Microsoft Security

Coordinated Defense: Building an AI-powered, unified SOC

Contents

The new threat landscape: An executive overview

The threat landscape is more complex than ever. While security teams are saddled with defending the most diverse digital environment in history, attackers are more resourced and capable than ever. They've shifted to orchestrating sophisticated campaigns that chain together multiple vulnerabilities across your systems, resulting in complex kill chains that are tailored to your particular environments. And the rapid adoption and growth of the cloud and generative AI are helping them scale their operations, ushering in a new era of social engineering, vulnerability discovery, and operational reach.

Tackling threats with traditional approaches—like focusing on protecting endpoints from ransomware or segmenting networks to restrict access—is no longer enough. Attackers are exploiting multiple vulnerabilities across your systems, like nodes in a complex graph, to move undetected and reach critical assets and sensitive data. Traditional security tools that operate in silos simply can't keep pace.

Organizations today need to deploy a defense-in-depth approach that utilizes deeply integrated security tools that work together to coordinate defense across security layers. These embrace AI and automation, shifting your organization from manual reaction to automated, proactive defense.

Today's threat landscape: A shift in tactics

Attackers are increasingly employing advanced tools and techniques in targeted, multi-stage attacks. Key trends include:

AI-powered social engineering

Attackers use generative AI to craft highly personalized phishing emails messages, and other communications—often orchestrating multi-channel attacks where, for example, a seemingly innocent ping on Teams primes the target before a malicious email arrives in their inbox.

Many of these attacks don't even contain suspicious links; instead, they might start with a seemingly urgent message from a spoofed email address that appears legitimate, warning about an incoming invoice that "requires immediate payment." **These sophisticated communications are harder to detect through traditional methods like link analysis or malware signatures.** Each message is unique, bypassing pattern recognition systems.

Self-learning malware

Malware incorporating large language models (LLMs) can adapt and rewrite itselfbased on the specific configuration of the device it's installed on—all without any external communication. This autonomous adaptation increases its sophistication and resilience, making it particularly dangerous since it can operate and evolve even when isolated from command-and-control servers.

Exploitation of technical debt

While patching software and implementing MFA remain crucial defenses, threat actors are increasingly taking advantage of technical debt (outdated systems, unpatched vulnerabilities, aging infrastructure, etc.) that organizations struggle to maintain. **Even organizations that have mastered traditional security measures are vulnerable because attackers specifically target these legacy weak points.** Unmanaged devices and less-monitored system integrations have become particularly attractive targets due to their often-overlooked security gaps.

Attacks on generic and multiuser accounts

Identities remain a primary target, with password attacks increasing from 579 to 7,000 per second since 2021.[1] Attackers increasingly target administrative and shared accounts, exploiting outdated passwords and shared access that complicate MFA implementation. The number of threat actors conducting these attacks has grown significantly, from 300 in 2023 to 1,500 in 2024.[2]

[1, 2] "Microsoft Digital Defense Report 2024," Microsoft, 2024

Lessons learned from the front lines

As the last 12 months have clearly demonstrated, working through vulnerability lists, keeping up to date on patches, and implementing security tools to protect critical vectors simply isn't enough. No organization, not even Microsoft, will "out-patch" threat actors. **We need to shift away from working through lists of vulnerabilities to thinking more like an attacker, viewing these not as a large collection of individual exposures but as a prioritized collection of paths that lead to critical assets.**

Recent cyberattacks have brought this need into sharp focus. One of our key learnings was that technical debt represents the biggest weakness for organizations. While you may be using the latest security tools to fortify your core environment, threat actors will find and exploit weak points in old infrastructure, unpatched systems, outdated configurations, and overprivileged applications—often in areas that security teams aren't even aware of.

The challenge intensifies as malign actors become better resourced and better prepared, wielding increasingly sophisticated tactics, techniques, and procedures (TTP) that challenge even the world's best cybersecurity defenders. Our customers face more than 600 million cybercriminal and nation-state attacks every day, ranging from ransomware to phishing to identity attacks. This requires us to address threats at the technique level—not just by attack vectors or top vulnerabilities.

However, there is hope in this evolving landscape. We've observed a 300% decrease in successful ransomware attacks among customers utilizing Defender for Endpoint, even as overall ransomware encounters have risen by 275%. This demonstrates the power of implementing a platform-based approach that unifies policies and controls and employs AI and automation to proactively address weaknesses and dynamically respond to hands-on-keyboard attacks.

As a direct result of these experiences and insights, we launched the Secure Future Initiative (SFI), a company-wide commitment to prioritize security above all else. The SFI serves as the cornerstone of our efforts to protect not only Microsoft but also our partners and customers. We believe that security is a team sport, and the SFI embodies this philosophy, making security everyone's top priority.

Putting security above all else

The Microsoft Secure Future Initiative (SFI) is a multiyear initiative to evolve the way we design, build, test, and operate our products and services, to achieve the highest possible standards for security.

It's our long-term commitment to protect both the company and our customers in the ever-evolving threat landscape.

730k

SFI noncompliant apps eliminated

5.75 million

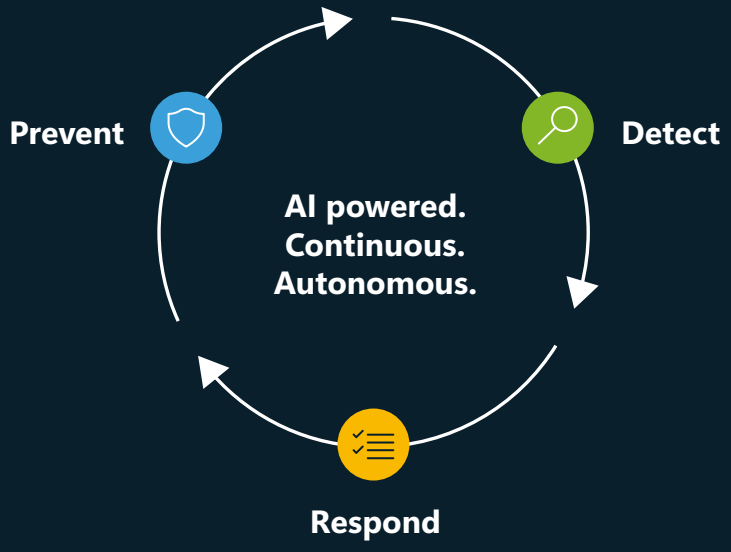
inactive tenants eliminated, drastically reducing the potential cyberattack surface

A new pre-breach/ post-breach paradigm

Tackling your vulnerabilities requires more than just burning down lists. Even small security gaps can lead to devastating breaches when attackers chain them together. Understanding these chains of connections in your environment is nearly impossible with traditional tools because they don't effectively share signal and threat intel. **Today's security teams need tools that work across various domains (identities, email, applications, etc.) and bridge the functional areas of security—connecting prevention, exposure management, detection and response, identity administration, cloud architecture, and other critical functions.**

With traditional tools, security teams face a fundamental problem: They must manually connect the dots between separate tools that don't communicate well with each other. This manual process means vulnerabilities are handled in isolation, making it difficult to see the bigger picture until after a breach occurs. Teams often lack the resources to systematically understand how their system was compromised until after an incident, creating a perpetually reactive security posture.

