Cortex AgentiX

The Industry's Most Secure Platform to Build, Deploy, and Govern the AI Agent Workforce of the Future

Cortex® AgentiX™ delivers end-to-end workflow autonomy with prebuilt and custom no-code agents that act as a seamless extension of your team—planning, reasoning, and executing like an expert. Your analysts can launch context-aware agents directly from any Cortex product or orchestrate complex, enterprise-wide actions from the standalone Cortex AgentiX platform. Enterprise-grade guardrails, including role-based access controls and human-in-the-loop approval for impactful actions, help ensure agentic workflows are safe and reliable.

Security and IT Operations in the Agentic Era

Human-driven operations are no longer sufficient to meet the demands of modern enterprises. As threats evolve and technology accelerates, security and IT teams face critical challenges that limit their efficiency and effectiveness:

- **Rapidly evolving threats:** Legacy, rule-based automation is effective for known issues, but it falters against novel attacks and quickly changing attacker tactics that leverage AI.
- **Automation maintenance overhead:** Manual coding is often needed to maintain and scale automation, and prebuilt playbooks cannot cover every possible scenario.
- **Hesitation in AI adoption:** Security leadership is cautious about delegating high-stakes tasks to AI without comprehensive auditability, visibility, and robust control mechanisms.

Cortex AgentiX: Fusing Agentic AI with Automation

Traditional security automation platforms handle known tasks with precision, scaling operations and improving efficiency, but they struggle to adapt to the unknown.

Cortex AgentiX unites the flexibility of agentic AI and the precision of automation to deliver end-to-end workflow autonomy. Its powerful prebuilt agents are able to dynamically plan, reason, and execute solutions just as an expert would, giving your security analysts a decisive advantage. You can automate repetitive tasks while your team leverages AI agents that adapt instantly to dynamic, novel threats or scenarios.

