AGENTIC AI TACKLES NETWORK OUTAGE PREVENTION CHALLENGES

NetBrain CEO Lingping Gao on How Agentic AI Decodes Intent to Automate Diagnosis

Lingping Gao,
NetBrain CEO

Solving the long-standing challenge of preventing recurring IT network issues has remained elusive. Lingping Gao, CEO and chairman of NetBrain, said agentic artificial intelligence combined with intent-based automation offers a proactive turnkey solution within a network infrastructure. The solution is not just reacting to outages but understanding and enforcing the underlying "intent" behind every function in a network.

Most networks have evolved over decades with input from hundreds of engineers. Human efforts to manually document operational intent fall short. But NetBrain's newest release solves this by discovering intent automatically and overlaying it with agentic AI for real-time diagnostics and prevention.

In this video interview with Information Security Media Group at RSAC Conference 2025, Lingping also discussed:

- How NetBrain's "Golden Assessment" builds herd immunity for network security;
- The three critical components of agentic AI for solving context-rich problems;
- How AI and automation can reduce operational costs and human dependency.

With more than two decades of experience at NetBrain, Gao leads various customer services, including outage prevention, diagnosis automation, network security enforcement and ensuring end-to-end visibility across physical, virtual, SDN and cloud networks. Previously, he was a network engineer at Thomson Reuters.

THE UNSOLVABLE IT PROBLEM

TOM FIELD:
What is the unsolvable IT problem you are helping customers solve?

LINGPING GAO:
NetBrain is an automation platform company. We have been for 20 years, so this unsolved IT problem is very familiar to everyone. It's called a prevention. Let me be more specific. Every company has a network attack, has network outages. They come back say, 'how can I prevent the next problem, similar to this happening again?' That problem is unsolved today and through 20 years of R&D and thousands of customers later and along with intent-based automation, agentic AI and the digital twin, we found a very just exciting solution towards that.

UNSOLVABLE NO MORE

FIELD:
Talk about the new product release that is solving recurring IT/network problem.

GAO:
As we talk about it for years, the way we solve the problem is trying to 'intent-ize' your network. So what that means is anything running your network, security, performance and application, there's an intent behind it. The challenge is to decode the intent. So for 20 years we were able to decode those intents,

"Every company having network attacks or outages keeps asking, 'How can I prevent the next similar problem?' This remains unsolved today. But we've found an exciting solution through 20 years of R&D, intent-based automation, agentic AI and digital twin technology ... agentic AI is a once in a lifetime innovation."

allow your system to proactively monitoring and enforcing those intents. This release is very exciting because we figured out a way how to make this turnkey. A lot of automation platforms took years, took a team to derive value. How to make this instant turnkey solution is the effort that we have worked on years with agentic AI. Two things come to play. One is agentic AI is coming to the fore. Secondly is we figured out a way to discover network intent, right, so to speak.

You have a network running for 20 years, there's 500 people who've worked on in the last 20 years and all kinds of intent behind it. If you rely on human to decode and discover, define those intents, you're never going to work because it's always changing. We figured out a turnkey to discover those intents. Two things together make it so exciting today. You're thinking about it when you have a network problem, when you have a security attack, you can discover that in matter of hours, all the intent underlying your network. Then agentic AI overlays on top of it. You're able to automatically diagnose it. You're able to build all kinds of observability on top of it, try to prevent as a problem to stay ahead of the game.

EVOLUTION OF AGENTIC AI

FIELD:
Agentic AI has been a big theme of the RSAC Conference. Talk about the evolution of agentic AI and how it really empowers your solution.

GAO:
In the infrastructure domain, you can see agentic AI moving from a tool. You want to ask AI, 'what is this IPS? What about macOS - is it going to become a system we call the copilot? You will do it, right?' Now it's rapidly getting to the world of experts. It can do things better than human doing. So the three big things underlying agentic AI is a reasoning capability,

especially it's a reflective reasoning. AI is like a human. It can reflect on its own. It has better memory than all of us. Typically, it can memorize millions of millions bits of data much better and in real time, right? Last thing is to have the capability to invoke tools. Those three together, agentic AI now is in the prime time. It's transforming entire business application, how it has been used and how it's been created.

People say this is a once in a decade innovation. This is a once in a lifetime innovation. That entire society, including our society, IT infrastructure, security can step on top of it. We are at an interesting time. We're standing on top of the giant, which is the agentic or generative AI.

WHAT IS HERD IMMUNITY?

FIELD:
You also mentioned that you're hoping to help the community develop a herd immunity. When you say that, what do you mean?