From reactive and manual to proactive and automated



- **Analyze** attack paths and reduce exposure
- **Disrupt** attacks in real time
- **Unify** investigation experience and accelerate response

Unified security operations platform: Overview and architecture

A unified security operations platform integrates protection capabilities for endpoints, identities, email, apps, data, and cloud environments with the critical SecOps functions of posture management, detection and response, and threat intel into a single experience. This goes beyond the analyst experience to unify the entity inventory, detection models, threat intel, security controls, and workflows across all your foundational security tools. **This helps security teams shift from reactive firefighting to streamlined triage and investigation, proactive posture improvement, and unified threat hunting.**

Instead of managing multiple consoles and struggling with disparate tools, security teams gain a single source of truth, streamlining operations and accelerating response times. A modern platform combines global threat intelligence with SIEM, XDR, cloud security, exposure management, and AI capabilities, spanning the entire threat lifecycle.

Unified security operations

A unified architecture transforms security operations by centralizing data and leveraging AI to enhance human expertise, enabling scale, adaptability, and continuous improvement across the threat lifecycle.

Foundation: Raw data (security and activity logs)

Security operations are only as effective as their data. This layer collects and centralizes entity and activity data from connectors, APIs, raw security logs, and threat intelligence feeds. This consolidation shifts the focus from collecting data to making it actionable.

Data processing and enrichment

This layer standardizes data and uses AI to build a relational graph model of your entire digital ecosystem. The platform enriches this model with threat intelligence, correlates alerts into actionable insights, and prepares it for AI-powered services like agents, attack path modeling, and automated responses. This ensures teams act on accurate, contextualized information.

Core security platform

This layer powers proactive defense by enabling your security platform to identify ongoing attacks, predict attacker steps, and automate responses to block lateral movement. For example, it maps vulnerabilities to potential attack paths using real-time threat intelligence, prioritizing them for remediation. During incidents, these insights predict lateral movement and enable containment.

Expert assistance and managed security services

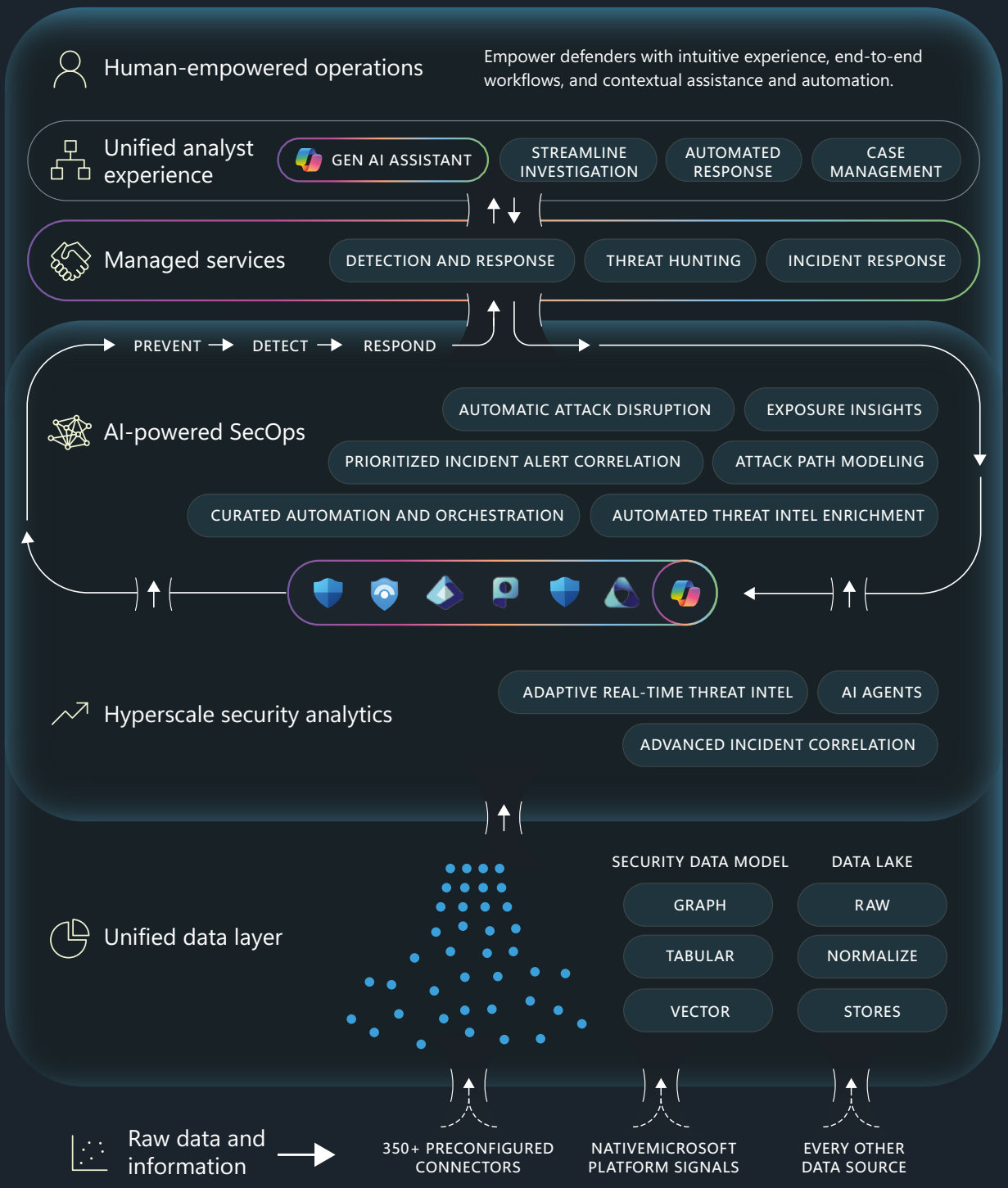
Many SOC teams rely on managed services for expertise and operational scalability. A unified platform integrates managed service workflows, giving external experts full visibility and rich insights into threats for seamless collaboration with the SOC team.

