Microsoft Security

Automatic Attack Disruption

The future of adaptive threat defense

Contents

Modern security: Adjusting to an ever-moving target

The security landscape has fundamentally shifted from defined perimeters to fluid boundaries, where multi-domain, advanced attacks can strike and adapt faster than traditional defenses can counter.

Modern attacks increasingly operate across multiple domains simultaneously, with threat actors orchestrating complex campaigns that can move between email, endpoints, identities, and cloud environments. This convergence of attack vectors means that threats can quickly pivot and adapt when blocked in one area.

These attacks, now even fueled by generative AI capabilities, operate at a scale and speed that require the transformation of digital defense. Threat actors can launch thousands of automated attempts across multiple vectors in seconds while simultaneously executing targeted campaigns. This combination of velocity and volume doesn't just overwhelm traditional defenses—it fundamentally changes the cost equation for security teams working to maintain effective monitoring and response capabilities.

Novel attack methods require defense in depth

Widespread reconnaissance campaigns are leading to increasingly targeted attacks. Yesterday's ransomware encrypted data from company devices to try and extort the company. Today it exfiltrates, analyzes, and weaponizes information while tampering with security products to remain undetected as attackers move deeper into the network.

Business email compromise (BEC) has emerged as one of the most financially devastating cyber threats to organizations globally. In 2023, the FBI received 21,489 BEC complaints with adjusted losses of over $2.9 billion.[1]

As malicious actors harness these modern methods for increased attack speed and effectiveness, Microsoft Defender XDR's automatic attack disruption capability provides inline, automated responses that use adaptive real-time threat intelligence to identify, contain, and respond to attacks. As we'll see, it's unlike anything on the market today.

> Basic security hygiene remains relevant, but it's now foundational. What's required is a 'defense-in-depth' approach, implementing layers of security that provide multiple checks.

[1] "Federal Bureau of Investigation Internet Crime Report 2023," Federal Bureau of Investigation, 2023.

Where do SOC solutions stand today?

Security solutions took a leap forward with automated defense solutions, namely SOAR and basic automation remediation. However, these tools were designed at a time when the threat landscape was more predictable and less complex.

SOAR (Security Orchestration, Automation, and Response) emerged as organizations faced an increasing volume of security alerts across multiple platforms. SOAR platforms coordinate security actions across an organization's technology stack, enabling teams to standardize response procedures and accelerate threat remediation through orchestrated playbooks.

Automated incident response (AutoIR) was created to provide immediate, automated responses to specific security incidents at the entity level. These solutions target discrete security events, like compromised credentials or suspicious endpoint activity, with predefined response actions. AutoIR tools help organization’s reduce response times and maintain consistent security protocols for known threat patterns.

Both these approaches were designed to initiate remediation post-breach rather than enabling disruption during an active attack.

Challenges facing today's leading security models:

SOAR Post-breach	**AutoIR (AIR)** Post-breach
Requires manual configuration and maintenance	Entity-specific responses only
Relies on predefined playbooks	Single-domain focus
Limited by organization's expertise and ability to update rules	Reactive rather than proactive

> Today's attacks do significant damage while the incident is ongoing. This leaves organizations vulnerable to dynamic attacks that move faster than traditional playbooks account for.

Closing the gap between security incident and solution

Speed is everything in modern security. Attackers begin moving laterally less than five minutes after they escalate privileges. Whereas they used to take hours or days, entire incidents that involve corrupting identities, apps, endpoints, email, and data now happen in minutes.

Traditional tools can't keep up, and it's unrealistic to shift that responsibility to the SOC team. Managing the volume of incoming alerts, while juggling multiple security tools with different interfaces and workflows, presents a serious challenge to an SOC team's bandwidth. While basic automation exists for known threats, it barely scratches the surface of what teams must monitor and manage daily.

These operational hurdles are compounded by technical limitations. Traditional playbooks remain static in the face of constantly evolving threats, while single-domain solutions leave dangerous gaps between security controls.

While threats can propagate across an environment in minutes, security teams often need hours to piece together a complete picture of an attack and coordinate an effective response. This disparity between rapid, orchestrated attack execution and manual defense creates windows of opportunity that adversaries are well equipped to exploit.

> Without proactive security capabilities, teams are perpetually caught in a reactive stance, always one step behind complex attacks. The consequence? A critical speed gap that favors attackers.

Automatic attack disruption: Bringing response closer to the point of attack

"Prevention is the goal, but preparation for an attack and being able to respond is the next step. At some point we're going to be in an active attack and how quickly we respond will be critical."

