



BCNET
CONNECT
HIGHER ED & RESEARCH TECH SUMMIT

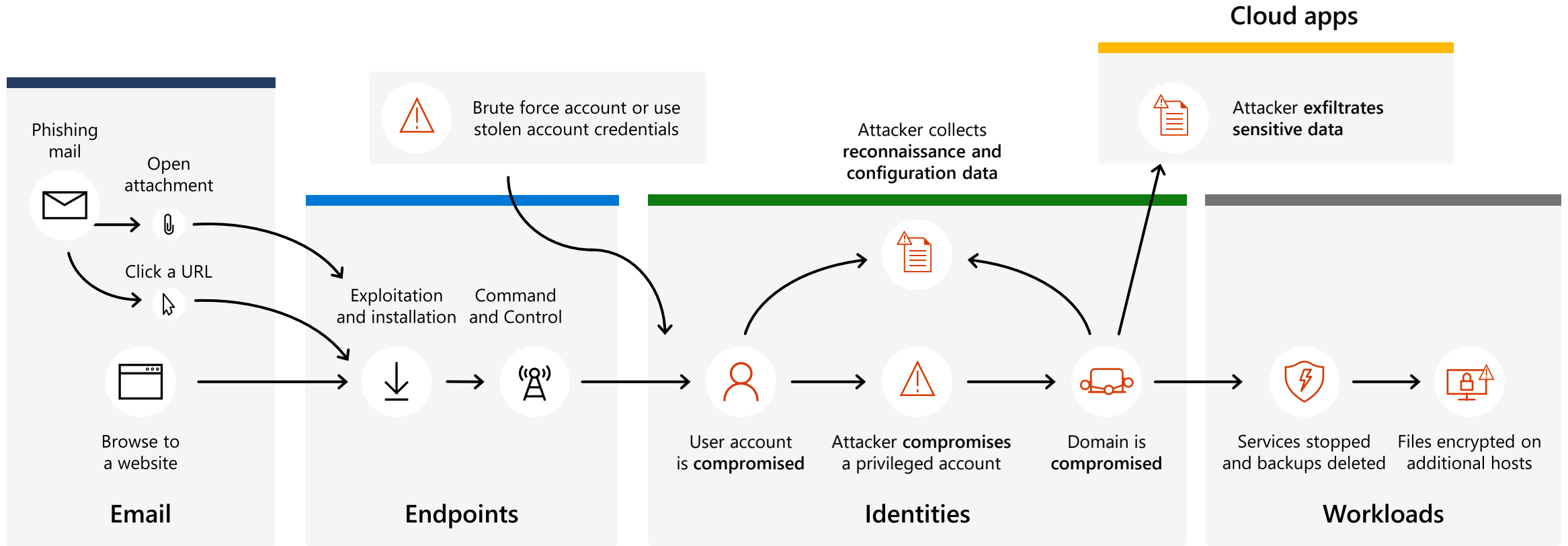
**Reduce Complexity &
Increase Security with XDR +
SIEM**

Why is defense so difficult?