Unified analyst experience

This layer provides a unified view of all security data, alerts, incidents, and insights. Built-in preventive controls enable the SOC team to protect the organization before breaches occur. Key features include automation to streamline tasks, case management for investigations, and generative AI to enhance analysis and simplify reporting.

SOC architecture

Integrating data, AI, and human expertise empowers security teams to prevent, detect, and respond to threats seamlessly across the entire lifecycle.



Building a closed-loop approach to managing threats

A modern security strategy must address the complete threat lifecycle—from preventing initial compromise, to detecting and disrupting active attacks, to investigating and responding to incidents. A unified security platform enables this closed-loop approach by connecting prevention, detection, and response capabilities across your environment. **Let's examine how each phase works together to create a comprehensive defense strategy.**

Prevent: For a better defense, think like an attacker

A unified security platform transforms vulnerability management by consolidating core security data and capabilities. The system can build a comprehensive graph of your entire network, resulting in a complete picture of your attack surface on a single pane of glass. This consolidated view eliminates blind spots created by siloed tools and allows security teams to effectively identify all potential entry points and weaknesses.

With entry points identified, attack path modeling reveals how an attacker might chain vulnerabilities together to breach critical assets. This allows organizations to prioritize remediation based on risk, maximizing the impact of security investments. Threat intelligence provides additional context about active exploits and attacker tactics, techniques, and procedures (TTPs).

Thinking like an attacker reveals the need for a proactive detection and response strategy. **A unified platform integrates essential tools—like SIEM, XDR, and exposure management—to help security teams spot patterns in suspicious activities and uncover potential incidents.** This approach enables faster threat detection and more efficient response while streamlining management, improving correlation, and automating workflows.

Benefits of unified exposure management

Prioritized risk mitigation:
Focus remediation efforts on the most critical vulnerabilities.

Reduced attack surface:
Minimize entry points through consistent security configurations.

Proactive gap identification:
Identify and address security weaknesses before exploitation.

Enhanced resilience:
Adapt to evolving threats with real-time intelligence and automated responses.

Detect: Coordinate defense and disrupt in-progress attacks

While having an environment with virtually zero exposure would help all of us sleep a lot better, it's simply not reality. And we need to be prepared for attackers to continuously try and breach our defenses. **In addition to strong prevention, this requires advanced detection models that always stay up to date and adapt to attackers as they evolve.**

Unlike traditional solutions that periodically scan for known malware and rely solely on endpoint signals, attack disruption uses AI and cross-domain signals to predict an attacker's next move and adapt its response. This means we can block lateral movement early in the kill chain and stop the attacker from progressing. Disruption stops ransomware attacks in an average of just three minutes!

Think of attack disruption as a series of adaptive playbooks that come built in and are constantly updated with the latest and greatest threat intel. This autonomous process ensures real-time response to an attack, no matter how busy your security team is.

Key benefits of attack disruption

Rapid ransomware response:
Neutralize ransomware attacks in an average of just three minutes.

Real-time threat isolation:
Immediately isolate compromised entities to contain breaches.

Predictive threat intelligence:
Use AI to anticipate attacker movements and proactively adapt defenses.

Cross-domain visibility:
Leverage signals from across your environment for comprehensive threat detection.

Autonomous defense:
Automate response actions to ensure consistent and immediate threat mitigation.

Continuous adaptation:
Dynamically update defenses with the latest threat intelligence.

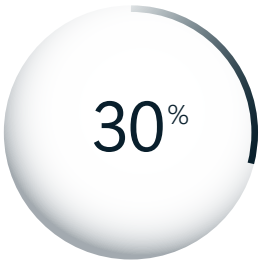
Investigate and respond: Rapidly remediate threats with generative AI

Analysts are drowning in alerts and triage, increasing the risk that the time-sensitive alert further down the queue leads to a catastrophic breach. There's a good chance they're investigating a routine alert while missing major incidents in progress that don't surface properly because they're comprised of numerous low-level alerts. **A unified, generative AI–powered platform improves SOC responsiveness by delivering a single, prioritized incident queue that automatically correlates alerts, enriches incidents with related threat intel, and prioritizes based on severity.** And the unified experience reduces context switching and delivers streamlined, threat intel–enriched investigations with step-by-step guidance and automation.

AI and automation: Empowering proactive security

AI assistants like Microsoft Security Copilot enhance unified platforms by providing valuable insights, automating routine tasks, and correlating alerts into comprehensive incidents. This empowers security analysts to focus on strategic decision-making.

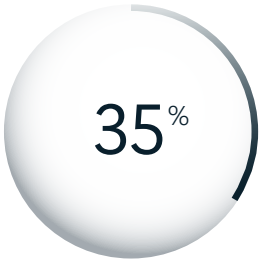
AI and automation also help adapt to the evolving threat landscape, enabling effective responses to new attacker tactics. For example, visualizing potential attack paths during an investigation can reveal how attackers might target critical assets—insight not possible with traditional siloed approaches.



faster incident resolution[3]

With Security Copilot, security analysts save significant time with a **30% reduction in incident mean time to resolution (MTTR)**, recovering 2.7 hours per day previously spent resolving incidents.

[3] "Generative AI and Security Operations Center Productivity: Evidence from Live Operations," Microsoft, November 2024



more accurate decisions[4]

Controlled studies show **35% more accurate outcomes** across security operations, including threat investigation and device policy management.

[4] "Randomized Controlled Trials for Security Copilot for IT Administrators," Microsoft, November 2024

ROI potential[5]

Forrester projects organizations can achieve up to **$1.76M NPV with 348% ROI** over three years based on high-impact scenario analysis.