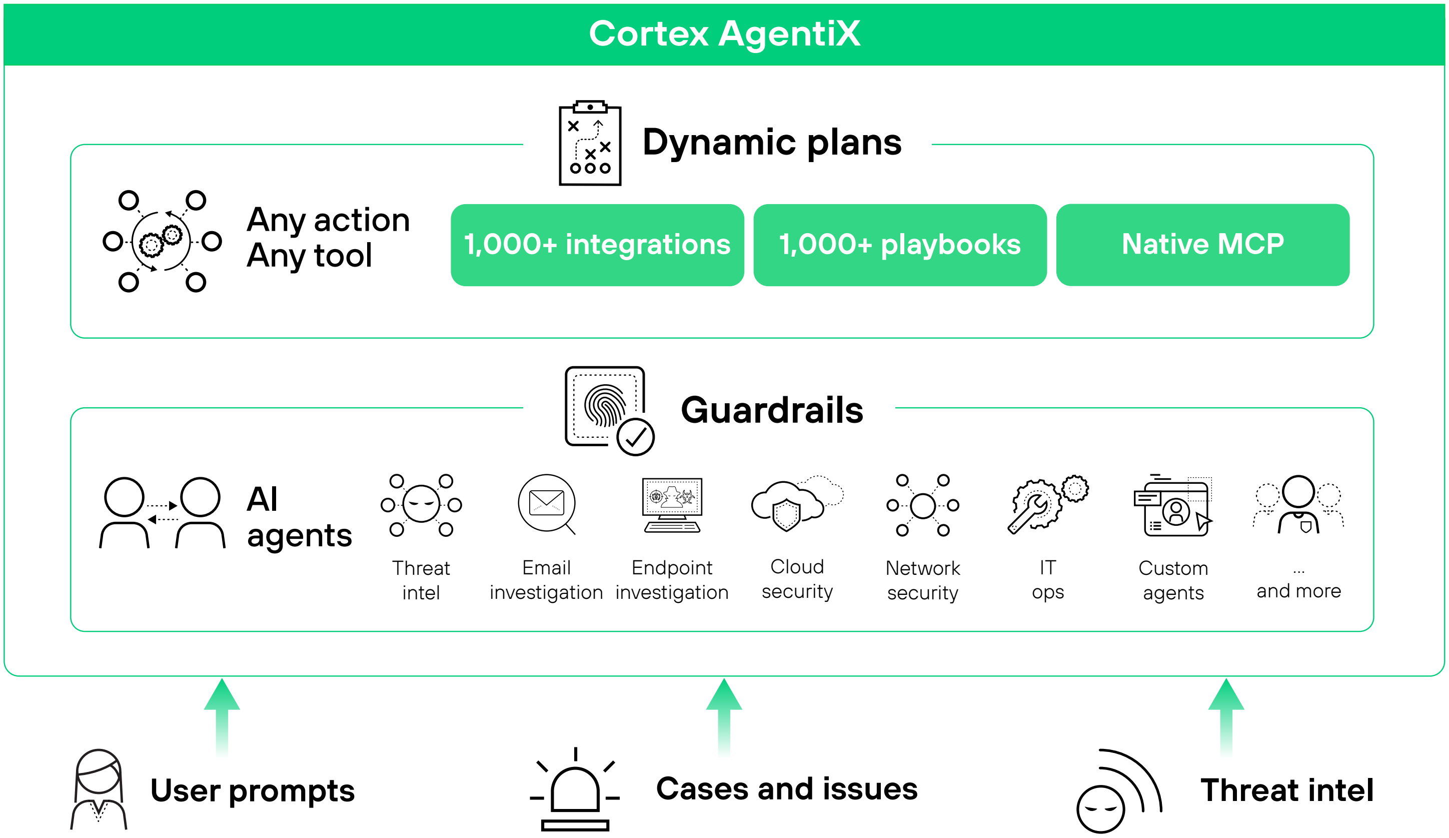


Figure 1. Cortex AgentiX powers workflow autonomy across the SOC

AI Agents That Elevate Your Team’s Impact

AgentiX AI agents are intelligent “teammates” available 24/7. Built on a decade of automation expertise and 1.2 billion playbook executions, these persona-based agents operate as the industry’s most experienced security experts. The AgentiX Command Center brings them together in one view—where you can see, manage, and orchestrate your entire AI agent workforce.