CIO, Manufacturing

3-minute

average disruption time for ransomware

Automating attack disruption within Microsoft Defender XDR represents a fundamental shift from reactive to inline defense, leveraging adaptive real-time threat intelligence and machine learning–based alert correlation to identify and stop attackers before they can cause significant damage. Now you can detect and contain attacks in real time.

Unlike traditional solutions that rely on predefined rules, this capability adapts in real time to emerging threats, providing a level of protection that was previously impossible.

Built-in protection eliminates complex configuration requirements and ensures immediate coverage. Cross-domain visibility and response capabilities provide seamless protection across the entire digital estate, while AI and machine learning power its active defense system—anticipating and neutralizing threats before they can execute their payload.

Together, these features create a proactive security posture that operates autonomously to protect organizations.

Microsoft's native breadth of signal, best-of-breed components, and threat intelligence acquired from 78 trillion signals and 10,000 security researchers, enables the development and maintenance of automatic attack disruption, integrated into a single, unified security operations platform.

35,000+ incidents disrupted monthly

Automatic attack disruption has created a 3x decrease in ransom attacks reaching encryption stage over the past two years.[2]

[2] "10 essential insights from the Microsoft Digital Defense Report 2024," Microsoft, Inc., December 2024

Rewriting the security playbook

"This anticipatory feature is something we haven't been able to automate before. It's like hiring a person who has experienced that type of breach at another company and has already learned the lessons."

Global Director of Cybersecurity, Retail/Wholesale

At its core, two main parts comprise attack disruption: a set of detections and a set of "automated actions" that are triggered when the detections have identified an incident.

Detections are fueled by an extensive AI-powered graph that collects and correlates alerts at the billion scale, incorporating adaptive real-time threat intelligence, security researcher expertise, and platform telemetry.

Automatic attack disruption functions like a living defense system, powered by continuously updated, built-in playbooks that adapt to emerging threats. In this way, your system maintains constant vigilance and takes decisive action—even when your security team is managing a multitude of tasks. The result is uninterrupted protection that operates at machine speed, independently applying critical controls when needed.

The result is the ability to detect an in-progress attack with above 99% confidence before the attacker can execute the rest of their campaign.

Automatic attack disruption identifies and disrupts in-progress attacks while containing compromised assets—building on, and improving, existing security models.

Automation within the SOC—what's available today?

Attack Disruption Active attack	**SOAR** Post-breach	**AutoIR (AIR)** Post-breach
Goal: **Identify and disrupt in-progress attacks** and contain the compromised assets	Goal: Auto-remediate known and common threats in the organization	Goal: SOC efficiency, remediate attacks after they have taken place
Built-in, no configuration required, multi-domain, and mantained solely by Defender XDR	Customizable templates maintained by the organization	Built-in, entity specific
Continuously tuned and refined with signals, research insights on latest attack patterns	Integrate with any product or service to use as a data source	No integrations available, relies only on entity signal
Adapts to behavior seen inline with an incident attack to take an automatic response	Out-of-the-box playbooks available for analysts to cutomize the response	Triggers based on single alerts, not incidents; response actions are limited to entity
Automated	Manual	Automated

Once the attack is detected, the path of an attacker can be predicted. This triggers adaptive, automated response actions built into the platform—like disabling a user, or containing a device.

Rather than treating security signals as isolated data points, attack disruption begins with comprehensive signal collection and incident correlation across the entire security ecosystem.

The system creates a unified view of potential threats that enables faster, more accurate responses, by consuming high-confidence signals from multiple sources:

- Endpoints and IoT
- SaaS applications
- Email and collaboration tools
- Hybrid identities
- Cloud workloads
- Data security tools
- Third-party data

Real-time analysis drives immediate, adaptive responses. When an attack is detected, the system automatically identifies and disables compromised assets that attackers are using as stepping stones, effectively cutting off their ability to move laterally through the environment.

The system's intelligence is continuously refined through careful monitoring of outcomes. Each incident marked as a false positive becomes a learning opportunity, with the system analyzing the reasons for incorrect detection to improve its models for greater decision-making accuracy in the future.

By dynamically pivoting based on identified attack paths, disruption stops the attack by pulling from a pool of response actions that are uniquely tailored to the attack, such as:

- Disabling users both on-premise and in the cloud
- Disabling OAuth apps
- Containing devices
- Containing IPs

180,000+

devices protected in six months

120,000+

disabled users in the last six months

> Attack disruption proves most valuable in scenarios where speed and precision matter most.