[5] "New Technology: The Projected Total Economic Impact™ Of Microsoft Security Copilot," Forrester, November 2024

Tackling your most critical security domains

A truly effective security posture requires a unified approach across all areas of your environment. Isolated solutions create gaps that attackers will exploit. **The following content explores five common security domains and demonstrates how a unified platform strengthens defenses in each area. These scenarios will help you identify the most impactful starting points for your organization.**

- Scenario 1: Protect endpoints
- Scenario 2: Protect identities
- Scenario 3: Secure cloud-native applications
- Scenario 4: Protect the entire organization with SIEM and XDR
- Scenario 5: Protect your data

Scenario 1: Protect endpoints

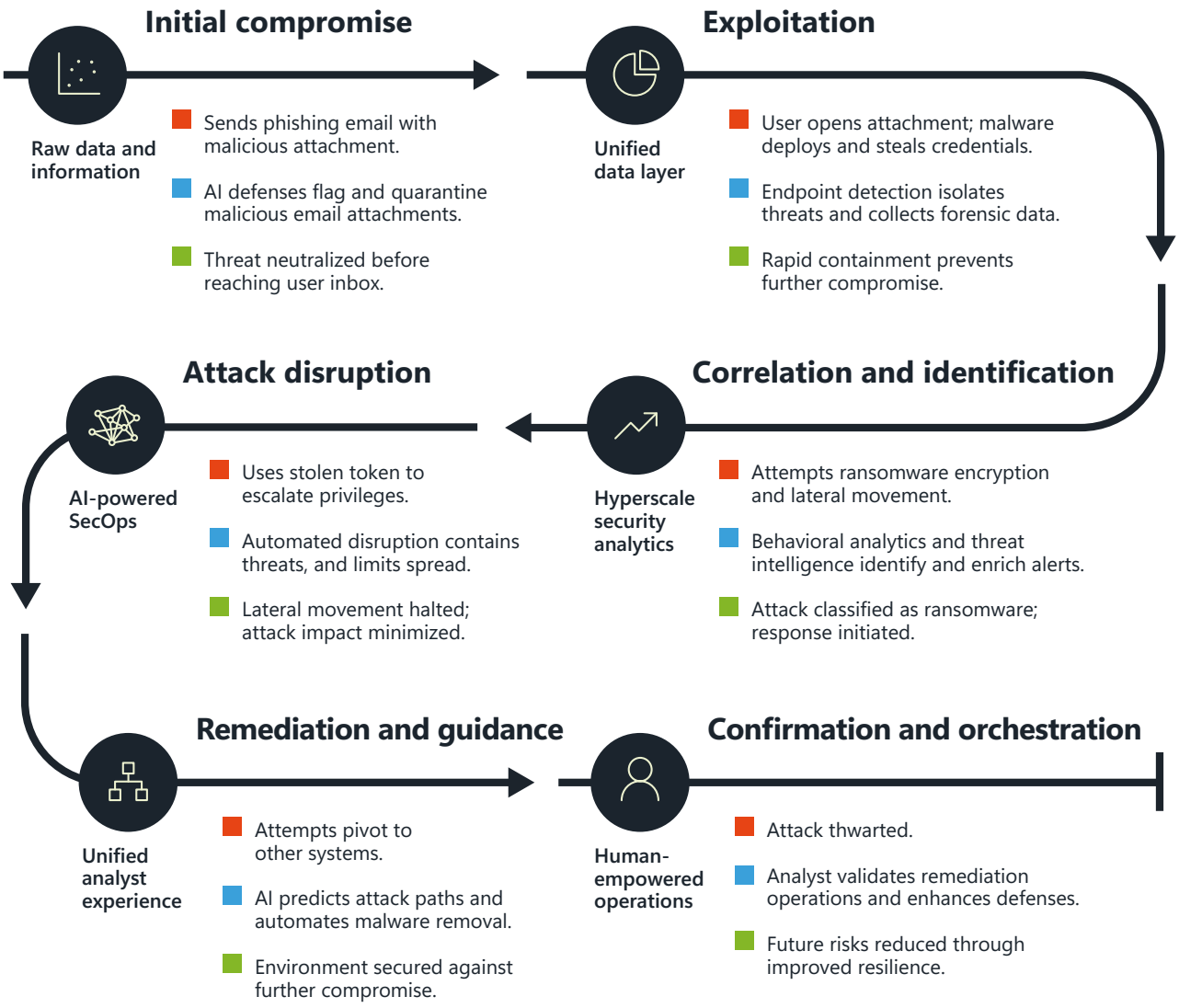
By connecting endpoint security with other defenses, organizations can create a unified approach to protect against ransomware, malware, and unmanaged device vulnerabilities.

LEGEND

- **Attacker Action:** Actions taken by the attacker along potential attack paths.
- **Platform Action:** How the platform responds to specific attacker actions.
- **Outcome:** The result of the platform's response.

Unified endpoint defense: Disrupting ransomware

This diagram shows how a unified security platform can disrupt ransomware attacks at various points. It illustrates potential attack paths and the platform's response to specific attacker actions.



Key considerations for endpoint protection

Explore critical trends shaping endpoint security and strategies to counter ransomware and malware threats.

The rise of ransomware

#1 Ransomware ranks as the top external threat among senior-level IT decision-makers whose primary role is security management.[6]

[6] "The Unified Security Platform Era Is Here," Microsoft, 2024

Solution: **Microsoft Defender for Endpoint** detects and contains ransomware at the device level, stopping lateral movement and encryption attempts. As part of **Microsoft Defender XDR**, it integrates with **Security Copilot** to disrupt attacks within three minutes, providing instant analysis and guided remediation. This coordination ensures endpoint protection aligns with broader, cross-domain defenses.

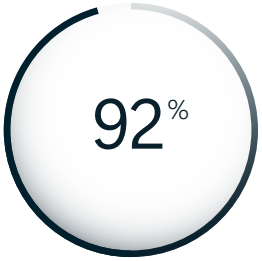
Pervasive malware

775 million malware-laden emails detected last year underscore the ongoing threat of malware.[7]

[7] "Microsoft Digital Defense Report 2024," Microsoft, 2024

Solution: Multilayered defenses analyze threats across email, web, and endpoints before they reach devices. **Defender for Endpoint** blocks malicious content, while **Security Copilot** identifies patterns and automates responses to strengthen defenses against evolving malware threats.

Unmanaged devices as entry points



of successful remote encryption attacks exploit vulnerabilities on unmanaged devices.[8]

[8] "Microsoft Digital Defense Report 2024," Microsoft, 2024

Solution: Automated policy enforcement and continuous monitoring protect unmanaged devices without deploying agents. **Defender for Endpoint** detects threats early, while **Security Copilot** analyzes context and guides remediation to prevent lateral movement and contain risks across your environment.

