BEFORE WE BEGIN

Can anyone guess what this is?

> Decorative uranium glass.
>
> Glass ornaments made of real uranium used as an ornament, because it glows nicely under UV.

> Today's talk is about one of those things that people keep on their shelf.
>
> **Kusto, KQL and Advanced Hunting.**



[ORG-NAME]

Leveraging KQL for agent telemetry in M365

KQL can tell you more about agents,
than the latest "Agentic AI control plane".

Sunny Chakraborty

Ignite NYC Community Summit · 11/16/26

BEFORE WE GET STARTED

There won't be any mention of "AI Control Planes"

Assumptions

- You're tired of hearing about Agentic AI security control planes
- You want to get value from what you already have and not buy something you don't understand
- You are a ***logs first, innovate later*** person
- **License pre-req:** E5/E5+EMS, or Defender for Endpoint P2 with MDCA. Gov/Edu equivalent

Attention is all you need. That includes ours.

Agentic AI security has a new "control plane" every quarter. Meanwhile, MDE, MDCA, Purview, and Entra ID logs sit in our tenants, mostly unexplored.
Let's learn what they do, find the gap, and then explore build/buy.

`CloudAppEvents`

Activity: Who interacted with which AI app, agent and model, and used which data-resource.
Source: MDCA with Microsoft 365 app connector enabled.

`AgentsInfo`

Inventory: Every AI agent running on a managed endpoint, with inventory, MCP and tool-call details.
Source: MDE XDR. MDAV Platform 4.18.2609
AI agent runtime protection requires E7

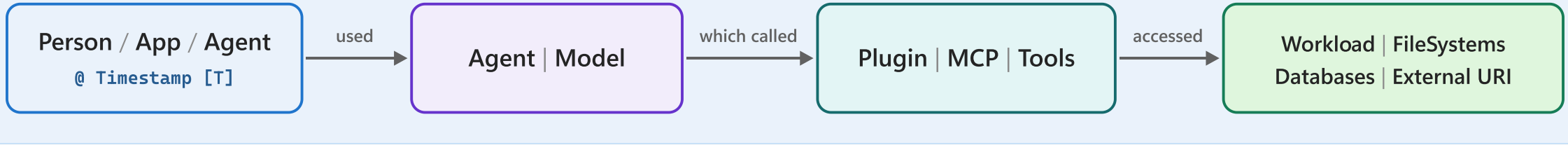
`ExposureGraphNodes` / `ExposureGraphEdges`

Relationships: Users, agents, service principals, OAuth apps and resources as a graph
Source: MDE Exposure management

THE BILLY BEANE QUESTION

What is the problem?

Map



1 Interaction

Map who, what, when and how for AI use in Microsoft 365: which user, used which plugin, to which agent and model, to which resources.

2 Local agents

Find the AI coding agents, desktop assistants and MCP servers running on devices onboarded to Defender for Endpoint. Then unwrap which tools and third parties they call.

3 Relationships

Walk the graph from users to agents to service principals and OAuth apps. Ask what each agent uses and what it can authenticate as. `ExposureGraphNodes` and `ExposureGraphEdges`.

We are LOGS-PEOPLE: You can't take over an infrastructure with AI, and not leave any logs.

To quote **Agent-K from Men in Black.** *He's not leaving the planet in a cab.*

PART ONE

Microsoft Defender for Cloud Apps (MDCA)

CloudAppEvents already records every SaaS agent interaction

KUSTO · CLOUDAPPEVENTS

Summary of AI interactions: Mapping AI tool to calling workload

KQL-01 Interaction volume by action, activity, source workload and AI workload

```
let _atype = pack_array("CopilotInteraction","ExecutedCopilotQuery","GetCopilotSettingsForEnvironment","InitializeStructuredDataCopilot","Register
Microsoft.SecurityCopilot","RequestCopilot","TeamCopilotMsgInteraction");
let _window = 1d;
let _limits = 1000;
CloudAppEvents
| where Timestamp > ago(_window)
| where ActionType in (_atype)
| extend _raw = parse_json(RawEventData), _activity = parse_json(ActivityObjects)
| extend Workload = tostring(_raw.Workload), Operation = tostring(_raw.Operation), CoPEvents = parse_json(_raw.CopilotEventData)
| extend _model_details = CoPEvents.ModelTransparencyDetails[0], SrcWorkload = Workload
| extend ModelProviderName = CoPEvents.ModelTransparencyDetails[0].["ModelProviderName"], AIWorkLoad = tostring(CoPEvents.AppHost), Plugins = tostring(CoPEvents.AISystemPlugin), DataResource =
CoPEvents.AccessedResources
| project Timestamp,AccountDisplayName, ActionType, ActivityType, Application, ModelProviderName, SrcWorkload, AIWorkLoad,Plugins,DataResource
| summarize Count = count() by ActionType, ActivityType, SrcWorkload, AIWorkLoad
```