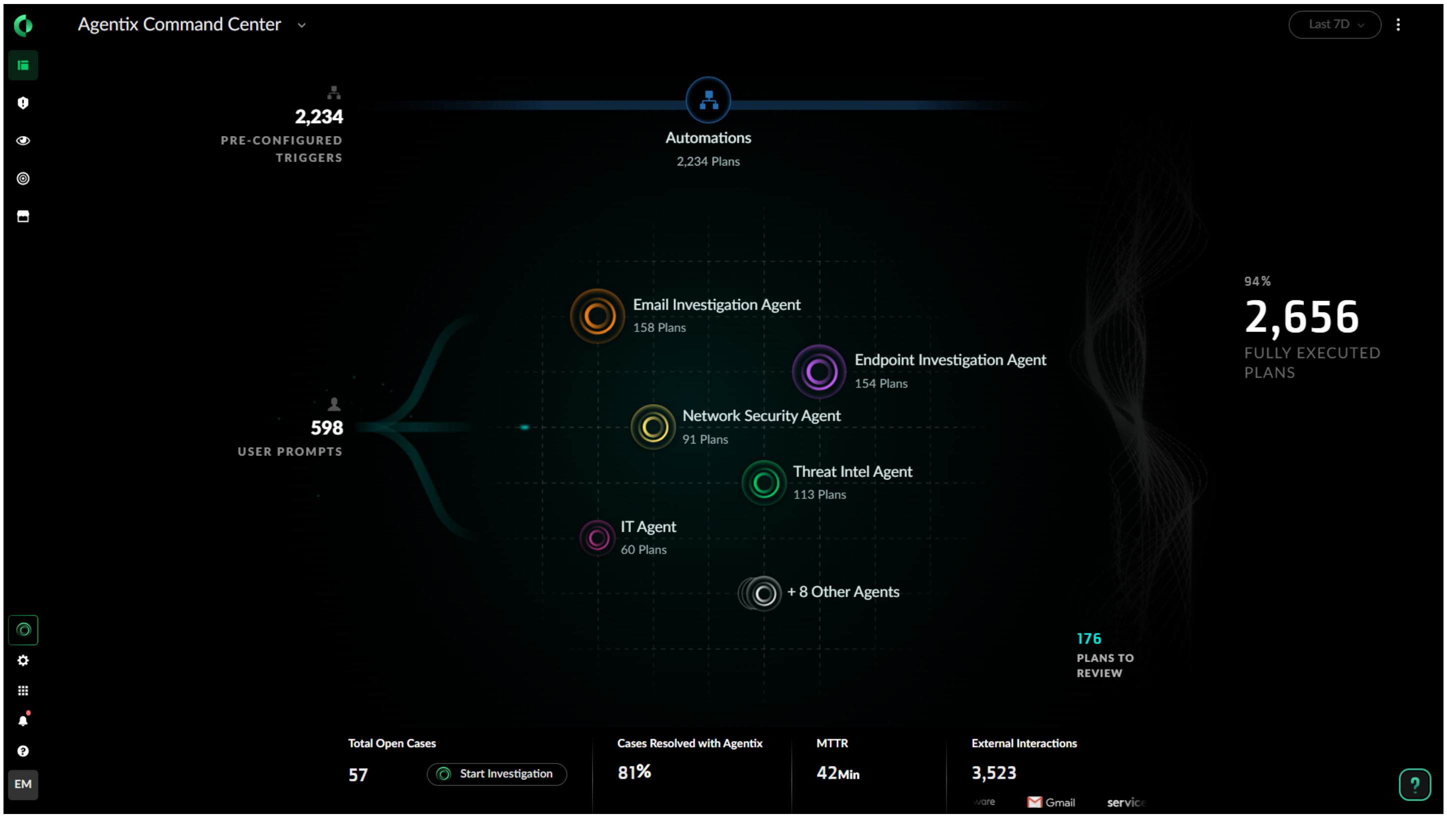


Figure 2. Manage and monitor agents in the AgentiX Command Center

Your analysts simply prompt agents in natural language. The agents then instantly create and execute plans—the sequences of actions designed to fulfill your requests. For example, researching a new threat, extracting indicators of compromise (IoCs), checking your network for impact, and performing basic remediation can take hours. Our Threat Intel Agent completes this task in minutes. The agents augment and accelerate your day-to-day operations, allowing your team to prioritize higher-value, strategic work.

Agents with Full Transparency. No Black Boxes.

Gain full transparency into an agent’s reasoning, such as how it interprets your request, the actions it takes, and the results it delivers. Every action is logged, showing the agent that ran it and the person who invoked it.

Enterprise-Grade Security and Governance

You can't automate what you don't trust, which is especially critical when moving from static rules to dynamic AI agents. Cortex AgentiX ensures trust is built-in, not bolted on. We manage this through robust, enterprise-grade governance:

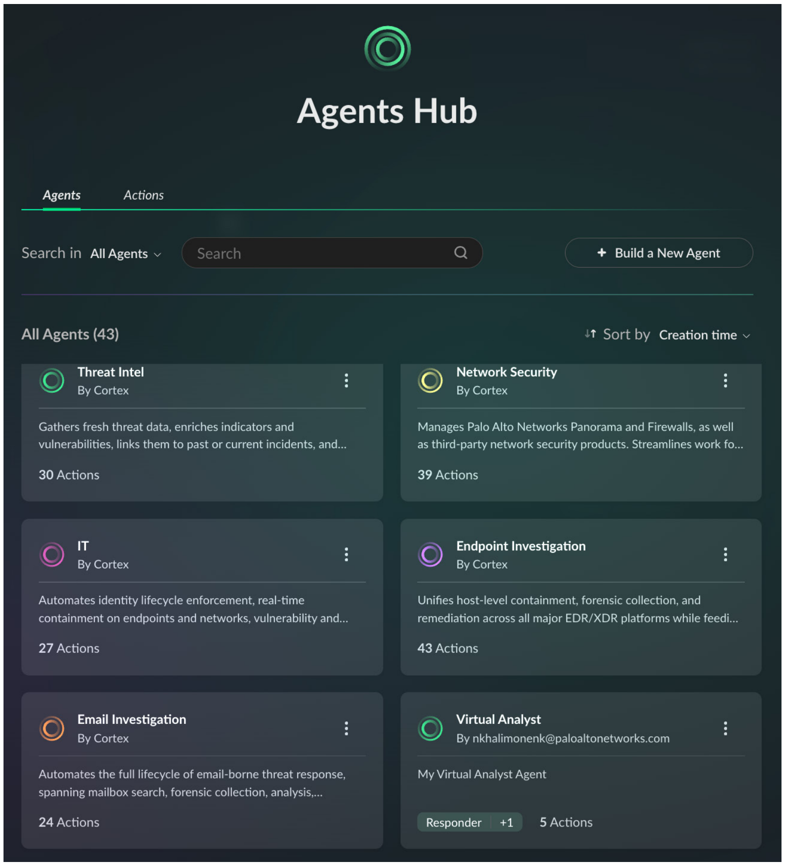
- **Granular access controls:** Agents are bound by the same roles and permissions as your human analysts.
- **Human-in-the-loop approval:** AgentiX flags any action as sensitive so it requires human validation before critical system changes are executed, guaranteeing you maintain final oversight.
- **Auditability by design:** Every action that an agent takes is logged and auditable, giving you complete transparency and peace of mind.