Move at machine speed against ransomware and malware with **Defender for Endpoint**, a key capability in the **Defender XDR** solution

Scenario 2: Protect identities

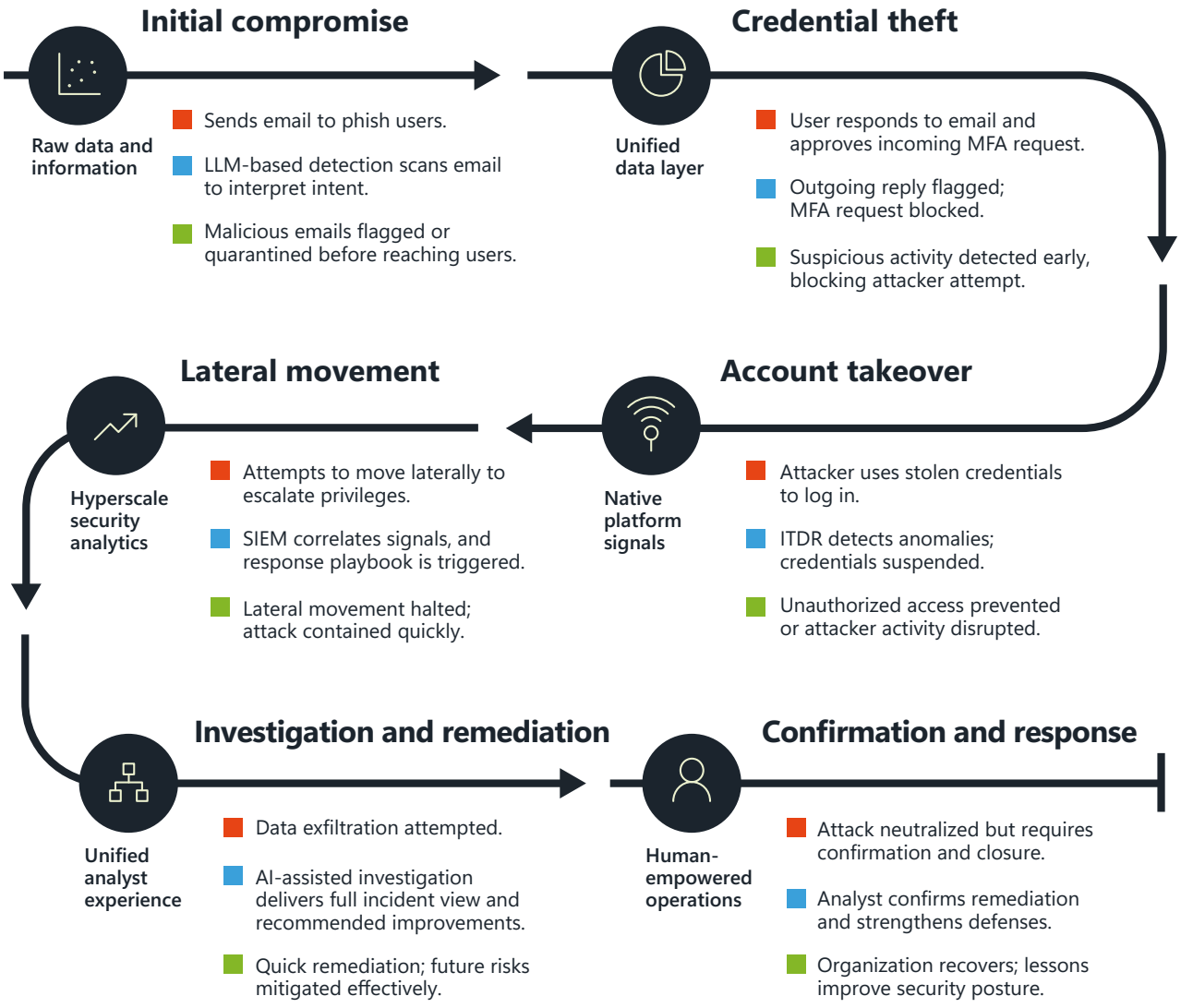
By unifying identity signals, organizations can detect phishing attempts, block credential theft, and prevent lateral movement, ensuring robust protection against account takeovers and insider threats.

LEGEND

- **Attacker Action:** Actions taken by the attacker along potential attack paths.
- **Platform Action:** How the platform responds to specific attacker actions.
- **Outcome:** The result of the platform's response.

Unified identity defense: Disrupting phishing and account takeover

This diagram shows how a unified security platform can disrupt phishing leading to account takeover at various points. It illustrates potential attack paths and the platform's response to specific attacker actions.



Key considerations for identity protection

Understand emerging identity-based threats and learn how unified defenses can prevent account takeovers.

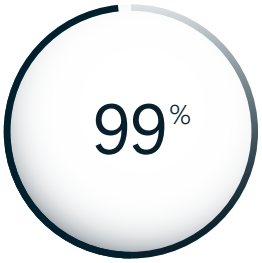
Phishing attacks

#5 Phishing attacks rank as the fifth most significant external threat among senior-level IT decision-makers whose primary role is security management.[9]

[6] "The Unified Security Platform Era Is Here," Microsoft, 2024

Solution: Microsoft's Identity Threat Detection and Response (ITDR) solution analyzes identity signals across your environment to detect stolen credentials in real time. By correlating signals and automating responses, ITDR unifies identity protection to stop threats quickly. **Security Copilot** further strengthens ITDR by containing credential theft incidents and minimizing damage with actionable insights.

Prevalence of password-based attacks

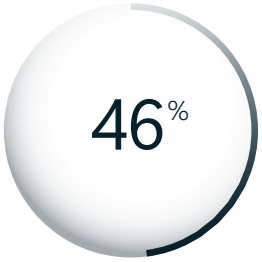


of daily identity attacks are password-based.[10]

[10] "Microsoft Digital Defense Report 2024," Microsoft, 2024

Solution: Microsoft Entra ID Protection, part of Microsoft's ITDR solution, defends against credential-based threats by enabling MFA and passwordless options across your environment. Security Copilot enhances this by monitoring adoption rates and providing recommendations to optimize defenses, ensuring continuous improvement against password-based attacks.

Rise in AiTM phishing attacks



increase in AiTM phishing attacks.[11]

[11] "Microsoft Digital Defense Report 2024," Microsoft, 2024

Solution: By analyzing authentication patterns and identity signals across all identity systems—cloud and on-premises—ITDR can detect sophisticated AiTM phishing attempts. Security Copilot helps investigate these advanced threats and guides teams through rapid response steps to protect user credentials.