ActionType	ActivityType	SrcWorkload	AIWorkLoad	Count
CopilotInteraction	Interactwithcopilot	Copilot	Edge	1266
CopilotInteraction	Interactwithcopilot	Copilot	Autonomous	17571
CopilotInteraction	Interactwithcopilot	Copilot	Office	16658
CopilotInteraction	Interactwithcopilot	Copilot	Teams	1094
CopilotInteraction	Interactwithcopilot	Copilot	SharePoint	60
CopilotInteraction	Interactwithcopilot	Copilot	Outlook	724
CopilotInteraction	Interactwithcopilot	Copilot	Microsoft Teams	310

ActionType	ActivityType	SrcWorkload	AIWorkLoad	Count
CopilotInteraction	Interactwithcopilot	Copilot	OutlookSidepane	2222
RequestCopilot	Basic	PowerBI		2353
CopilotInteraction	Interactwithcopilot	Copilot	cowork	3548
CopilotInteraction	Interactwithcopilot	Copilot	Power BI	238
CopilotInteraction	Interactwithcopilot	Copilot	OfficeCopilotSear...	26
CopilotInteraction	Interactwithcopilot	Copilot	Copilot Studio	151
CopilotInteraction	Interactwithcopilot	Copilot	Fabric AI Hub	156

KUSTO · CLOUDAPPEVENTS

Trace AI interaction from user to model to data

KQL-02 AI and agent interaction activity logs

```
let _atype = pack_array("CopilotInteraction","ExecutedCopilotQuery","GetCopilotSettingsForEnvironment","InitializeStructuredDataCopilot","Register
Microsoft.SecurityCopilot","RequestCopilot","TeamCopilotMsgInteraction");
let _window = 1d;
let _limits = 1000;
CloudAppEvents
| where Timestamp > ago(_window)
| where ActionType in (_atype)
| extend _raw = parse_json(RawEventData), _activity = parse_json(ActivityObjects)
| extend Workload = tostring(_raw.Workload), Operation = tostring(_raw.Operation), CoPEvents = parse_json(_raw.CopilotEventData)
| extend _model_details = CoPEvents.ModelTransparencyDetails[0], SrcWorkload = Workload
| extend ModelProviderName = CoPEvents.ModelTransparencyDetails[0].["ModelProviderName"], AIWorkLoad = CoPEvents.AppHost, Plugins = CoPEvents.AISystemPlugin, DataResource = CoPEvents.AccessedResources
| project Timestamp,AccountDisplayName, ActionType, Application, ModelProviderName, SrcWorkload, AIWorkLoad,Plugins,DataResource
| take _limits
```