Disruption within the Microsoft SecOps ecosystem

Microsoft is uniquely positioned with global security infrastructure and industry-leading software development, enabling unprecedented visibility across the threat landscape. This comprehensive view, combined with insights from millions of endpoints and thousands of security experts, creates a security ecosystem that becomes more effective with each attempted attack.

When you unify security operations with Microsoft, you combine global threat intelligence with all the capabilities of SIEM, XDR, cloud security, exposure management, and generative AI solutions in a single experience.

6,000+

adversary in the middle (AiTM) attacks disrupted monthly

Attack disruption leverages Microsoft's ability to create holistic threat visibility from connected signals across the entire Microsoft ecosystem—some of which may already be part of your organization's digital estate:

- Microsoft Defender for XDR
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Microsoft Purview
- Microsoft Sentinel

Beyond specific security solutions, attack disruption is informed by Microsoft's wider access to threat intelligence, gathered from:

78 trillion
signals daily

10,000
security experts

1 million
security customers

Attack disruption blurs the boundaries between pre-breach and post-breach, harnessing a vast centralized database from Microsoft, and adding new intervention capabilities to be more responsive and scale your digital defense.

> Unlike traditional solutions that rely on predefined rules, this capability adapts in real time to emerging threats, providing a level of protection that was previously impossible.

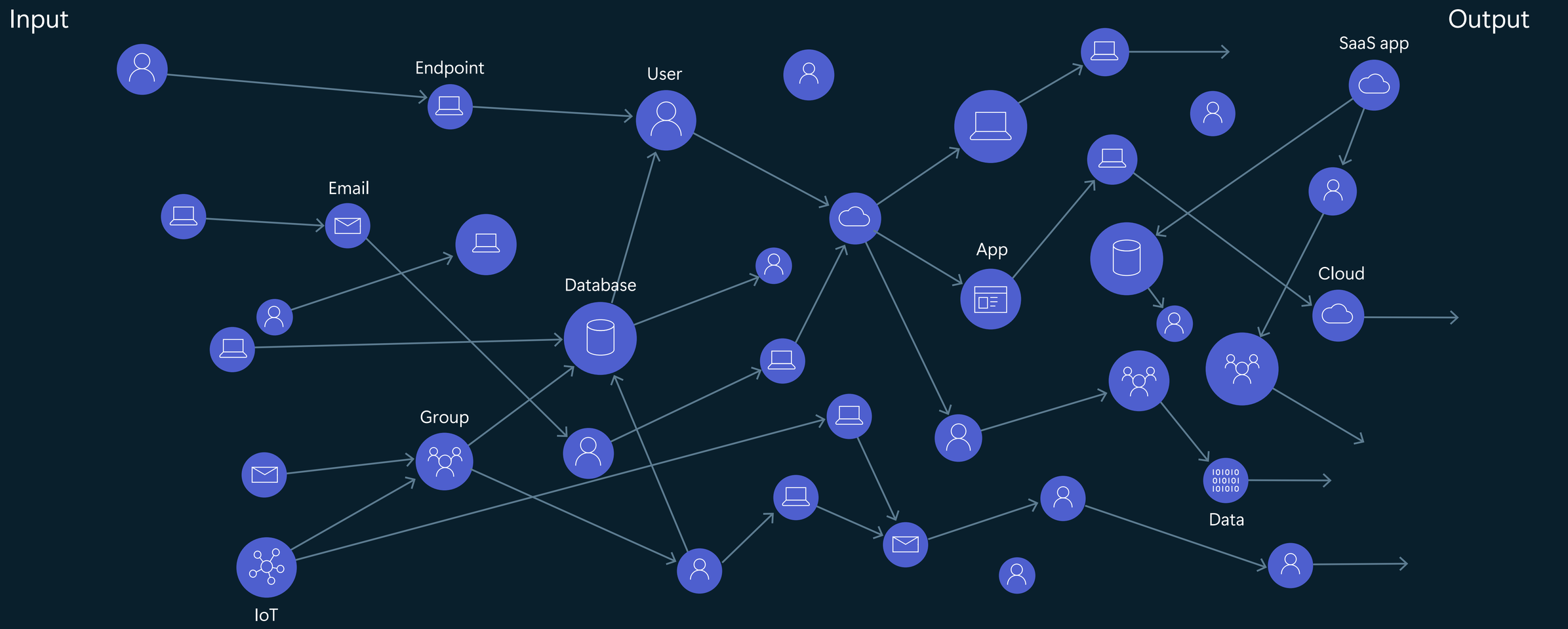
Use case: Attack disruption in action

Modern cyberattacks are complex, coordinated campaigns that can target multiple domains simultaneously. The following sequence demonstrates the challenge and the solution: from mapping the complex interconnected landscape defenders must protect, to revealing how attacks progress, and ultimately showing how automatic attack disruption works to stop threats in their tracks.