Unify your identity signals and disrupt phishing attempts with **Identity Threat Detection and Response (ITDR)**, which integrates capabilities like **Entra ID Protection** for comprehensive account takeover protection

Scenario 3: Secure cloud-native applications

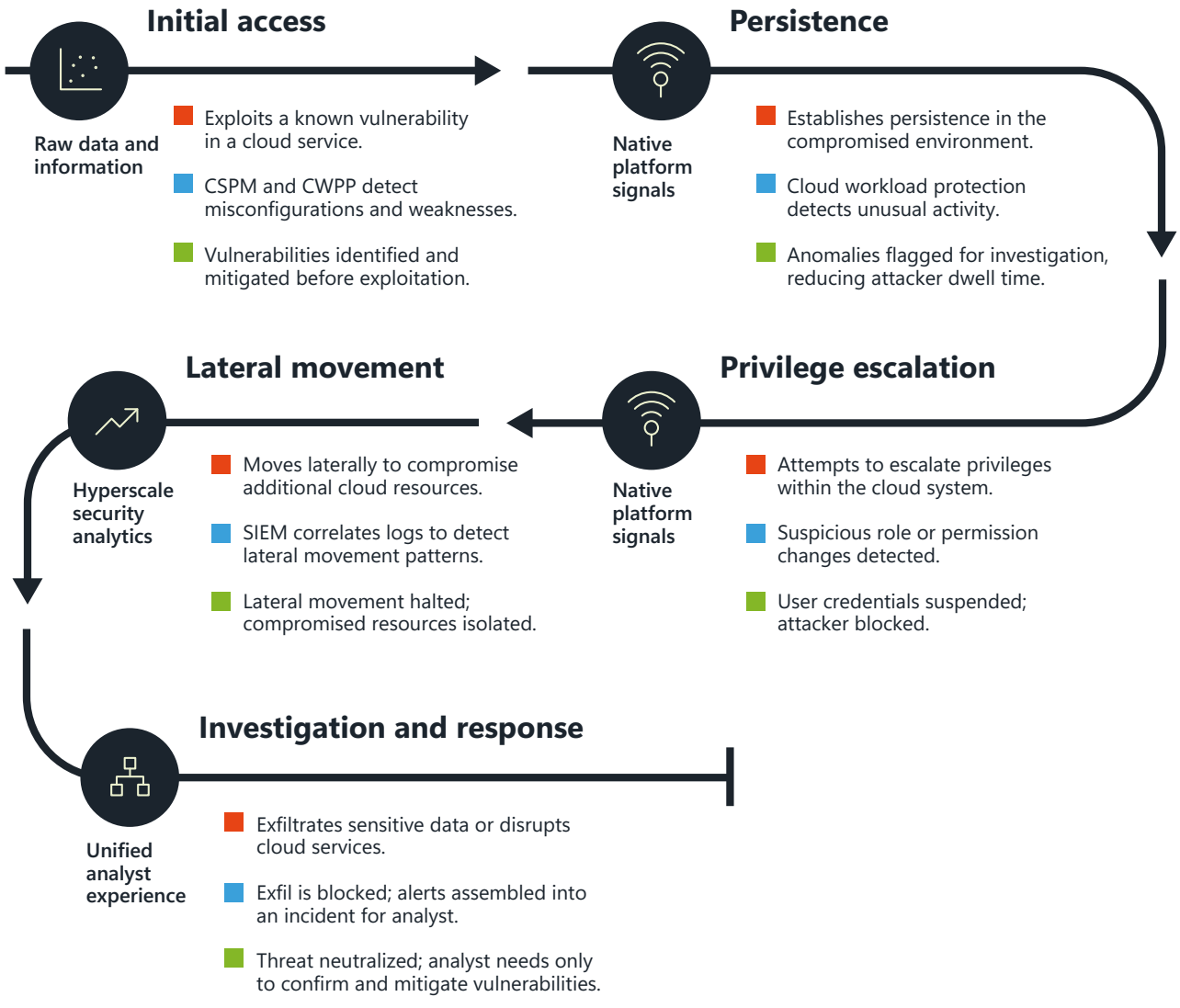
Unified cloud security detects vulnerabilities, blocks privilege escalation, and halts lateral movement, empowering organizations to mitigate risks, contain breaches, and secure critical cloud resources effectively.

LEGEND

- **Attacker Action:** Actions taken by the attacker along potential attack paths.
- **Platform Action:** How the platform responds to specific attacker actions.
- **Outcome:** The result of the platform's response.

Unified cloud security: Disrupting cloud infrastructure compromise

This diagram shows how a unified security platform can disrupt cloud infrastructure compromise attacks at various points. It illustrates potential attack paths and the platform's response to specific attacker actions.



Key considerations for securing cloud-native applications

Gain insights into cloud vulnerabilities and best practices for securing modern application environments.

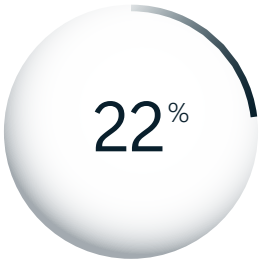
Cloud compromises

#2 Cloud compromises rank as the second most significant external threat among senior-level IT decision-makers whose primary role is security management.[12]

[12] "The Unified Security Platform Era Is Here," Microsoft, 2024

Solution: Microsoft Defender for Cloud unifies protection across your application lifecycle, from code to runtime, in all cloud environments. **Security Copilot** continuously analyzes configurations and automates security controls to prevent compromises.

Cloud vulnerabilities



of organizations had an attack path identified in the cloud.[13]

[13] "Microsoft Digital Defense Report 2024," Microsoft, 2024

Solution: Defender for Cloud creates a unified view of attack paths across your cloud environment. **Security Copilot** prioritizes critical exposures and orchestrates rapid remediation across affected systems.

Loop attack risk

300,000 application servers worldwide are at risk from new 'loop attacks.'[14]

[14] "Microsoft Digital Defense Report 2024," Microsoft, 2024

Solution: Defender for Cloud unifies server protection across environments to block emerging threats like loop attacks. **Security Copilot** learns from attack patterns to automatically strengthen defenses across your server fleet.