GAO:
Herd immunity is similar to endpoint security. If your laptop had a virus, compromised, everyone can learn from it. Then all the other people will have that immunity, herd immunity, but the herd immunity did not work very well in a context rich environment. For example, CVE is one type. You have vendors publish their vulnerabilities. Notice that CVE turned to a knowledge of my network, how many violations it had. Processes like this took a long time, where context gets more convoluted. The herd immunity doesn't exist. We actually push that herd immunity to the next level.

My network had the outages, had an attack. I can turn around to do post-mortem, post-attack assessments, figure out I have 50 other instances like this that I can secure, I can monitor, but what about if they're not attacked on my environment? What if it's other people's environment? Can I benefit from that? That's when herd immunity comes into play. With the newer technology intent based on agentic AI innovations, what happened in the whole society? As long as I see it, I can define it and I can download that pattern and analyze my infrastructure, my network and figure out, 'oh, I have similar issue. That company had a split brain causing network outages.' I also find I have 500 similar problems through this one thing.

Through this herd immunity defense, NetBrain invented this concept called golden assessment. The idea is that you learn from industry, you will make it a pattern. That pattern is downloadable to your instance of NetBrain. It will discover your network, figure out, 'oh, you have 5,000 similar incidents that you can look at it. Is that now being violated?' You can continually monitor it so together the herd immunity is really the ultimate solution to prevention.

"We're talking about a lower operational cost. We're talking about a less dependency on humans. With agentic AI, those are going to be rapidly realized. So we will see an IT industry that for the first time agility becomes real. The operational cost is going to go down because the majority of a human dependency tasks now can be shifted to AI along with automation."

DO SOLUTIONS RESIDE WITH AI?

FIELD:
In this environment, where does your AI solution stand out?

GAO:
Everyone really thinks that AI can transform their industry and how they do things for the right reasons. It is a true, very powerful yet simple AI solution. You can do it over the weekend but a complex AI takes a very long time to construct. Why? AI is very difficult. I would say AI falls short of solving context-rich problems. What do I mean by context-rich problems?

I'll use the network as an example. You need to understand your entire network to be able to diagnose this AI. Think about AI like a doctor. Using this analogy, let's say many patients come in saying they have a headache. When patients come in and say this, the first thing the doctor needs to do is to decode, to understand this patient and get all the context. His history and all those things. That's called a context.

It's not like the doctor is saying 900 other patients have similar headaches. But allowing him to immediately diagnose this one, make him better and not enable them immediately is the solution. This context is a challenge on agentic AI, especially when the security and network infrastructure is big.

How does NetBrain go about solving it? First of all, we talk about agentic AI as three components, reasoning components, memory components and tool components. In order to make the agentic AI work well you first have to feed it the right data, the context side of it. So NetBrain has worked for 20 years to build a digital twin across physical,

virtual and cloud networks. So you have to have accurate data about a patient to provide the best care or solution possible.

Second thing you have to do is to allow agentic AI access to rich tools. In the case of NetBrain, we actually invented this concept called intent. Each intent is also an automation tool. So a network of 10,000 nodes could have a million intents. Each intent is an automation tool that is orchestrated by AI. So now the AI has, with this capability, a magic workaround to solve context rich problems like network security or network troubleshooting issues.

So today, if you look at how an intent-based AI platform works you have to load in a customers' past data. Intent will learn from it and NetBrain will learn from it and decode it into a set of requests and intents being discovered across your entire network. Now, each of the problems in the future are automatically weaved together between user request and the intent itself. So together it's magic. Its magic, but its magic that's only possible because of three things that came together and that's where I say AI is good, but you need to figure out how to feed AI with the right context.

AI AND THE FUTURE OF NETBRAIN

FIELD:
Where do you see the future of AI's transformative power and the future of NetBrain?

GAO:
For the industry, for the entire industry, we are talking about agility. We're talking about a lower operational cost. We're talking about a less dependency on human. With agentic AI, with AI in general, those are going to be rapidly realized. So we will see an IT industry that, for the first time, has the agility to become real. The operational cost is going to go down because the majority of human dependent tasks now can be shifted to AI along with automation. This is very exciting.

Every one of us is standing on top of this giant. Now for NetBrain, what are we focusing on? We're going to let AI learn from a human. We'll let AI augment a human. This is a long road, a very exciting road. Every day we see something exciting and new and think about every problem that happened in the past. Slow automation through AI is going to help us automatically prevent and even diagnose cyber issues. That's unheard of, but that's the reality now and that's what NetBrain is working on.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach Prevention. Response. Notification. TODAY CyberEd.io

CIO.inc DeviceSecurity.io PaymentSecurity.io FraudToday.io

CYBER THEORY CyberEdBoard Xtra mile LIFECYCLE MARKETING GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io