Learn how sophisticated attacks are met with equally sophisticated defense mechanisms that operate in real time across your entire digital estate.

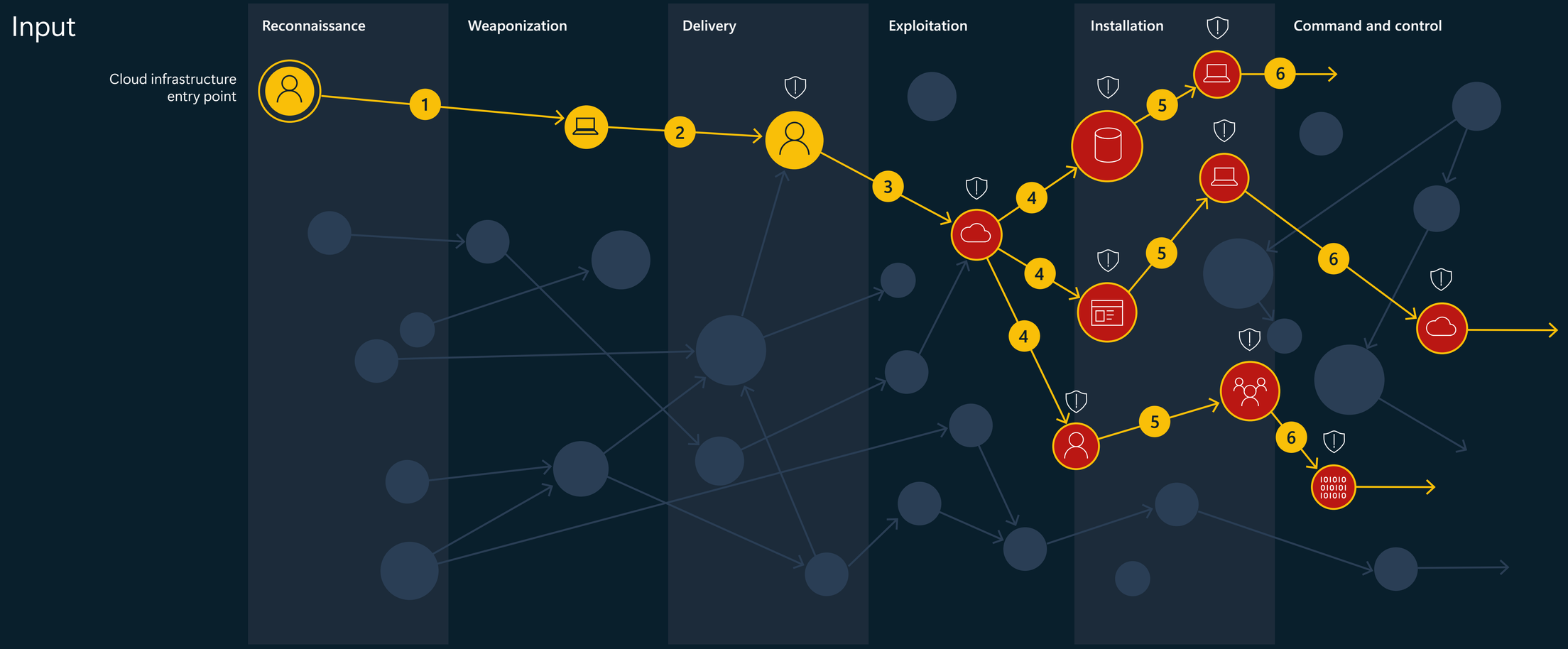
A relationship entity map of the enterprise

Today's SOC protects a complex ecosystem where diverse workload assets intersect and interact.