Mitigate cloud risks and secure your applications from code to runtime with unified protection from **Defender for Cloud**

Scenario 4: Protect the entire organization with SIEM and XDR

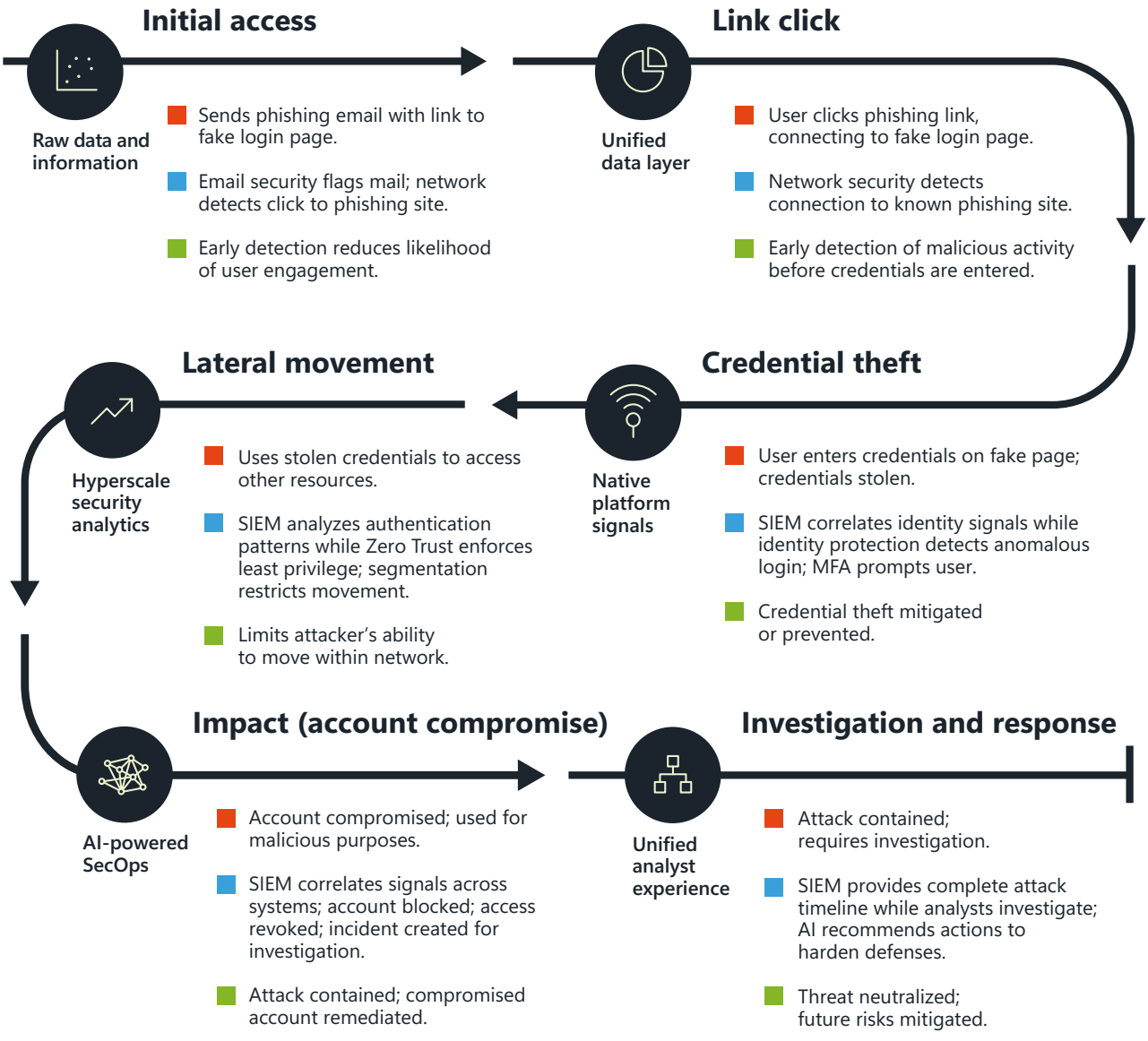
By combining SIEM and XDR in a single platform, security teams get native, platform-level protection from their XDR with the ability to correlate alerts from their existing tools and seamlessly investigate and respond to an incident.

LEGEND

- **Attacker Action:** Actions taken by the attacker along potential attack paths.
- **Platform Action:** How the platform responds to specific attacker actions.
- **Outcome:** The result of the platform's response.

Unified cloud-native security: Disrupting AiTM phishing attacks

This diagram shows how a unified security platform can disrupt adversary-in-the-middle (AiTM) "attacks with a layered defense." It illustrates potential attack paths and the platform's response to specific attacker actions.



Key considerations for integrating SIEM + XDR

Discover how integrated tools can help address advanced persistent threats and reduce false positives.

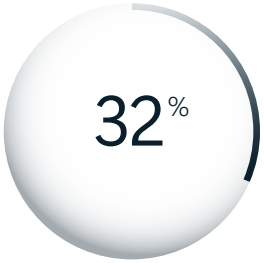
Advanced persistent threats (APTs)

#3 APTs rank as the third most significant external threat among senior-level IT decision-makers whose primary role is security management.[15]

[15] "The Unified Security Platform Era Is Here," Microsoft, 2024

Solution: **Microsoft Sentinel** unifies security signals across clouds and platforms to expose hidden APT patterns. **Security Copilot** maps these complex attack chains and automates response actions across your entire environment.

False positives

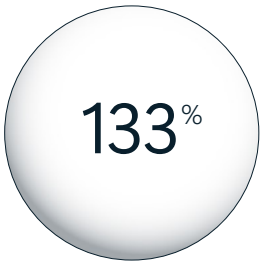


of incidents investigated by SOC teams end up posing no threat.[16]

[16] "Global Security Operations Center Study Results," IBM, March 2023

Solution: Sentinel and Defender XDR dramatically reduce the number of false positives in your alert queues with out-of-box XDR detections.

Expanding attack surface



increase in cyber assets year-over-year.[17]

[17] "Microsoft Digital Defense Report 2024," Microsoft, 2024

Solution: Sentinel provides tailored recommendations to help security engineers enhance coverage and manage costs. Customers who have implemented recommendations have increased their security coverage by up to 17% and were able to increase data utilization by 31%.