Speed is essential, but control is paramount. With Cortex AgentiX, you gain machine-speed autonomy while always operating within strict, defined guardrails.

Agents Hub to Manage Your Agents

Through the Agents Hub, you can launch prebuilt expert agents or use the intuitive builder to create custom agents tailored to your needs:

- Register scripts and commands as custom actions that can be assigned to agents.
- Review system actions and modify existing custom actions.
- Define agent permissions, roles, and sensitive actions.
- Create, revise, and remove custom agents.



Threat Intel
By Cortex
Gathers fresh threat data, enriches indicators and vulnerabilities, links them to past or current incidents, and...
30 Actions

Network Security
By Cortex
Manages Palo Alto Networks Panorama and Firewalls, as well as third-party network security products. Streamlines work fo...
39 Actions

IT
By Cortex
Automates identity lifecycle enforcement, real-time containment on endpoints and networks, vulnerability and...
27 Actions

Endpoint Investigation
By Cortex
Unifies host-level containment, forensic collection, and remediation across all major EDR/XDR platforms while feedi...
43 Actions

Email Investigation
By Cortex
Automates the full lifecycle of email-borne threat response, spanning mailbox search, forensic collection, analysis,...
24 Actions

Virtual Analyst
By nkhalimonenk@paloaltonetworks.com
My Virtual Analyst Agent
Responder +1 5 Actions

Figure 3. Manage and build your agents in the Agents Hub

AgentiX System Agents

Table 1 lists some of the agents, which are subject to change with version updates.

Table 1. AgentiX System Agents

Agent Name	Agent Role
Email Investigation Agent	Automates the full lifecycle of an email-borne threat response, spanning mailbox search, forensic collection, analysis, containment, and incident closure across all major mail platforms and security layers.
Endpoint Investigation Agent	Unifies host-level containment, forensic collection, and remediation across all major EDR/XDR platforms, while feeding evidence and status into the SOC ticketing and collaboration stack.
Threat Intel Agent	Gathers fresh threat data, enriches indicators and vulnerabilities, links them to past or current incidents, and publishes clear briefings so the whole SOC acts on the latest attacker tactics.
IT Agent	Automates identity lifecycle enforcement, real-time containment on endpoints and networks, vulnerability and patch governance, asset intelligence upkeep, and end-to-end incident workflow coordination to deliver policy-driven remediation across the enterprise.
Network Security Agent	Manages Palo Alto Networks Panorama® and firewalls, as well as third-party network security products. Streamlines work for network security engineers by performing configuration checks, policy optimization, vulnerability assessment, certificate expiration monitoring, as well as log analysis and threat response.
Cloud Security Agent	Investigates and remediates complex cloud security posture issues as well as responds to active threats across multicloud environments.
Help Center Agent	Provides instant, context-aware answers drawn from the Cortex knowledge base, helping analysts resolve questions, surface best practices, and accelerate every investigation.

Boosting Operational Efficiency with AI

AgentiX removes the biggest pain point in automation: building and maintaining complex playbooks. You can use natural language to create automation scripts, turning anyone on your team into a powerful workflow builder.

