



AI & Automation

Eirik Valderhaug
Cortex EMEA Sr. Solutions Architect

A Very Brief History of AI

- First we had statistics...now we have “AI”.
- **Statistics:** useful for quantifying relationships in numerical data (avg, max, ..)
 - Linear regression - graph a line based on known data, tell me where new data will go (residuals)
- **Machine Learning:**
 - **Supervised** - Predict future values with multivariate data. (Support vector machines)
 - **Unsupervised** - Group data based on similar characteristics (K means clustering)
- **Natural Language processing (NLP):** quantify human language into numbers...to then run ML algorithms on
- **LLMs** - next level of NLP in which language meaning is inferred based on context of the human language documents
- **AI** - eliza with a PhD

AI Today

- **LLMs** - computer processing of human language with contextual understanding.
 - Often used in prompt based format.
 - ChatGPT, NotebookLM, etc.
- **Models**
 - Trained datasets with varying accuracy, size, capabilities
 - Deepseek, Ollama, Gemini, etc.
- **MCP** - a protocol for communicating with LLMs programmatically
 - Servers - interface with outside apis, local files, etc to augment the knowledge a LLM has
 - Clients - code that queries MCP servers and LLMs
- **Agents**
 - MCP clients and traditional code...

The Historical Challenges of SOC Automation

- **Reduce Effort Required by Repetitive Tasks**
 - Create a Workplan
 - Where manual effort was previously required, apply automation
- **Build Static Context**
 - Reduce pivoting and perform aggregating between tools (threat intel, SIEM searches, etc)
 - Predefined aggregation of data in playbook tasks
 - Flexible but static logic design
- **Customize Actions**
 - Large library of out of the box automations and scripts
 - Also can create python scripts and do anything python can do
- **Standardize Response Procedures**
 - Manual and automated tasks

Automation Workflow Challenges

- I have an alert but I know not what to do with it
 - Real life response to security incidents is not always a clear cut path
 - Predefined static workflows can be inflexible in regards to variability and time of execution
 - Response processes are hard to clearly define..which makes it hard for junior analysts to make confident decisions or understand what to actually investigate
- I know what to do but I have no idea how to do it
 - Inputs and outputs are hard to work with between various tools
 - Multiple API calls / commands may be required to achieve single automation goal
 - Many automations in the marketplace but which to use can be difficult to determine



Cortex AgentiX

**Build, deploy, and govern the AI
agent workforce of the future.**

Eirik Valderhaug
Cortex EMEA Sr. Solutions Architect



AI attacks are fast,
adaptable and
infinitely scalable

Sources:

1. Unit 42 2025 Global Incident Response Report

2. Gartner Over 100 Data, Analytic and AI Predictions through 2031

100X

Faster attacks with AI.¹

1 Hr

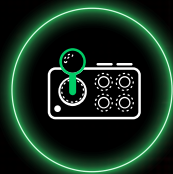
Time to exfil in 20% of
Unit 42 cases.¹

50%

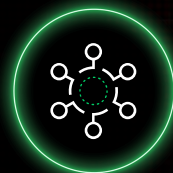
Less time to exploit
account exposures.²

Security needs to be **autonomous**. But **agentic AI** poses its own risks.

Autonomy



Flexibility



Accessibility



Unsafe actions and downtime
without proper guardrails



Unpredictable results
without human oversight



Bad prompts or risky
actions from untrained users

What if you could bring autonomy and control **together**?