Timestamp	AccountDisplayName	ActionType	Application	ModelProvide…	SrcWorkload	AIWorkLoad	Plugins	DataResource
11/13/2026 7:48	SVCACCOUNT1	CopilotInteraction	Microsoft 365 Copilot Chat		Copilot	Autonomous		[{"Id":"8d3865a3-f38e-4311-bff7-acd630355479",…
11/13/2026 7:43	SVCACCOUNT1	CopilotInteraction	Microsoft 365 Copilot Chat		Copilot	Autonomous		[{"Id":"80c60546-ce60-41ee-a855-c39a60664378",…
11/13/2026 14:14	John Doe	CopilotInteraction	Microsoft 365 Copilot Chat	OpenAI	Copilot	Office	[{"Id":"BingWebSearch","Name":"BuiltIn"…	[{"SiteUrl":"https://example.com","A…
11/13/2026 12:06	Jane Doe	CopilotInteraction	Microsoft 365 Copilot Chat	OpenAI	Copilot	Office	[{"Id":"BingWebSearch","Name":"BuiltIn"…	[{"SiteUrl":"https://example.com…
11/13/2026 7:25	Alex Bennett	CopilotInteraction	Microsoft 365 Copilot Chat	OpenAI	Copilot	Teams	[{"Id":"BingWebSearch","Name":"BuiltIn"…	[{"SiteUrl":"https://example.com…
11/13/2026 10:01	Taylor Bennett	CopilotInteraction	Microsoft 365 Copilot Chat	Anthropic	Copilot	cowork	[{"Id":"TaskCreate","Name":"TaskCreate"…	[{"Id":"AAMkAGZkZjJiZTM3LWI3MTgtNDAxMC1hYWRjLW…
11/13/2026 10:40	Morgan Bennett	CopilotInteraction	Microsoft 365 Copilot Chat	OpenAI	Copilot	Office	[{"Id":"BingWebSearch","Name":"BuiltIn"…	[{"SiteUrl":"https://example.com…
11/13/2026 10:45	SVCACCOUNT2	CopilotInteraction	Microsoft 365 Copilot Chat		Copilot	Autonomous		[{"Id":"0f05f768-d267-470c-b6e1-dc6c4a4fe0d8",…
11/13/2026 7:42	SVCACCOUNT4	CopilotInteraction	Microsoft 365 Copilot Chat		Copilot	Autonomous		[{"Id":"398ba376-012f-4ba3-a143-6d0c9477338e",…
11/13/2026 11:40	Casey Bennett	CopilotInteraction	Microsoft 365 Copilot Chat	OpenAI	Copilot	Office	[{"Id":"BingWebSearch","Name":"BuiltIn"…	[{"SiteUrl":"https://example.com…
11/13/2026 10:02	SVCACCOUNT2	CopilotInteraction	Microsoft 365 Copilot Chat		Copilot	Autonomous		[{"Id":"fd78a246-5e45-45e4-a2b3-a5a78a657419",…
11/13/2026 7:43	SVCACCOUNT5	CopilotInteraction	Microsoft 365 Copilot Chat		Copilot	Autonomous		[{"SiteUrl":"Microsoft Security for AI RTP","I…
11/13/2026 11:50	Parker Bennett	CopilotInteraction	Microsoft 365 Copilot Chat	OpenAI	Copilot	Office	[{"Id":"BingWebSearch","Name":"BuiltIn"…	[{"SiteUrl":"https://example.com…
11/13/2026 10:45	Jamie Bennett	CopilotInteraction	Microsoft 365 Copilot Chat	OpenAI	Copilot	Edge	[{"Id":"BingWebSearch","Name":"BuiltIn"…	[{"SiteUrl":"https://example.com…
11/13/2026 10:37	SVCACCOUNT2	CopilotInteraction	Microsoft 365 Copilot Chat		Copilot	Autonomous		[{"Id":"9bc2322d-f871-41eb-aa92-33e39aff5395",…
11/13/2026 10:34	SVCACCOUNT2	CopilotInteraction	Microsoft 365 Copilot Chat		Copilot	Autonomous		[{"Id":"aee66e5c-3fe0-4509-ae59-af9efacba88a",…
11/13/2026 7:23	SVCACCOUNT2	CopilotInteraction	Microsoft 365 Copilot Chat		Copilot	Autonomous		[{"Id":"39fb1f40-aba4-4709-993a-825c93af761a",…
11/13/2026 9:55	Reese Bennett	CopilotInteraction	Microsoft 365 Copilot Chat	OpenAI	Copilot	Office	[{"Id":"BingWebSearch","Name":"BuiltIn"…	[{"SiteUrl":"https://example.com…
11/13/2026 7:25	SVCACCOUNT2	CopilotInteraction	Microsoft 365 Copilot Chat		Copilot	Autonomous		[{"Id":"0180bdd1-df25-4ee9-a848-989ada3653f6",…

PART TWO

LocalAgents: MDE XDR and MDAV (Microsoft Defender Antivirus)

Coding agents, desktop assistants and MCP servers running on managed endpoints, with the user's permissions

LOCAL AI AGENT DISCOVERY USING MDE

MDE already inventories agents on endpoints (Windows and macOS)

CLI AGENTS

Terminal-native

- Claude Code
- Codex CLI
- Gemini CLI
- GitHub Copilot CLI

DESKTOP APPS

Assistants

- ChatGPT Desktop
- Claude Desktop
- Ollama Desktop
- Perplexity Desktop

AGENTIC IDES

Editors with agency

- Cursor
- Kiro IDE
- Antigravity IDE
- Devin Desktop

VS CODE EXTENSIONS

Inside the IDE

- GitHub Copilot
- Cline · Roo Code
- Codex · Claude Code
- Gemini Code Assist

MCP SERVERS

What agents can reach

- Local and remote MCP server configs
- Tied to the discovered agent, device and account

Prerequisites. Defender for Endpoint P2, commercial cloud, supported Windows or macOS build. MCP config discovery needs Defender Antivirus in active mode with real-time protection. Results land in the AI agent inventory and in `AgentsInfo`.