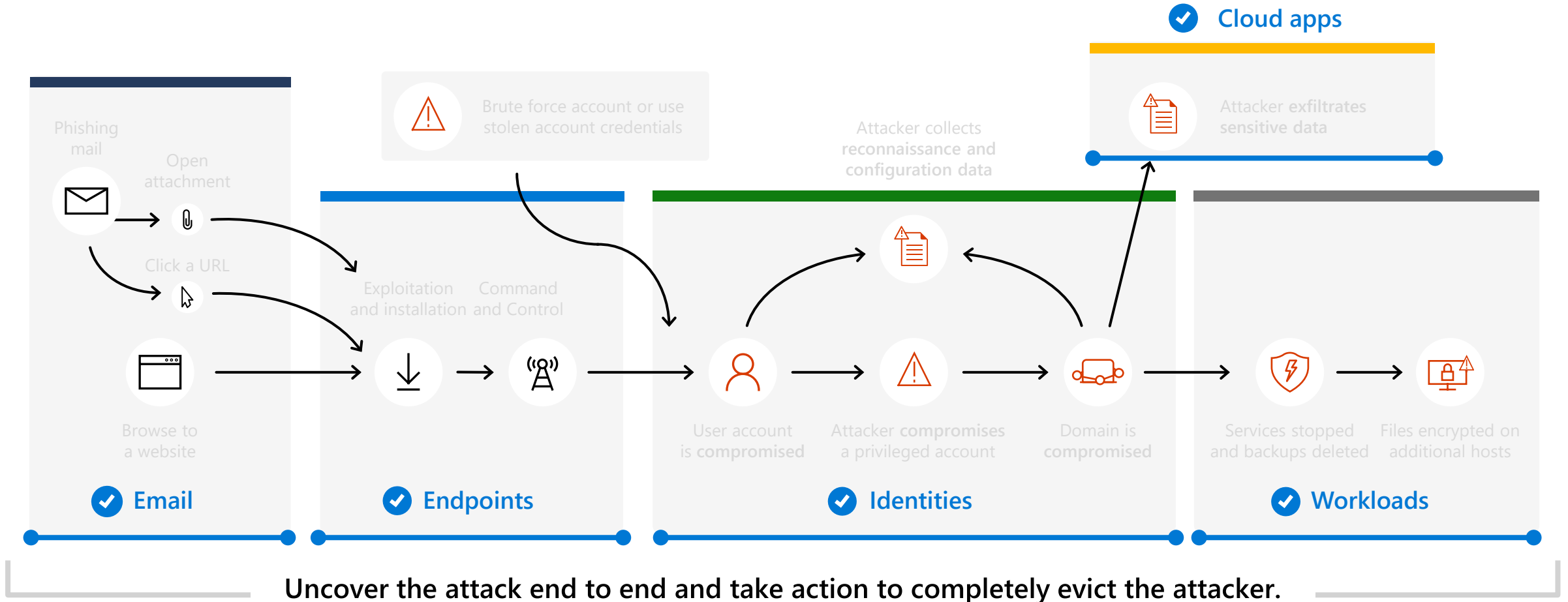
Attacks are crossing modalities

Typical human-operated ransomware campaign



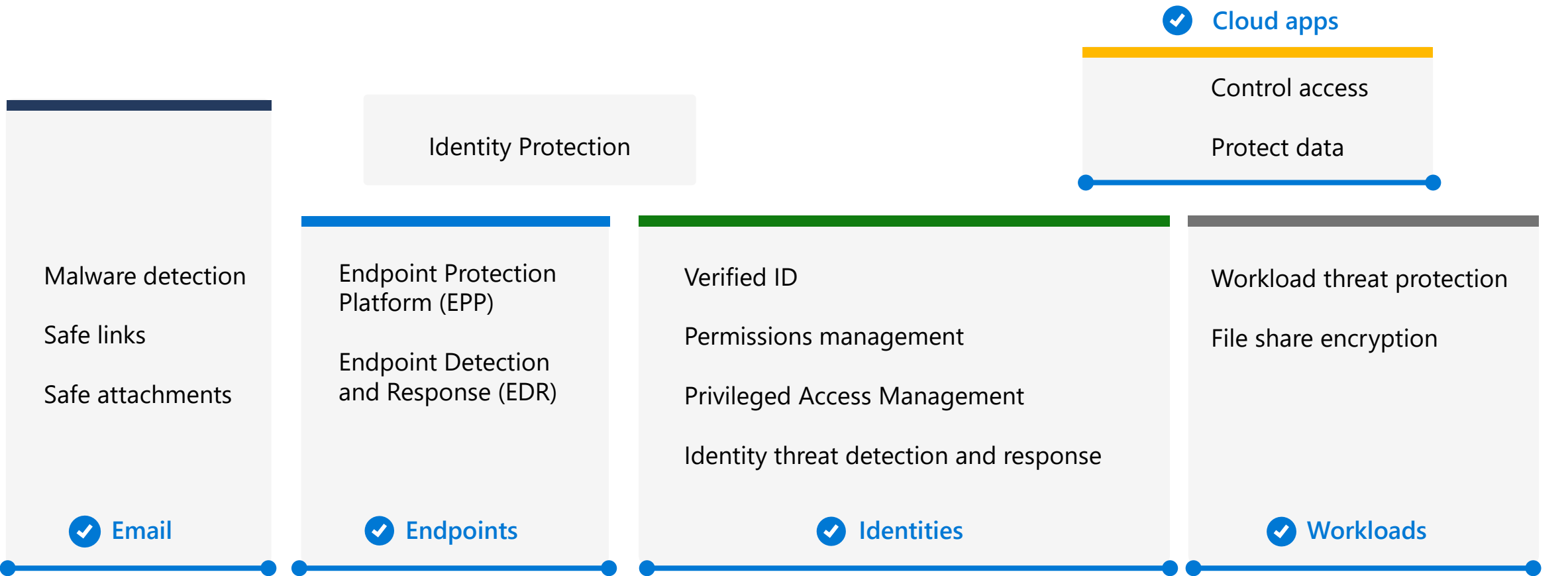
Protection across the entire kill chain

With Microsoft SIEM and XDR



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



Microsoft 365 Defender

Secure your end users

Microsoft Defender for Cloud

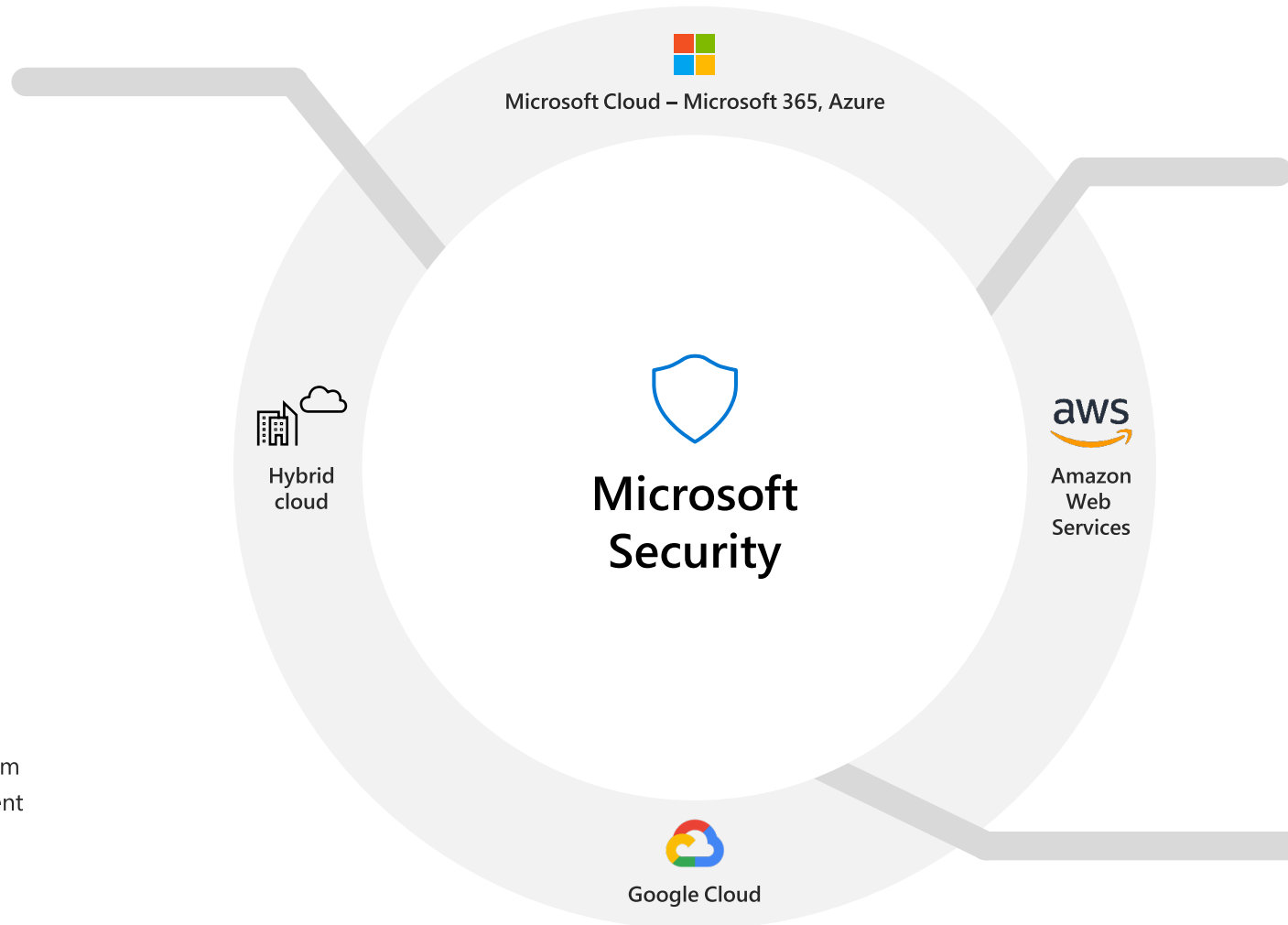
Secure your infrastructure

XDR

Microsoft's end-to-end security

Integrate over 40 categories

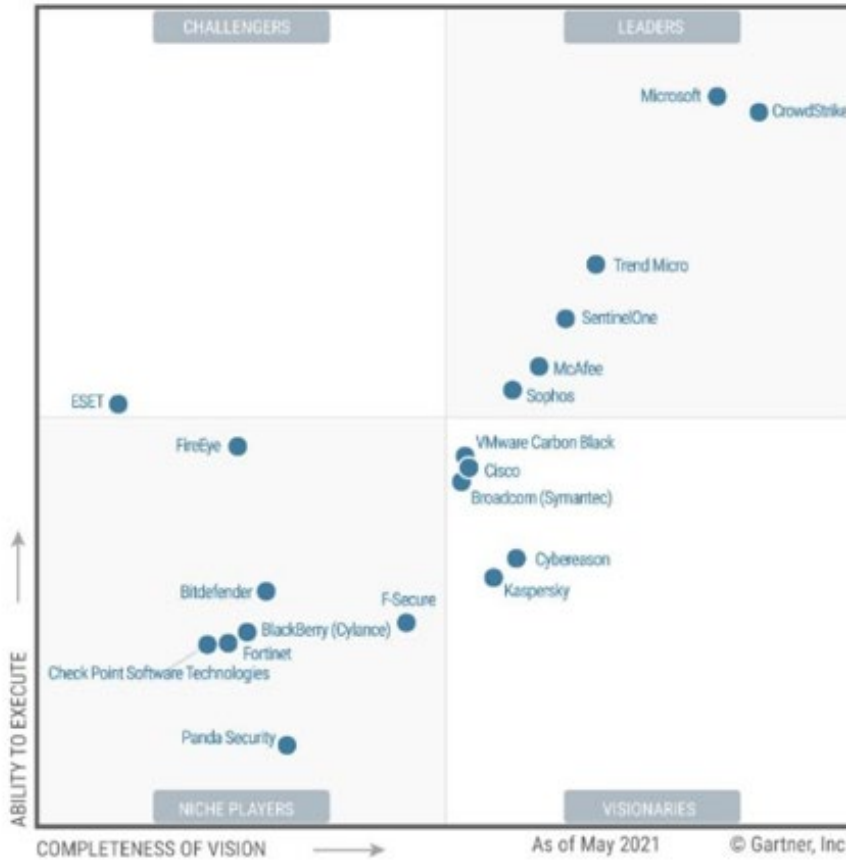
- Endpoint detection and response
- Endpoint protection platform
- Forensic tools
- Intrusion prevention system
- Threat vulnerability management
- Anti-phishing
- User and entity behavior analytics
- Threat intelligence feeds
- App and browser isolation
- Attachment sandboxing
- Application control
- 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
- Privileged 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

These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

Don't take our word for it...