Automation

Precision



Agentic AI

Flexibility

What's needed to harness the **power** of agentic AI

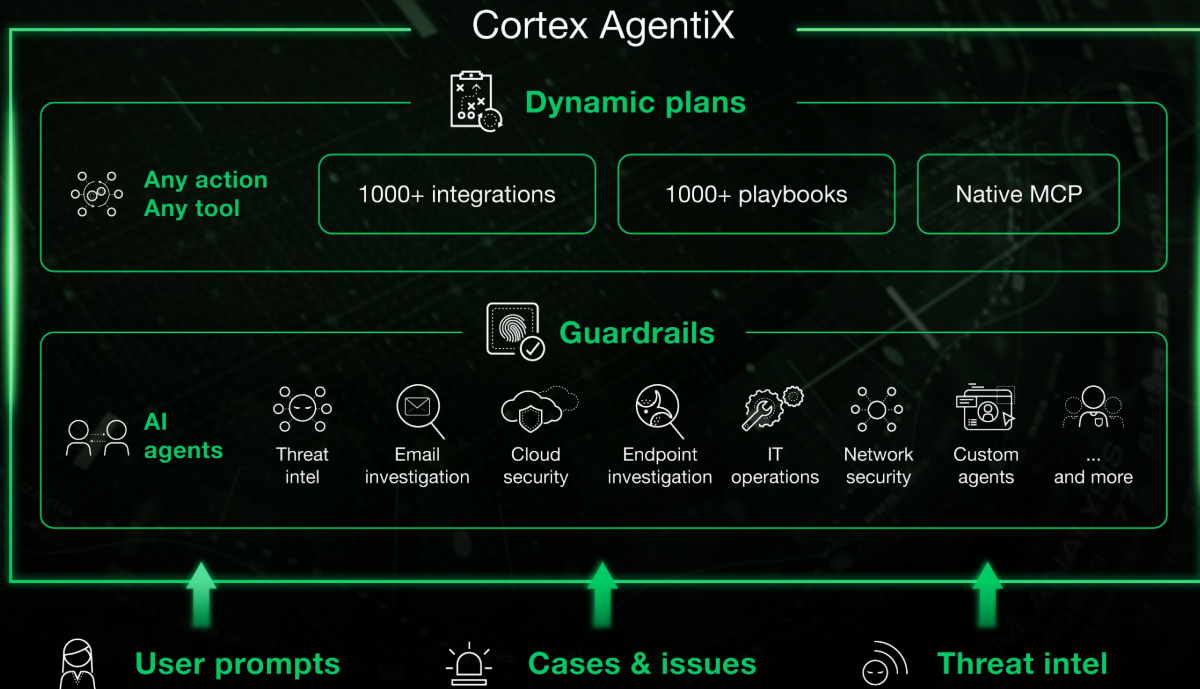




Introducing

Cortex AgentiX

Build, deploy and govern the agentic workforce of the future



Limitless AI agent workforce

Agents use deep security data and 1.2B+ playbook executions.