What's included.

- **Agent-native event inspection:** Using vendor-supported hook interfaces / lifecycle hooks. (Claude Code, GH CLI, GH Copilot, Claude Desktop in Code mode, VS Code with GH Copilot and Claude Code extension)
- **Network inspection:** Agent communication with LLMs. (Exclusion: Cert-pinning, HTTP/3)

Sources: Discover local AI agents · Local AI agent discovery overview · Coverage map (60+ platforms) | Support matrix

KUSTO · AGENTSINFO

Coding agents: Estate summary

KQL-03 Agent inventory by user and device

```
let _window = 7d;
AgentsInfo
| where Timestamp > ago(_window)
| where Platform == "LocalAgents"
| summarize arg_max(Timestamp, Name, Version, LifecycleStatus, RawAgentInfo) by AgentId
| where LifecycleStatus !in~ ("Deleted", "Uninstalled")
| extend AgentMetadata = RawAgentInfo.localAgentMetadata
| extend Vendor = tostring(AgentMetadata.vendor), Process = tostring(AgentMetadata.relatedProcess), Device = tostring(AgentMetadata.deviceName), Account = tostring(AgentMetadata.accountName)
| summarize Installations = count(),DeviceCount = dcount(Device),Devices = make_set(Device, 100),Versions = make_set(Version, 20) ,Accounts = make_set_if(Account, isnotempty(Account), 50) by Agent = Name,
Vendor, Process
| sort by DeviceCount desc, Installations desc
```

Agent	Vendor	Process	Installations	DeviceCount	Versions
Claude Code	Anthropic	claude.exe	5000	3000	["2.1.319.0","2.1.318.0","2.1.322.0","2.1.296.0","1.0","2.1.323.0","","2.1.321.0"…
Codex CLI	OpenAI	codex.exe	274	273	["","1.0"]
GitHub Copilot CLI	GitHub	copilot.exe	234	234	["1.0.110","1.0.109","1.0.107","1.0.106","1.0.108","1.0.102-0.unstable.r417799009…
Codex CLI	OpenAI	codex	78	78	["0.169.0","1.0","","0.164.0","0.167.0","0.166.0","0.167.1","0.168.0","0.167.2","…
VSCode GitHub Copilot Extension	GitHub	code.exe	36	35	["1.388.0","1.372.0","0.37.8","0.36.2","0.44.1","0.48.1","0.45.1","0.32.5","0.23.…
Claude Desktop	Anthropic	claude.exe	34	34	["4.29.0","2.9939.2","4.4212.0","4.23118.0","5.11492.5","5.1231.2","1.52386.6"]
GitHub Copilot App	GitHub	github.exe	13	13	["1.1.33","1.1.30","1.1.11","1.1.35","1.0.13","1.1.23","1.1.34"]

KUSTO · AGENTSINFO

Coding agents: Local and Remote MCP server discovery with transport

KQL-04 Remote MCP servers in use

```
let _window = 7d;
let localAgentProfiles = AgentsInfo | where Platform == "LocalAgents" | extend AgentMetadata = RawAgentInfo.localAgentMetadata
    | project Timestamp,Agent = Name, Device = tostring(AgentMetadata.deviceName), Account = tostring(AgentMetadata.accountName),McpServers,DeclaredTools,LocalServers = AgentMetadata.localMcps;
let remoteMcpServers = localAgentProfiles | mv-expand Server = McpServers
    | project Timestamp, Agent, Device, Account,McpServer = tostring(Server.name),Origin = "Remote MCP server",Transport = tostring(Server.type),Location = tostring(Server.endpoint);
let agentDeclaredTools = localAgentProfiles | mv-expand Tool = DeclaredTools
    | project Timestamp, Agent, Device, Account,McpServer = tostring(Tool.name),Origin = "Declared tool",Transport = tostring(Tool.type),Location = tostring(Tool.endpoint);
let localMcpServers = localAgentProfiles | mv-expand Server = LocalServers
    | project Timestamp, Agent, Device, Account,McpServer = tostring(Server.name),Origin = "Local MCP server",Transport = tostring(Server.transportType),Location = tostring(Server.commandName);
remoteMcpServers
| union agentDeclaredTools, localMcpServers
| where isnotempty(McpServer)
| summarize LastSeen = max(Timestamp),Agents = make_set(Agent, 20),Devices = make_set(Device, 20), Accounts = make_set_if(Account, isnotempty(Account), 20) by McpServer, Origin, Transport, Location
| sort by McpServer asc, Origin asc
```

