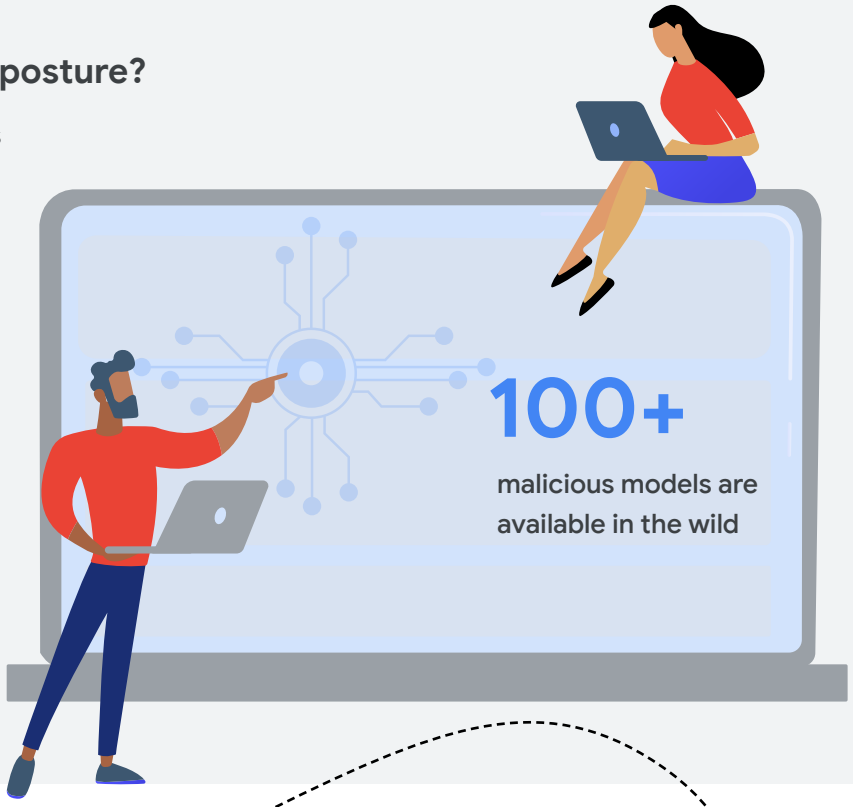
Google Cloud paloalto NETWORKS

Fuel AI Growth, Not Risk

Secure Your Future with Expert Guidance

Are you confident in your AI security posture?

The drive to innovate with AI is strong, but concerns about data security and compliance are real. Are you truly aware of the AI models operating within your environment and their potential risks?



50%
of employees use AI without permission and proper controls

80%
of public models can be easily jailbroken

100+
malicious models are available in the wild

Introducing the AI Security Discovery: Your Path to Secure AI Innovation

Benefit from the combined expertise of Palo Alto Networks and Google Cloud. Our multi-stage AI Security Discovery program provides a thorough analysis of your AI projects and processes, guiding you from initial understanding to secure deployment. Through collaborative sessions at your workplace, we'll help you:

- Achieve complete visibility into your AI security risks.
- Pinpoint and address your AI security vulnerabilities.
- Protect your valuable AI investments.
- Secure your AI models, datasets, and applications end-to-end.
- Unlock the full business value of AI with peace of mind.
- Accelerate your AI adoption securely. Let our experts guide you.

Limited Spots Available.

Book your first consultation today

Building Security into the Foundation of Your AI

Security cannot be bolted onto your AI initiatives but must be built into every facet of AI, including people, processes, and technology.

Understand and address the security risks associated with your AI deployments

To understand potential threats and vulnerabilities, you need a comprehensive view of your AI environment and posture, from model ideation to rollout. This AI Discovery exercise can help you:

- Know the distribution and utilization of AI applications, models, and datasets throughout your cloud estate.
- Identify potential vulnerabilities and misconfigurations within your AI models, applications, and datasets is crucial. This allows you to quantify associated risks and understand the security posture of your AI ecosystem.
- Understand how your networks interact with your AI infrastructures. This includes having an operational and security view of your network to see how users and networks interact with AI models, datasets, and plugins.
- Be aware of the mechanisms in place to detect and respond to threats as they occur within your AI ecosystem. Understanding your real-time monitoring capabilities is essential.
- Be clear on the governance and compliance aspects of your AI initiatives, including the potential for "shadow AI" models and applications, and ensure your AI usage aligns with evolving regulations.

How it works

From initial discovery to the rollout of your AI applications and models, our **AI Security Discovery** aligns with your journey, reveals potential risks, and protects your data. Together, we run through these phases:

Discovery:
Proactively identify and classify AI assets to address early-stage security risks.

Ideation:
Integrate security best practices into AI use cases to

Pilot:
Implement and test real-time threat detection to secure your expanding AI workloads.

Trial & Rollout:
Maintain continuous visibility and adapt to evolving threats and regulations for sustained AI security and compliance.

Take the First Step Towards Secure AI Innovation

Don't let uncertainty or fear delay your AI ambitions. Our complimentary **AI Security Discovery** is the first step in building a resilient and secure foundation for your AI-driven future. Gain actionable insights into your current AI security posture to confidently deploy AI workloads, knowing your sensitive data and critical infrastructure are protected.

Space is limited! Sign up today to secure your first discovery.

Google Cloud paloalto NETWORKS