizations but also public infrastructures. Now more than ever, it's important to know what's happening in the threat landscape to prepare for what you're up against, and build resilient, if not reinforce security solutions against such cybersecurity attacks.



Incident information

RANSOMWARE

Ransomware Incident response playbook

View Ransomware recommended steps for this incident

Open playbook

Incident details

Incident ID	2356358
First activity	11/18/21 7:57 AM
Last activity	11/24/21 2:24 PM
Classification	Not set
Assigned to	Unassigned

Comments

Type comment

Add comment

BCNET CONNECT

Thank You!