Enterprise-grade guardrails

Safely operate AI agents with ironclad role-based access controls

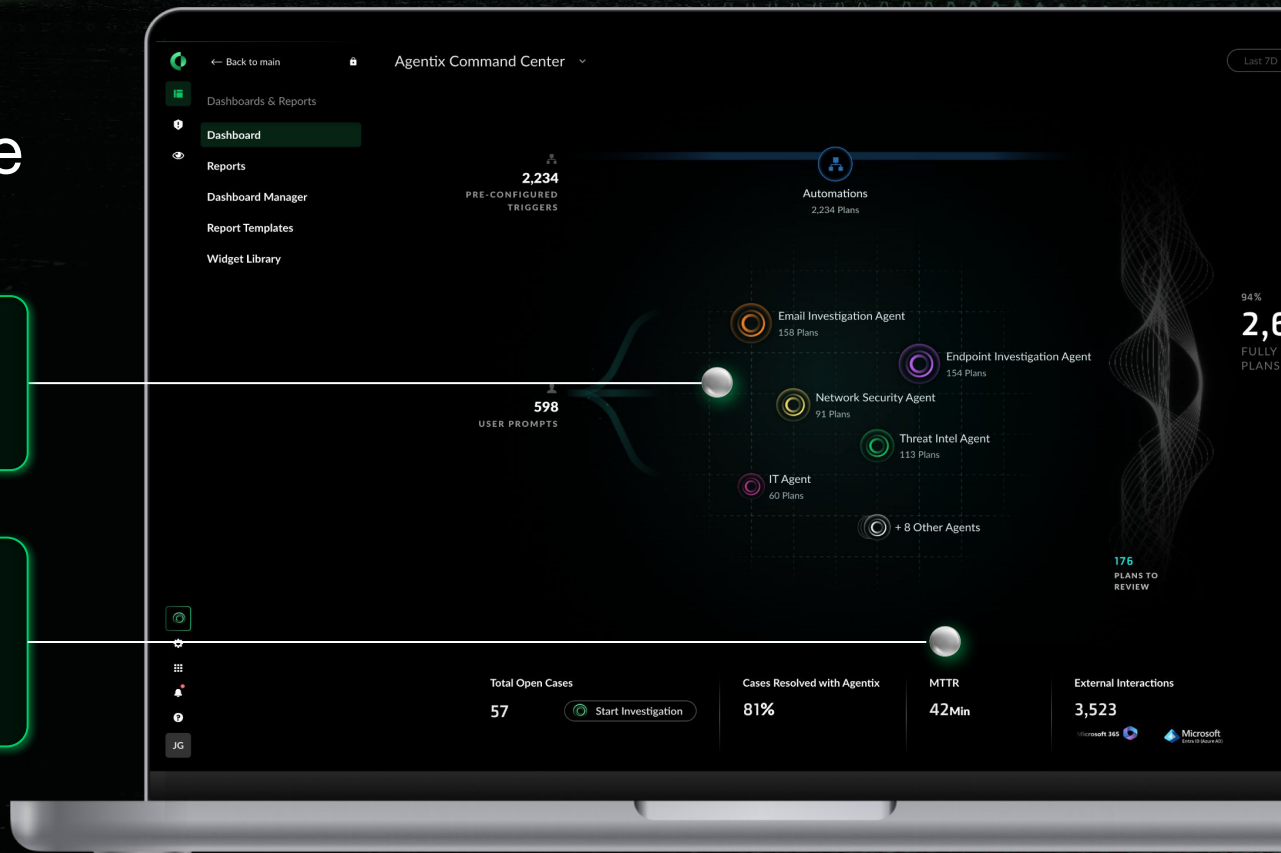
Agentic AI everywhere

Deploy context-aware agents directly within any Cortex product

Your limitless AI agent workforce

Scale your team with AI agents
that can dynamically plan, reason
and execute complex workflows.