McpServer	Origin	Transport	Location	Agents
Atlassian MCP Server	Remote MCP serv…	sse	https://examp…	["Claude Code","GitHub Copilot CLI"]
Chrome DevTools MCP	Local MCP server	stdio	npx	["GitHub Copilot CLI"]
Playwright MCP	Local MCP server	stdio	powershell.exe	["GitHub Copilot CLI","Claude Code"]
Playwright MCP	Local MCP server	stdio	cmd	["Claude Code","GitHub Copilot CLI"]
Playwright MCP	Local MCP server	stdio	npx	["Claude Code","GitHub Copilot CLI"]
Playwright MCP	Local MCP server	stdio	powershell	["GitHub Copilot CLI"]
Playwright Test MCP	Local MCP server	stdio	npx	["Claude Code"]
angular-cli	Local MCP server	stdio	npx	["Codex CLI","Claude Code"]
apple-docs	Local MCP server	stdio	npx	["Claude Code","Codex CLI"]
browser-use	Local MCP server	stdio	node	["GitHub Copilot CLI","GitHub Copil…
chrome-devtools	Local MCP server	stdio	npx	["GitHub Copilot CLI","Claude Code"]
chrome-devtools-mcp	Local MCP server	stdio	npx	["Codex CLI"]
code-review	Local MCP server	stdio	/bin/sh	["ChatGPT Desktop","Codex CLI"]

McpServer	Origin	Transport	Location	Agents
codex-security	Local MCP server	stdio	node	["Codex CLI","Claude Code"]
discord	Local MCP server	stdio	bun	["Claude Code"]
fakechat	Local MCP server	stdio	bun	["Claude Code"]
filesystem	Local MCP server	stdio	npx	["Claude Code"]
github	Local MCP server	stdio	npx	["Claude Code"]
github	Remote MCP serv…	sse	https://examp…	["Claude Code"]
github-copilot-brows…	Local MCP server	stdio	node	["GitHub Copilot CLI"]
mcp-search	Local MCP server	stdio	node	["Claude Code","GitHub Copilot CLI…
mongodb	Local MCP server	stdio	npx	["Claude Code"]
playwright-test	Local MCP server	stdio	npx	["GitHub Copilot CLI","Codex CLI","…
playwright-test	Local MCP server	stdio	powershell.exe	["Claude Code"]
playwright-test	Local MCP server	stdio	cmd	["GitHub Copilot CLI"]

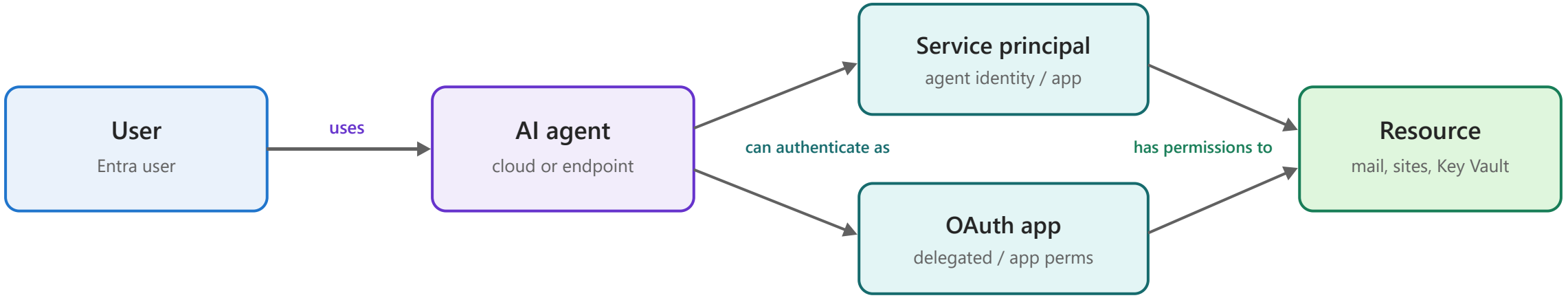
PART THREE

Attackers think in graphs. Defenders *also* think in graphs.