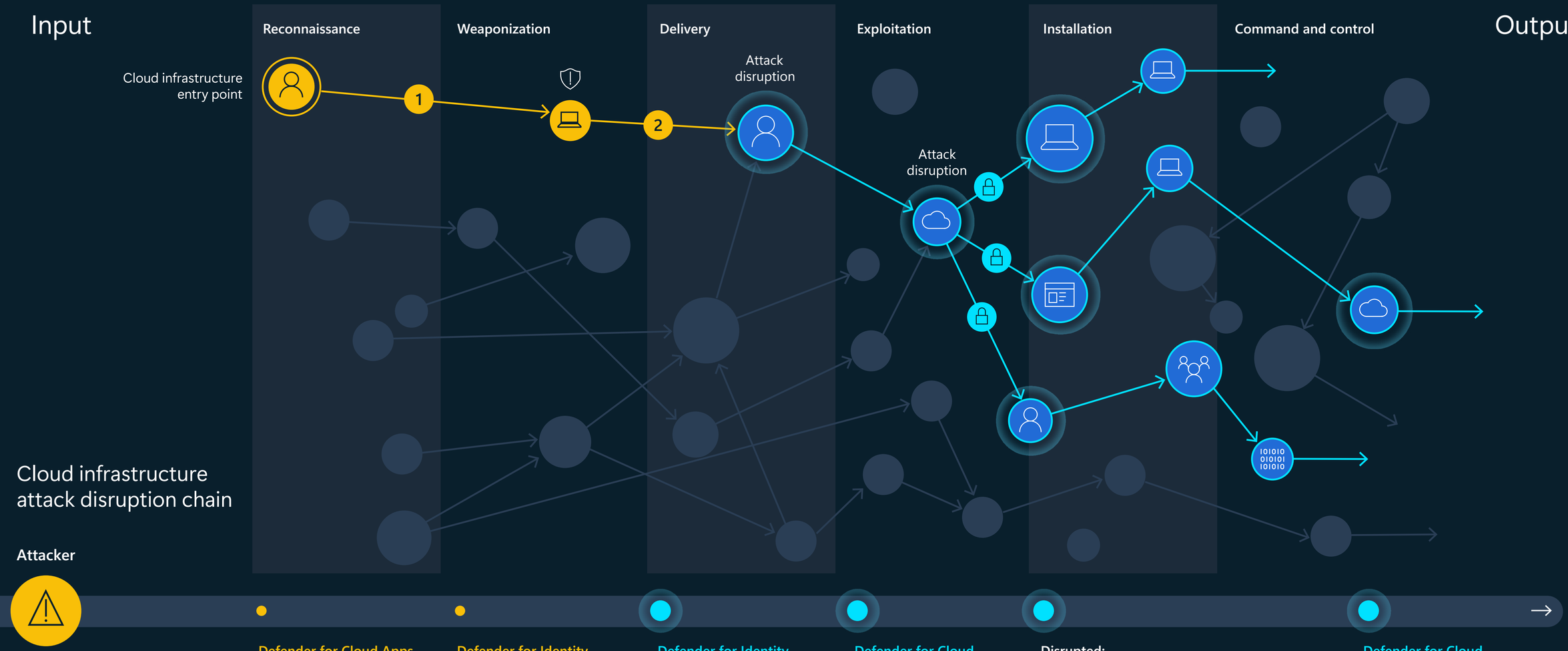
Cloud infrastructure attack chain

Here's a complex, multistage incident—one that could happen in any digital environment. A cloud infrastructure attack progresses through its attack path, from initial reconnaissance to command and control. Of the thousands of potential permutations and combinations of attacks, this attacker has taken four different attack paths—and is ready to backtrack and pivot based on the SOC's responses.



Automatic attack disruption | Cloud infrastructure

Automatic attack disruption leverages cross-domain visibility to identify and stop threats earlier in the kill chain, using advanced mapping to detect malicious activity and harden protection before it progresses laterally. In this instance by using attack disruption SecOps teams have detected, intercepted, and anticipated a complex attack path, isolating real-time attempts while predicting and blocking alternative routes.



The ultimate defense for stopping active threats before they unfold

Modern threats don't wait, and neither can your defenses. By harnessing attack disruption, you're not just adding another security tool—you're fundamentally transforming how your organization responds to threats.

The ability to analyze threats across multiple domains, predict attack patterns, and respond automatically—all while empowering your SOC team to focus on high-value security initiatives—moves your security from manual playbooks to intelligent, automated responses. From reactive to predictive. From isolated security tools to an integrated, self-defending ecosystem.

Take the next step in your security journey. Explore how attack disruption can level up your existing Microsoft security investments, enhance your threat response capabilities, and help secure your organization against evolving threats, by evolving ahead of them.

Supercharge your SecOps effectiveness

Take your SOC team to the next level with automatic disruption of advanced cyberattacks and accelerated response across endpoints and IoT, hybrid identities, email and collaboration tools, software as a service (SaaS) applications, cloud workloads, and data.

Get incident-level visibility across the cyberattack chain with **Microsoft Defender XDR**