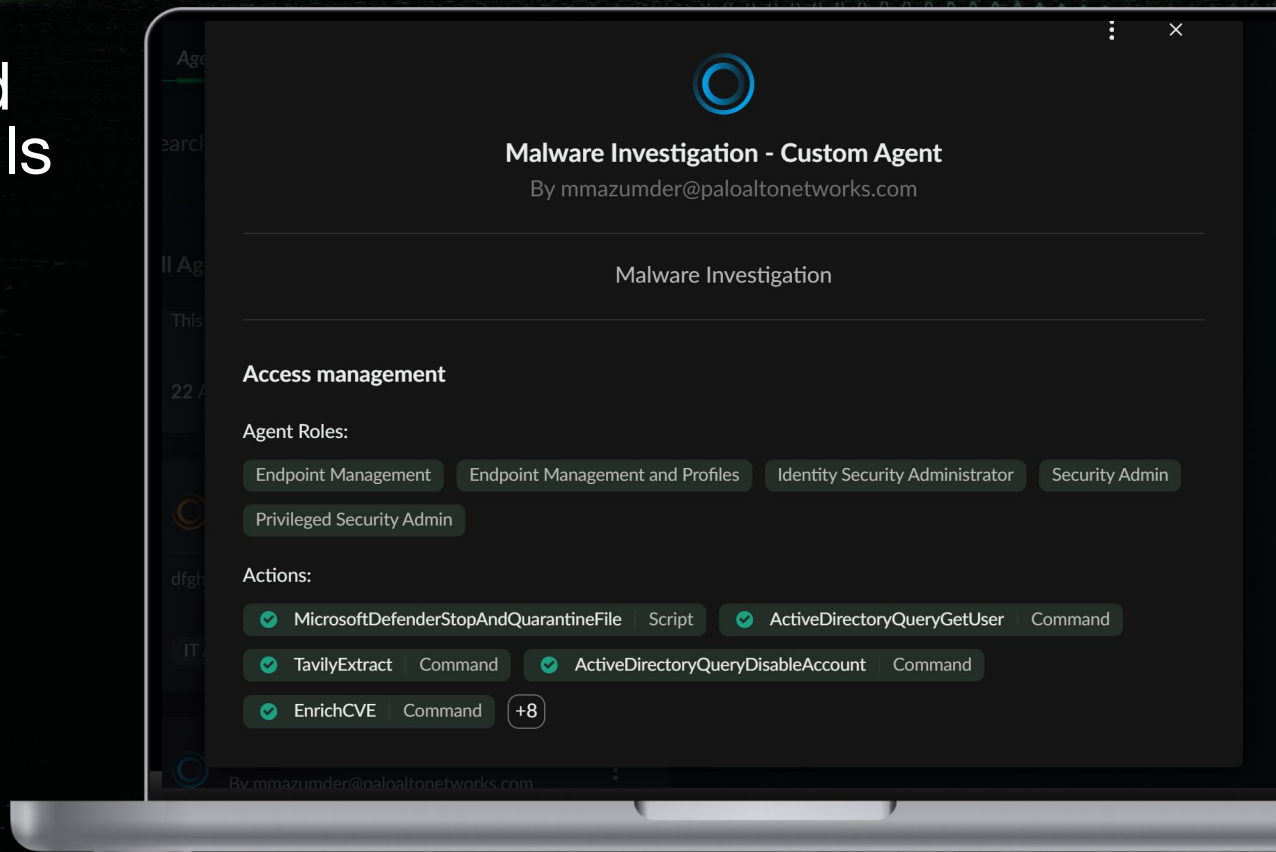
**Reduce MTTR and automate
manual tasks**, letting your team
prioritize higher-value, strategic
work.



Managed & bound by robust guardrails

Achieve predictable, safe outcomes with agent actions bound by the same permissions as human analysts.

Remain in control with human-in-the-loop approval and manual oversight for high-impact actions.



With full transparency into all actions

See every step an agent takes with 360-degree visibility and control.

Achieve complete auditability, with every prompt and query logged and available for review.

The screenshot displays the Cortex Agentix interface, which is divided into several sections:

- Left Sidebar:** Contains navigation links for Dashboards & Reports, Cases & Issues, Investigation & Response (highlighted), Threat Management, and Marketplace.
- Top Bar:** Shows the Cortex Agentix logo, a lock icon, and a 'New Conversation' button.
- Agentix Hub:** A central area showing a list of conversations. The selected conversation is titled 'https://unit42.paloaltonetworks.co...'. Below it, a list of prompts is visible, including 'From this Unit 42 post - https://uni...', 'Have any of the SSL certificates on ...', 'What can I ask you?', and 'what's the weather today in santa c...'. At the bottom of this section are buttons for 'Agentix' and 'Settings'.
- Plan:** A detailed view of the agent's reasoning process for the selected prompt. It includes:
 - Interpreted User Input:** A list of steps: 'Extract the file indicators of compromise (IOCs) from the URL https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/', 'Enrich the extracted file IOCs', 'Check for sightings of the enriched file IOCs in the tenant', 'Check for related alerts (issues) associated with the enriched file IOCs', 'Provide a brief summary of the extracted IOCs, their enrichment, and any sightings or related alerts (issues)', and 'Display the summary in the chat'.
 - Planned Steps to Address Your Request:** A numbered list of actions: 1. Use the 'TavilyExtract' action to extract the content from the provided URL. 2. Use the 'ExtractIndicators' action to extract file IOCs (hashes) from the extracted content. 3. Use the 'EnrichFile' action to enrich the extracted file IOCs. 4. Use the 'SearchIndicators' action to check for sightings of the enriched file IOCs within the tenant. 5. Use the 'SearchIssues' action to find related alerts (issues) for each of the enriched file IOCs. 6. Generate a summary of the extracted IOCs, their enrichment, and any sightings or related alerts using the 'InvokeLLM' action. 7. Display the summary in the chat using the 'SendNotification' action.
 - Extracting content from the provided URL using TavilyExtract to prepare for IOC extraction.**
 - Threat Intel:** A section with a warning icon and the text 'Sensitive action detected - User approval required'. Below it, the text reads: 'Extracting content from the provided URL using TavilyExtract to prepare for IOC extraction.'

AgentiX Agents

Prebuilt and custom AI agents, available 24/7



Endpoint Investigation Agent



Threat Intel Agent



Email Investigation Agent



Cloud Security Agent



Network Security Agent



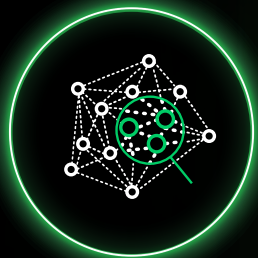
IT Agent



Custom Agent

...and more

The **Cortex AgentiX** advantage



Industry's largest security automation ecosystem with **2000+ integrations and playbooks**



Security guardrails battle-tested from a **decade** of SOAR deployments



Deep security expertise from the world's largest cybersecurity company with 1.2 billion automations



Manage agents on a **single platform** for any IT and security domain

Hyperscale your security and IT operations



Supercharge efficiency

Automate tasks that slow your team down



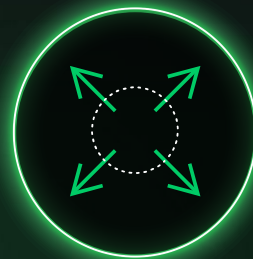
Empower analysts

AI agents serve as intelligent teammates, available 24/7



Adapt quickly

Adapt to novel cases & new threats in real-time



Scale confidently

Deploy agents with 100% control to scale your operations



Cortex XSIAM, XDR and Cloud **customers**



Put AI agents to work from day one

Command a fleet of embedded autonomous AI agents that operate like experts—ready to think, plan, and act.



Use AI to accelerate automation

Generate playbook scripts using natural language prompts—no coding required.



Get full Agentic AI seamlessly

Get full agentic AI with the unified platform. Just turn it on, no SKUs needed, no additional cost



Cortex XSOAR customers



Worry-free upgrade

Run AgentiX in parallel with your current XSOAR deployment for 6 months. Request early access now.



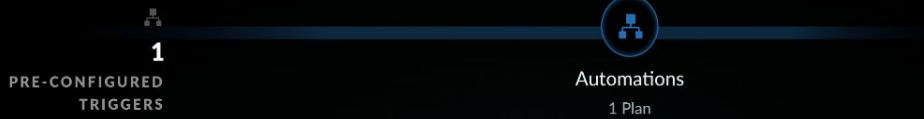
Your partner through the process

We'll partner with you every step of the way, with customer support and professional services.



Supercharge your team with AgentiX

Command a fleet of agentic AI agents that can plan and execute complex workflows, serving as specialized, expert assistants to your team.



Demo time...



89%

66

FULLY EXECUTED PLANS

7

PLANS TO

Total Open Cases

23

Start Investigation

Cases Resolved with Agentix

0%

MTTR

0Min



Thank You

paloaltonetworks.com