Exposure Management: Users, agents, service principals and OAuth apps

THE RELATIONSHIP MODEL

Two questions per agent: who uses it, and what can it authenticate as



Nodes live in `ExposureGraphNodes` (`NodeLabel` , `Categories` , `NodeProperties`). **Edges** live in `ExposureGraphEdges` (`SourceNodeId` , `EdgeLabel` , `TargetNodeId`).

Sources: Microsoft Learn, ExposureGraphEdges · ExposureGraphNodes · Query the enterprise exposure graph

KUSTO · EXPOSUREGRAPH

Graph: MCP server to vendor, agent, auto-approval by distinct users and devices

KQL-05 Mapping reach of specific MCP servers with auto-approve

```
let riskyAgentProfiles =
    AgentsInfo | where Platform == "LocalAgents"
    | summarize arg_max(Timestamp, Name, Version, LifecycleStatus, RawAgentInfo) by AgentId
    | where LifecycleStatus !in~ ("Deleted", "Uninstalled")
    | extend AgentMetadata = RawAgentInfo.localAgentMetadata
    | extend AutoApprove = tostring(AgentMetadata.autoApprove), TrustedProcess = tostring(AgentMetadata.trustedProcess)
    | where AutoApprove =~ "true" or TrustedProcess =~ "false"
    | project AgentId = tostring(AgentId), Agent = Name, Version, Vendor = tostring(AgentMetadata.vendor),Account = tostring(AgentMetadata.accountName), AutoApprove, TrustedProcess;
let localAgentNodes = ExposureGraphNodes | where NodeLabel == "ai-agent"
    | where tostring(NodeProperties.rawData.aiAgentMetadata.platform) == "LocalAgents"
    | project AgentNodeId = NodeId, AgentId = tostring(NodeProperties.rawData.aiAgentMetadata.id);
let agentDeviceEdges = ExposureGraphEdges | where SourceNodeLabel == "ai-agent"
    | project AgentNodeId = SourceNodeId, DeviceId = TargetNodeId, Device = TargetNodeName, DeviceType = TargetNodeLabel;
riskyAgentProfiles
| join kind=inner localAgentNodes on AgentId
| join kind=inner agentDeviceEdges on AgentNodeId
| where DeviceType == @'mcp/server' | extend MCPServer = Device
| summarize DistinctUsersCount = dcount(Account), DistinctDevices = dcount(DeviceId) by MCPServer, DeviceType, Vendor, Agent, Version, AutoApprove, TrustedProcess
```

MCPServer	DeviceType	Vendor	Agent	Version	AutoApprove	TrustedProcess	DistinctUsersCount	DistinctDevices
context7	mcp/server	Anthropic	Claude Code	2.1.318.0	TRUE	TRUE	18	1
Atlassian MCP Server (Streamable HTTP)	mcp/server	Anthropic	Claude Code	1	TRUE	FALSE	2	1
context7	mcp/server	Anthropic	Claude Code	2.1.322.0	TRUE	TRUE	10	1
figma	mcp/server	Anthropic	Claude Code	1	TRUE	TRUE	9	1
figma	mcp/server	Anthropic	Claude Code	1	FALSE	FALSE	8	1
atlassian	mcp/server	Anthropic	Claude Code	1	TRUE	TRUE	8	3
context7	mcp/server	Anthropic	Claude Code	2.1.319.0	TRUE	TRUE	7	1
atlassian	mcp/server	Anthropic	Claude Code	1	FALSE	FALSE	6	3
github	mcp/server	Anthropic	Claude Code	1	FALSE	FALSE	6	2
github	mcp/server	OpenAI	Codex CLI		TRUE	TRUE	5	2

KUSTO · EXPOSUREGRAPH

Graph: AgentId to vendor, agentic tool, auto-approval by distinct users and devices

