

Blog 1: What Is Agentic AI - And Why Everyone's Talking About It

From the CSA Agentic AI Summit Series

By TekSol Global | Cybersecurity & AI Practice

Imagine you hired a very capable assistant. You tell them: "Book me a flight to New York, find a hotel nearby, and add it to my calendar." And then - without you doing anything else, they just ***do it***. They go to the airline website, compare prices, make the booking, find a hotel, reserve a room, and drop everything into your calendar. All by themselves.

That's the idea behind ****Agentic AI****.

So What Exactly Is It?

Most people have heard of AI tools like ChatGPT. You ask it a question, it gives you an answer. Simple. Back and forth.

Agentic AI is different. These are AI systems that don't just answer questions, they ****take actions****. They can:

- Browse the internet on your behalf
- Send emails
- Write and run computer code
- Access your company's data systems
- Talk to **other** AI agents

Think of the difference like this: a regular AI is like a very smart encyclopedia. Agentic AI is like a very capable employee who can actually ***do the work***.

Why Is This Happening Now?

The speakers at the CSA Agentic AI Summit explained it well. Computing has always been evolving. We went from big computers in rooms, to personal computers on desks, to phones in pockets, to apps in the cloud. Each step made technology more powerful and more woven into our daily lives.

AI agents are the next step. And it's happening fast, faster than any shift before.

One speaker from Qualys described it like this: just a few years ago, you needed an entire team of specialists to do complex security analysis. Today, you can deploy an AI agent that does it around the clock, automatically, without getting tired.

What Does "Agentic" Actually Mean?

The word "agentic" comes from "agent", something that acts on its own to achieve a goal.

An agentic AI system has a few key traits:

1. ****It has a goal.**** You give it a task, and it figures out the steps to get there.
 2. ****It makes decisions.**** It doesn't wait for you to approve every little move.
 3. ****It uses tools.**** It can search the web, run code, access databases, and send messages.
 4. ****It can work with other agents.**** One agent might hand off work to another, like a relay race.
-

A Real - World Example

Let's say a company wants to check whether its software is up-to-date and secure. Traditionally, a team of engineers would spend days manually reviewing systems.

With agentic AI, you could have:

- One agent scanning all software for outdated versions
- Another check to see if any of those outdated versions have known security holes
- Another is automatically fixing the low-risk ones
- Another is writing a report for the management team

All happening simultaneously. All overnight. All without a human having to do each step.

That's the power people are excited about.

But Here's the Thing - This Power Comes With Risk

When an AI agent can act on its own, make decisions, and access important systems... what happens if something goes wrong? What if it does something it wasn't supposed to? What if a bad actor tricks it?

That's exactly what the Cloud Security Alliance summit was focused on. The excitement is real, but so are the dangers. And right now, the technology is moving faster than the safety measures.

As one summit speaker put it: *"The tools that we've built, the security architectures we've deployed, they're all pointed at layers of the enterprise that are no longer where the most interesting action is happening."*

The playing field has changed. And the conversation at this summit was about how we keep up.

What's Coming in This Blog Series?

Over the next 14 blogs, we'll walk through everything discussed at the CSA Agentic AI Summit, translated into plain language so anyone can understand it. No prior tech knowledge required.

We'll cover:

- Why AI agents are a brand new kind of security problem
- How hackers are already using AI to attack companies
- What "identity" means for an AI (yes, AI needs ID too)
- How companies should govern AI agents
- What the security industry is doing about all of this

Whether you work in tech, business, policy, or you're just curious, this series will give you a real understanding of one of the most important technology shifts happening right now.

Let's get into it.

Next up → Blog 2: The New Attack Surface - How AI Changed What Hackers Can Do