Protect your organization with the combined power of **Sentinel** and **Defender XDR**, key components of **Microsoft's unified security platform**

Scenario 5: Protect your data

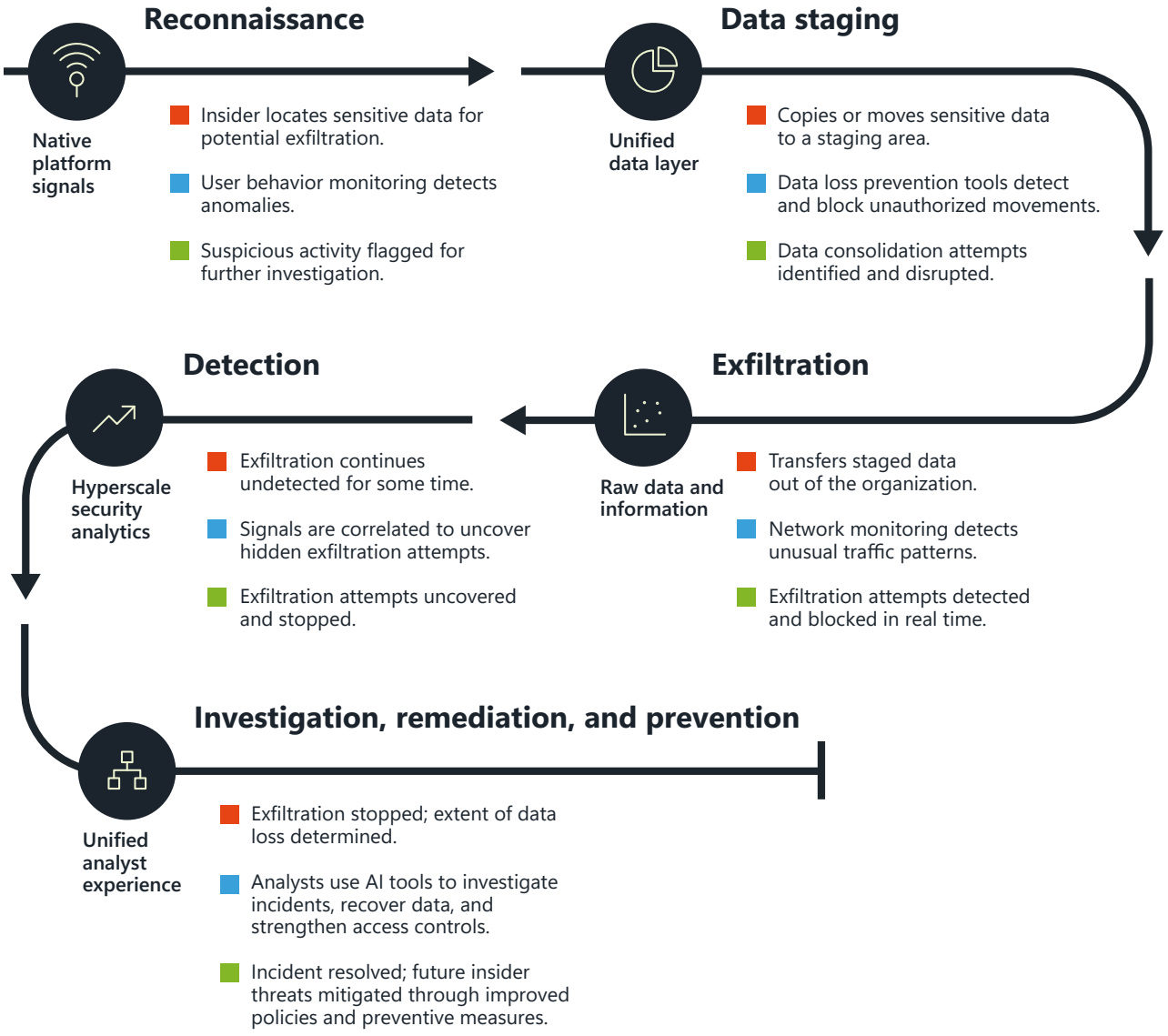
Unified data protection detects insider threats, blocks unauthorized access, and prevents exfiltration, enabling faster investigation, remediation, and stronger safeguards against future breaches across the organization.

LEGEND

- **Attacker Action:** Actions taken by the attacker along potential attack paths.
- **Platform Action:** How the platform responds to specific attacker actions.
- **Outcome:** The result of the platform's response.

Unified data protection: Disrupting insider data exfiltration

This diagram shows how a unified security platform can disrupt insider data exfiltration at various points. It illustrates potential attack paths and the platform's response to specific attacker actions.



Key considerations for protecting your data

Examine key challenges in safeguarding sensitive data and mitigating insider risks effectively.

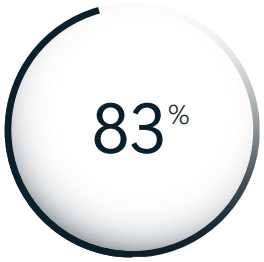
Insider threats

#6 Insider threats rank as the sixth most significant security concern among senior-level IT decision-makers whose primary role is security management.[18]

[18] "The Unified Security Platform Era Is Here," Microsoft, 2024

Solution: Microsoft Purview unifies data protection policies and controls across your organization to expose insider risks. **Security Copilot** identifies suspicious data access patterns and automates protective actions across all environments.

Repeated data breaches



of organizations face repeated breaches.[19]

[19] "Microsoft Digital Defense Report 2024," Microsoft, 2024

Solution: Purview creates consistent data protection across your digital estate through unified controls and policies. **Security Copilot** continuously monitors for gaps and automates improvements to prevent recurring breaches.

Credential exposure

1.5 million credentials were exposed in repositories from January to June 2024.[20]

[20] "Microsoft Digital Defense Report 2024," Microsoft, 2024

Solution: Defender XDR unifies credential monitoring across all identity systems, revealing exposure risks that isolated tools miss. **Security Copilot** automates detection and response to protect credentials across your environment.

Detect insider threats, prevent data exfiltration, and strengthen safeguards with unified data protection policies and controls from **Purview** and advanced credential monitoring from **Defender XDR**

Conclusion

The future of security operations demands a fundamental shift from reactive to proactive defense. A unified SOC architecture makes this possible by:

- Breaking down barriers between security functions
- Enabling AI-powered automation across your environment
- Creating a continuous loop of protection and improvement

Microsoft's integrated security platform delivers this transformation through:

- Real-time threat detection and automated response
- Unified visibility across your entire digital estate
- AI-enhanced investigation and remediation
- Continuous exposure management and security optimization

The result

A security operation that's faster, smarter, and more resilient—ready to protect your organization against today's sophisticated threats and tomorrow's emerging challenges.

Empower your organization with Microsoft's unified security platform

Strengthen your security posture with a unified SOC architecture

Defender XDR
Endpoint protection and credential monitoring

Defender for Endpoint
Multiplatform endpoint detection, response, and ransomware disruption

Sentinel
SIEM and organization-wide security

Entra ID Protection
Identity and access management

Defender for Cloud
Cloud-native application security

Purview
Data protection and governance

Security Copilot
AI-powered analysis and automation across all scenarios

For more details on the data points featured in these infographics, as well as insights into the evolving cyber threat landscape, centering organizations on security, and early insights on AI's impact on cybersecurity, please see the **2024 Microsoft Digital Defense Report**.