KQL-06 With AgentId, user and device details

```
let riskyAgentProfiles =
    AgentsInfo | where Platform == "LocalAgents"
    | summarize arg_max(Timestamp, Name, Version, LifecycleStatus, RawAgentInfo) by AgentId
    | where LifecycleStatus !in~ ("Deleted", "Uninstalled") | extend AgentMetadata = RawAgentInfo.localAgentMetadata
    | extend AutoApprove = tostring(AgentMetadata.autoApprove), TrustedProcess = tostring(AgentMetadata.trustedProcess)
    | where AutoApprove =~ "true" or TrustedProcess =~ "false" | project AgentId = tostring(AgentId), Agent = Name, Version, Vendor = tostring(AgentMetadata.vendor), Account =
tostring(AgentMetadata.accountName), AutoApprove, TrustedProcess;
let localAgentNodes = ExposureGraphNodes | where NodeLabel == "ai-agent"
    | where tostring(NodeProperties.rawData.aiAgentMetadata.platform) == "LocalAgents"
    | project AgentNodeId = NodeId, AgentId = tostring(NodeProperties.rawData.aiAgentMetadata.id);
let agentDeviceEdges = ExposureGraphEdges | where SourceNodeLabel == "ai-agent"
    | project AgentNodeId = SourceNodeId, DeviceId = TargetNodeId, Device = TargetNodeName, DeviceType = TargetNodeLabel;
riskyAgentProfiles
| join kind=inner localAgentNodes on AgentId
| join kind=inner agentDeviceEdges on AgentNodeId
| where DeviceType == @'mcp/server'
```

AgentId	AutoApprove	Agent	Version	Vendor	TrustedProcess	DeviceType
c21061c1-65ad-4…	TRUE	GitHub Copilot CLI	1.0.105	GitHub	TRUE	user
86867991-9413-4…	FALSE	Claude Code		Anthropic	FALSE	mcp/server
a21771ab-0d0f-4…	TRUE	Claude Code	2.1.325.0	Anthropic	TRUE	user
8f2cbe4d-36ce-4…	FALSE	Claude Code	1	Anthropic	FALSE	mcp/server
8f2cbe4d-36ce-4…	FALSE	Claude Code	1	Anthropic	FALSE	mcp/server
cdc9673c-943c-4…	TRUE	Claude Code	2.1.322.0	Anthropic	TRUE	user
adfd079d-3f85-4…	TRUE	Claude Code	2.1.318.0	Anthropic	TRUE	user
3de05f2e-fb6b-4…	TRUE	Claude Code	2.1.323.0	Anthropic	TRUE	user
cad3a130-d250-4…	TRUE	Claude Code	2.1.296.0	Anthropic	TRUE	user
f478d823-395c-4…	TRUE	Claude Code	2.1.322.0	Anthropic	TRUE	mcp/server

AgentId	AutoApprove	Agent	Version	Vendor	TrustedProcess	DeviceType
2f9182d1-bb5d-4…	TRUE	Claude Code	2.1.318.0	Anthropic	TRUE	user
9430cc58-d61f-4…	TRUE	GitHub Copilot CLI	1.0.110	GitHub	TRUE	user
154efa98-4c00-4…	FALSE	Claude Code	2.1.318.0	Anthropic	TRUE	user
93421e50-01f3-4…	TRUE	Claude Code	2.1.229.0	Anthropic	TRUE	user
66b57b87-0e10-4…	TRUE	Claude Code	2.1.323.0	Anthropic	TRUE	user
b96ac28f-2efe-4…	TRUE	Claude Code	2.1.162.0	Anthropic	TRUE	user
aff472bd-e425-4…	TRUE	Claude Code	2.1.112	Anthropic	FALSE	mcp/server
aff472bd-e425-4…	TRUE	Claude Code	2.1.112	Anthropic	FALSE	mcp/server
cd4b27a9-6227-4…	TRUE	Claude Code	2.1.325.0	Anthropic	TRUE	mcp/server
cd4b27a9-6227-4…	TRUE	Claude Code	2.1.325.0	Anthropic	TRUE	mcp/server

PART FOUR

Defining an agent. Agents need an identity.

You can vibe-code an agent. *You can't vibe-log.*

WHAT IS AN AGENT

Franklin & Graesser definition of agents (1996)

Three core characteristics of an agent

An autonomous agent is a system situated within and a part of an environment that senses that environment and acts on it, over time, in pursuit of its own agenda and so as to effect what it senses in the future.

- **Situatedness:** perceives an environment; takes input from it.
- **Actuation:** has the capacity to act back on that environment.
- **Goal-directedness:** actions are selected because they're evaluated against an objective, not emitted as a hardwired stimulus-response.

We also need

- Autonomy of control flow
- Generality of policy
- Open-endedness of environment
- Degree of statefulness

How is this different from a workflow?

Autonomy of control flow: An agent's **own policy dynamically decides which actions to take, in what order, and when to stop.**

- In a workflow, and in a thermostat's fixed sense-compare-actuate cycle, those decisions are hardcoded by a human in advance.
- An agent's actions are an effort to control its own trajectory.

