Exaforce

Microsoft

MICROSOFT 365 E5 AND EXAFORCE BETTER TOGETHER

Put E5 protection to work across Microsoft 365, Azure, and your wider environment.

SOLUTION BRIEF

The Challenge

Security teams face growing alert volumes and evidence spread across multiple tools. Microsoft 365 E5 provides protection across identities, email, endpoints, and data, but understanding the full scope of a threat often requires connecting Microsoft activity with evidence from other SaaS applications and cloud services.

Analysts must piece together the affected user's access, device posture, application permissions, and subsequent activity across systems. They then need to determine whether that activity reflects normal behavior or a developing attack. Gathering and connecting this evidence takes time, delays response decisions, and leaves less capacity to address high-priority threats.

Better Together

Microsoft provides protection, detections, and controls. Exaforce adds AI agents that continuously triage, investigate, hunt, and coordinate governed response across the connected environment. Exabots combine Microsoft alerts with activity history and current identity, device, application, and cloud context. They assess suspicious activity and present a verdict with supporting evidence, helping teams put more of their E5 investment to work.

Exaforce connects directly to supported Microsoft services and other data sources. E5 detections become the starting point for investigations that follow an identity from a suspicious sign-in to mailbox changes, shared files, and cloud access. Exaforce provides an AI investigation layer on top of an existing SIEM, such as Microsoft Sentinel, adding context and analysis while preserving established SIEM workflows. Microsoft protection and controls remain in place, with response governed by customer policy and required approvals.

KEY HIGHLIGHTS

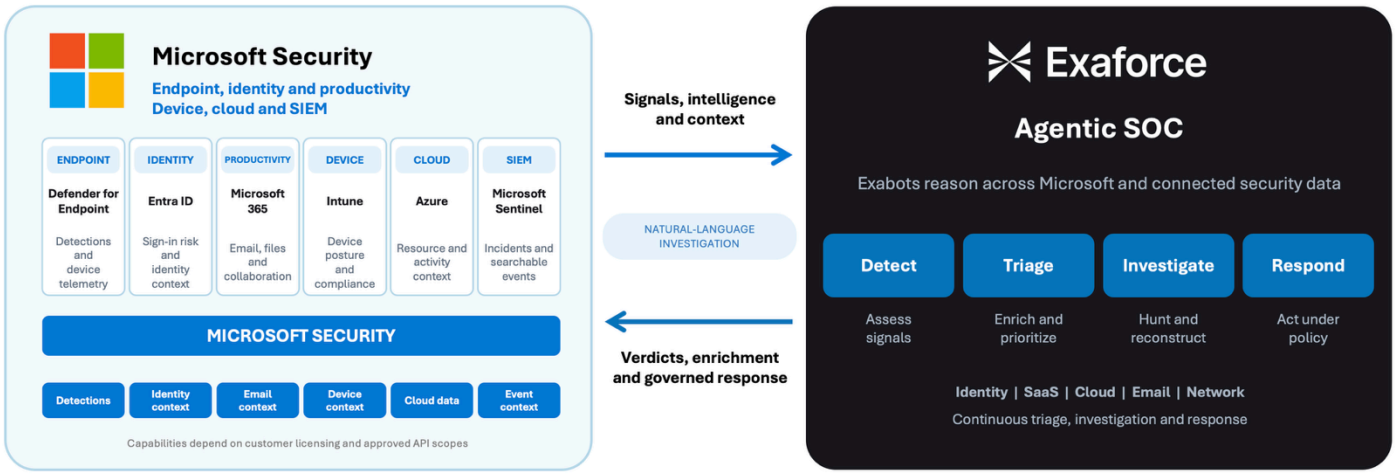
- **Put E5 detections and controls to work with less manual triage**
- **Connect Microsoft 365 activity with identity, device, SaaS, and cloud context**
- **Investigate directly across supported Microsoft and connected data**
- **Review verdicts with the evidence and reasoning behind them**
- **Revoke risky access and remediate harmful changes under policy**

Key Use Cases

USE CASE	JOINT MOTION	BUSINESS VALUE
Autonomous triage of E5 detections	Exabot Triage evaluates supported Defender alerts and incidents, adds identity and asset context from Microsoft and connected tools, and distinguishes benign activity from threats with an evidence-backed rationale.	Put E5 threat protection to work while reducing repetitive review and focusing analysts on threats that need attention.
Natural-language investigation and threat hunting	Ask, "What did this user access after the suspicious sign-in?" Exabots combine Defender hunting data with Entra ID, Microsoft 365 activity, and connected SaaS and cloud evidence.	Scope incidents faster and answer security questions without manually searching each source.
Governed identity and data response	Exabot Respond can revoke Entra ID sessions and delegated OAuth access, remove Microsoft 365 forwarding rules or file-sharing permissions, and update Defender incident status under customer policy.	Use Microsoft controls to limit further access and remove harmful changes while keeping analysts in control of response decisions.

How it works

E5 protection with Exaforce investigation across Microsoft and connected tools



Operational Outcomes

MORE VALUE FROM E5	BROADER CONTEXT	FASTER ANSWERS	GOVERNED RESPONSE
Put licensed signals and controls to work in investigations.	Connect the same user and device across Microsoft and other tools.	Ask security questions in plain language and get answers with evidence.	Apply approved actions with policy controls and human oversight.