THE FORRESTER NEW WAVE™ Extended Detection And Response (XDR) Providers Q4 2021

*A gray bubble or open dot indicates a nonparticipating vendor.



The Forrester New Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester New Wave™ is a graphical representation of Forrester's call on a market. Forrester does not endorse any vendor, product, or service depicted in the Forrester New Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

THE FORRESTER WAVE™ Security Analytics Platforms Q4 2022



The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

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

The screenshot displays the Microsoft 365 Defender interface. The main heading is "Multi-stage incident involving Execution & Lateral movement including Ransomware...". The incident is categorized as "High" and "Active". A central alert story lists several events:

- Nov 18, 2021 7:57:40 AM | New: An active 'Petya' ransomware was blocked.
- Nov 24, 2021 2:12:45 PM | New: Suspicious file creation initiated remotely.
- Nov 24, 2021 2:18:30 PM | New: Suspicious file dropped.
- Nov 24, 2021 2:18:30 PM | New: Suspicious WMI activity initiated remotely.
- Nov 24, 2021 2:18:30 PM | New: Compromised user account delivering ransom...

Below the alert story, a network diagram shows the attack path. It includes nodes for "cont-jonathan" (containing automation), "jonathan.wolcott@contoso.com" (disabled by automation), "22.44.555.22", "DC1", "CLIENT1", "CLIENT2", and "http://18y3bmy65yauw.companyaacce.ss.xyz/". A central node shows a command: "tabsim.exe --config C:\Users\KDiskeno\AppData\Local\catback\config.json".

On the right, the "Incident information" panel shows details such as Incident ID (2356358), First activity (11/5/21 4:41am), Last activity (11/5/21 12:05pm), Classification (Not set), and Assigned to (Unassigned). The "Comments" section shows automation actions: "Automation disabled possible compromised account" and "Automation contained possible compromised device".

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

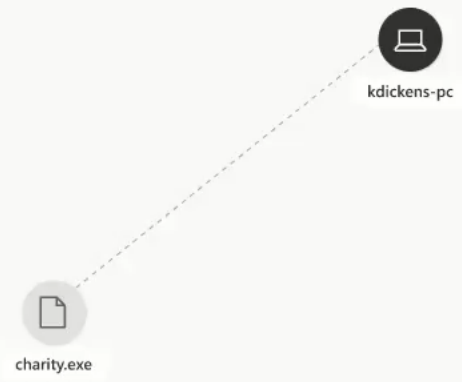
An active 'Petya' ransomware was blocked

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!