Source: Franklin and Graesser, "Is it an Agent, or just a Program?", Proceedings of the Third International Workshop on Agent Theories, Architectures, and Languages, Springer-Verlag, 1996

AN AGENT WITHOUT A TYPE IS JUST A GUID

Should be able to distinguish an agent from a {user, svcAcc, SP, process}.

We need `ObjectType=Agent` just like we have `ObjectType=User`

Identity type is instantiated at creation.

- Purpose of an identity in an IdP is not inferred, it's assigned.
- An agent ID is not a user, a computer, a gMSA, an App ID, a SID or a GUID free of an IdP.

Questions to ask:

- How many users do you have?
- How many agents do you anticipate in your env in 2026?
- What about 2029?
- What do you think an agent lifecycle is (mm, hh, dd)? Or do you think agents are persistent like a User/AppId?

Lifecycle and velocity of agents are different from users and apps

How much time will it take your pwsh script to delete 1,000,000 agent identities from Entra ID with a lifetime of 5 minutes?

All controls are geared towards remediating a "misaligned agent", but what does remediation mean?

- Kill an OAuth2 session?
- Delete an identity in an IdP like Entra ID?
- Stop a process? Reboot a machine, VM, K8s pod?

The test: can your SIEM, DLP and proxy tell an agent's action from a user's and an app's without a lookup table you maintain by hand? If not, you don't have an agent type. You have a naming convention.

DELEGATION VS. IDENTITY

On-behalf-of extends your blast radius. Entra ID agent blueprints contain it.

Agent acting on-behalf-of the user

- The token's subject is the user. The agent is recorded only as the actor in logs.
- The agent's reach is the user's delegated reach, every scope that was consented
- Agent and user activity is indistinguishable during investigation
- One compromised, misaligned or prompt-injected agent inherits every user entitlement

Agent with a blueprint-backed identity

- Credentials live on the blueprint, not scattered across instances
- Each agent identity has its own object ID and an optional sponsor
- Permissions are inheritable from the blueprint and admin-consented. Child identities can't run interactive consent
- Agents can act as themselves, so logs show the agent as the subject

How do you disable a misaligned-agent?

Kill the blueprint, and all agent identities are disabled. One governed identity class, one conditional-access policy, one consent detection. 1 kill-switch for all Copilot Studio sessions.

Assuming highlander design principles.

Sources: Microsoft Learn, Agent OBO flow · Agent identity blueprints · LazyAdmin on MC1506733

We need new controls that can deal with Agent-Physics*

Not a control plane. A new kind of physics.
Users and apps had their controls. Agents need theirs, and it starts with identity.

* Yes, I just made up a term. Have fun with it, Gartner.

Many thanks to the 0G team for creating Kusto

Oded Sacher · Avner Aharoni · Alexander Sloutsky ·
Evgeney Ryzhyk · Ziv Caspi

Changed my life.

Many thanks to my friends

Ashish Jain · Rico Mariani · Mady Marinescu · Yong Rhee · Mati Goldberg · Noam Hadash · Artem Merkovich · Amir Kutcher · Adi Weisberg · James Singh · Sarahzin Shane · Serina Vartanian

I learnt from the best.

APPENDIX

References

1. Microsoft Learn, "AgentsInfo table in the advanced hunting schema"
2. Microsoft Learn, "Advanced hunting schema: naming changes"
3. Microsoft Learn, "CopilotInteraction audit schema"
4. Microsoft Learn, "Audit logs for Copilot and AI applications"
5. Microsoft Tech Community, "Investigating M365 Copilot activity with Sentinel and Defender XDR"
6. Microsoft Learn, "Discover local AI agents with Microsoft Defender for Endpoint"
7. Microsoft Learn, "Local AI agent discovery overview"
8. Microsoft Tech Community, "Now generally available: Discover local AI agents"
9. Microsoft Learn, "ExposureGraphEdges table"
10. Microsoft Learn, "ExposureGraphNodes table"
11. Microsoft Learn, "Query the enterprise exposure graph"
12. Microsoft Learn, "Agent identity blueprints in Microsoft Entra Agent ID"
13. Microsoft Learn, "Agent OAuth flows: on-behalf-of"
14. Hybrid Brothers, "Correlating AgentsInfo with CloudAppEvents"
15. LazyAdmin, "Microsoft Entra lets users create agent blueprints by default"