Exaforce connects directly to supported Microsoft services and can add an AI investigation layer on top of Microsoft Sentinel. Microsoft Defender and Graph security APIs provide access to incidents, alerts, and hunting data. Broader context comes from workload-specific Microsoft Graph APIs, Microsoft 365 audit APIs, and Azure APIs. Together, these integrations bring identity, mailbox, file, device, and cloud resource evidence into the investigation. For Sentinel deployments, Exaforce combines supported incident data and Log Analytics query results with this direct source context.

Exabots combine available Microsoft evidence with connected SaaS and cloud data to produce a verdict, activity timeline, and recommended next steps. Analysts can ask follow-up questions and review the reasoning before acting. Approved workflows can revoke Entra ID sign-in sessions and delegated OAuth access, disable inbox forwarding, remove file-sharing permissions, and update Defender incident status.

The Integration in Action

Investigating account compromise with E5 and Exaforce

Illustrative workflow and timings using Defender XDR, Entra ID, Microsoft 365, and connected tools

10:14:00

Detect. A Defender for Office 365 alert is correlated into a Defender XDR incident. Exaforce receives the supported incident and evidence directly to begin investigation.

Triage. Exabots examine the message and affected user, then correlate Entra ID sign-ins and endpoint evidence to assess whether the account was compromised.

Scope. Exabots inspect Microsoft 365 mailbox rules, file activity, and sharing permissions, then follow the identity into connected SaaS and Azure resources.

Ask. The analyst asks, "What did this user access after the suspicious sign-in?" Exaforce queries supported Microsoft and connected sources, then returns an answer with evidence.

Verdict. Exaforce presents the activity timeline, affected assets, supporting evidence, and recommended actions for analyst review.

10:19:00

Respond. Under customer policy and required approvals, revoke Entra ID sessions, remove unauthorized OAuth grants or forwarding rules, and update the Defender incident status.

Key integrations across E5 and the Microsoft ecosystem

Exaforce builds on Microsoft's security capabilities to connect evidence, investigate threats, and coordinate approved response actions. The integrations below show how this works across Microsoft 365 E5 and Azure, with support for existing Microsoft Sentinel workflows.

MICROSOFT CAPABILITY	INTEGRATED MOTION	BUSINESS OUTCOME
Microsoft Defender XDR	Use E5 protection from Defender for Endpoint P2, Defender for Office 365 P2, Defender for Identity, and Defender for Cloud Apps. Exaforce triages supported incidents and alerts, queries hunting data, and adds connected-source context.	Extend native Defender investigations across the wider environment and get more operational value from E5 threat protection.
Microsoft Entra ID	Correlate sign-ins, risky identities, audit activity, roles, applications, and OAuth grants. Add identity risk and access context to investigations; approved actions include session revocation and OAuth consent removal.	Turn E5 identity signals into an assessment of who gained access, what they could reach, and how to limit further exposure.
Microsoft 365 and Purview	Combine supported Exchange Online, SharePoint, OneDrive, and Teams activity with identity and sharing context. Purview supplies audit capabilities; Exaforce investigates mailbox and file access.	Determine which mailboxes and files were affected, connect data access to the user, and remediate harmful mailbox or sharing changes under policy.
Microsoft Intune	Add managed-device inventory, compliance, applications, and configuration context. Assign approved management scripts through Intune; execution follows device check-in.	Bring E5 device management context into investigations and support governed remediation through existing Intune workflows.
Microsoft Azure and Defender for Cloud	Combine Azure resource inventory, activity, and access context with supported Defender for Cloud alerts. Follow identities into Azure to assess the resources involved.	Follow a compromised Microsoft identity into Azure and assess the resources and permissions involved in cloud exposure.
Microsoft Sentinel	Build on existing Sentinel connectors, custom detections, retained history, and playbooks. Exaforce investigates supported incidents and queries Log Analytics history alongside direct source context.	Add AI investigation and broader context to existing SIEM workflows while keeping Sentinel detections, retained history, and playbooks in place.

About Exaforce

Exaforce delivers an agentic SOC platform that helps security teams detect, triage, investigate, hunt, and respond to threats. Its task-specific Exabots combine connected security data with transparent reasoning and governed actions, helping analysts spend less time gathering evidence and more time resolving threats. Read our customer case studies, explore the platform, or learn more at exaforce.com.

About Microsoft

Microsoft 365 E5 combines productivity, advanced threat protection, identity, device management, and data security capabilities. Microsoft 365 services, Defender, Entra ID, Intune, and Purview provide protection and context that Exaforce builds on. Azure and Defender for Cloud extend the joint value to cloud resources; Sentinel provides SIEM capabilities that Exaforce complements with AI investigation.

See E5 and Exaforce working together

Explore how your E5 investment becomes evidence-backed investigations and governed actions across Microsoft and connected tools. Visit exaforce.com or scan the code to request a demo.

Joint Solution Brief | REV24 | September 2026.

exaforce.com