- **Agentic actions:** Our LLM-powered script generator enables you to create fully functional Python automation scripts based on natural language prompts. You can then save these scripts as actions for agents or playbooks to use.
- **Agent prompts:** You can manage and refine your LLM prompts, turning your meticulously crafted prompts into reusable assets sharable across your organization. Plus, you can also easily register prompts as actions for use in playbooks or by agents, ensuring consistent, high-quality results.
- **AI-generated playbooks:** You can build playbooks using AI or by embedding AI tasks within existing playbooks, enabling them to adapt to dynamic, real-time situations.

Key Components in Cortex AgentiX

Table 2. Cortex AgentiX Components

Name	Description
Actions	Wrap diverse capabilities (such as playbooks, scripts, commands, and AI tasks) to make them accessible and executable by an agent. You can use out-of-the-box system actions or create and save your own actions.
Agent	Virtual personas that create and execute complex, domain-specific plans to assist in your SOC operations. These agents are fully governed. Each one is bound by strict guardrails and the same roles and permissions (role-based access control [RBAC] and scope-based access control [SBAC]) as a human analyst, ensuring every action it takes is orchestrated within a trusted, defined scope. The types of agents include: • **System agents** are provided by Cortex AgentiX for specific use cases. • **Custom agents** are created by the user.
Playbook	A series of tasks that run in a predefined flow. They can include subplaybooks, manual tasks, automated tasks that run scripts or commands, AI tasks, or quick actions.
Quick Actions	Preset commands that enable you to automate basic tasks, such as creating tickets in third-party systems, sending Slack messages, and changing issue severity.
Issue	An individual security finding or suspicious event.
Case	A collection of related issues that provide a comprehensive, high-level view of a security incident.
Plan	A sequence of actions that run in parallel or sequentially to satisfy a user request. The agent dynamically chooses the relevant actions to execute the plan.

Playbook Management

Not every task requires an agent. For routine tasks and known complex processes, automated playbooks deliver consistent results, saving significant staff time and accelerating case resolution.

- **Playbook catalog:** Quickly find and adopt expert playbooks. You can choose from thousands of prebuilt options designed by our automation experts that cover a broad range of security and IT use cases.
- **Playbook playlist:** All playbooks that your team uses are centralized into the Org Playbooks list, making access and management fast and simple.

Collaborative Case Management

Cortex AgentiX unifies investigations, evidence, and collaboration in a single workspace—streamlining analysis and accelerating resolution. Its built-in collaborative functions include, for example, a war room for every incident, a real-time chatbot, and tight integrations with case management and ticketing tools like ServiceNow, Jira, Remedy, and Slack. They promote teamwork across departments and help you speed up remediation.

You can leverage our vast library of over 1,000 prebuilt integrations to power your agents or connect seamlessly to services in your AI ecosystem with our native Model Context Protocol (MCP) server.

Integrate Agentic AI Everywhere

Cortex AgentiX is natively embedded in Cortex XSIAM® and Cortex Cloud™, delivering autonomous workflows precisely where they're needed most. Access AgentiX through the embedded Cortex Agentic Assistant, which puts an AI agent workforce at your command to tackle any security challenge. The Cortex Agentic Assistant engages AI agents to plan and execute advanced workflows—turning tedious, manual effort into instant, expert action.

Cortex AgentiX will be available in the future, both embedded in Cortex XDR and as a powerful standalone agent orchestration platform, advancing Cortex XSOAR® into the era of agentic AI. For early access to Cortex AgentiX, sign up now.

Forward-Looking Statements

This data sheet contains forward-looking statements that involve risks, uncertainties and assumptions, including, without limitation, statements regarding the benefits, impact, or performance or potential benefits, impact or performance of our products and technologies or future products and technologies. These forward-looking statements are not guarantees of future performance, and there are a significant number of factors that could cause actual results to differ materially from statements made in this data sheet. We identify certain important risks and uncertainties that could affect our results and performance in our most recent Annual Report on Form 10-K, our most recent Quarterly Report on Form 10-Q, and our other filings with the U.S. Securities and Exchange Commission from time-to-time, each of which are available on our website at investors.paloaltonetworks.com and on the SEC's website at www.sec.gov. All forward-looking statements in this data sheet are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main:	+1.408.753.4000
Sales:	+1.866.320.4788
Support:	+1.866.898.9087

www.paloaltonetworks.com