C VISION INTERNATIONAL

AGENDA

AI-driven Cybersecurity

Security Innovations Forum

SPEAKERS

Francis de Souza
COO, Google Cloud
and President,
Security Products
Google Cloud

Google Cloud

Click Here to Register

September 29, 2026

Pacific Time

Registration 9:00 AM-9:30 AM

Breakfast & Morning Networking

9:30 AM-10:30 AM

Opening Remarks

10:30 AM-10:35 AM

KEYNOTE

10:35 AM-11:10 AM

The Agentic Revolution: Security, Trust, and the Future of AI

Agentic AI is rapidly transforming how work gets done across the enterprise. No longer limited to generating content or answering questions, AI systems are increasingly capable of reasoning, making decisions, and taking action on behalf of users. As organizations move from AI experimentation to deploying autonomous agents across business processes, software development, operations, and customer engagement, security leaders face a new challenge: how to enable innovation without losing control.

This keynote explores what it takes to secure the next generation of AI-powered enterprises. Attendees will examine the emerging risks associated with autonomous agents, including identity sprawl, data exposure, model misuse, and increasingly sophisticated AI-enabled threats. The discussion will also highlight the foundational capabilities organizations need to build trust in agentic systems, from secure-by-design architectures and Zero Trust principles to governance, observability, and continuous validation of AI actions.

Drawing on lessons from early adopters and industry trends, the session will provide a practical framework for balancing innovation, security, and resilience as AI becomes embedded into core business operations. Leaders will leave with a clearer understanding of how to prepare their organizations for a future where humans and AI agents work side by side, and where trust becomes the defining factor in successful AI adoption.

PANELISTS

Francis de Souza
COO, Google Cloud and President, Security Products
Google Cloud

KEYNOTE PANEL

11:15 AM-12:00 PM

Cyber Agentic Resilience: Securing Autonomous Enterprises

As organizations embrace Agentic AI to automate decisions, orchestrate workflows, and accelerate business outcomes, the cybersecurity landscape is undergoing a profound transformation. Autonomous AI agents are creating new opportunities for productivity and innovation, but they are also introducing new risks, from identity sprawl and unintended actions to data exposure and AI-driven attacks. Traditional security models, designed for human users and static systems, are being challenged by a world where intelligent agents can act independently at machine speed.

This executive panel will explore how leaders can build cyber resilience in an era where humans and AI agents operate side by side. The discussion will examine how organizations can securely deploy Agentic AI while maintaining visibility, governance, and trust across increasingly autonomous environments. Panelists will share perspectives on securing machine identities, establishing guardrails for autonomous decision-making, preparing for AI-enabled threats, and ensuring business continuity when AI systems become part of critical operations. As cybersecurity evolves into a strategic business imperative, attendees will gain insight into how leading organizations are balancing innovation, resilience, and risk to confidently navigate the next generation of digital transformation.

Networking Break

12:00 PM-12:30 PM

PANEL

Innovation Showcase: Agentic Defenses

12:30 PM-1:15 PM

Agentic AI is rapidly moving beyond copilots and assistants to become an active participant in business operations, analyzing information, making decisions, executing workflows, and interacting with systems with increasing levels of autonomy. As organizations embed AI agents across customer service, software development, operations, and security, the challenge is no longer simply adopting AI, it is ensuring these agents operate safely, transparently, and in alignment with business objectives. The rise of autonomous decision-making introduces new questions around trust, accountability, governance, and risk that traditional security and operating models were never designed to address.

This executive panel will explore what it takes to securely scale Agentic AI across the enterprise while maintaining confidence in the outcomes it produces. Leaders will discuss how to govern AI agents as they access sensitive data, make decisions, and take action across critical business processes; how to establish effective guardrails and human oversight; and how to build resilient architectures that can adapt as autonomous systems become increasingly embedded in day-to-day operations. Attendees will gain practical insights into balancing innovation with control, creating trust in AI-driven outcomes, and preparing their organizations for a future where AI agents become a core part of the workforce.

Lunch & Networking

1:15 PM-2:15 PM

FIRESIDE CHAT

The Agentic Enterprise: The True Measurable Business Value

2:25 PM-2:55 PM

As organizations move beyond AI experimentation, the conversation is shifting from what AI can do to the business outcomes it can deliver. Agentic AI represents the next evolution of enterprise transformation, enabling intelligent systems to not only generate insights, but also take action, coordinate workflows, and drive outcomes across the business. From improving customer experiences and accelerating decision-making to streamlining operations and unlocking new revenue opportunities, Agentic AI is changing how organizations create value.

This executive discussion will explore how business leaders are leveraging Agentic AI to improve productivity, increase agility, and drive growth at scale. Attendees will examine where autonomous AI is delivering the greatest impact today, what organizational and operational changes are required to realize value, and how leaders can move from isolated pilots to enterprise-wide transformation. The conversation will focus on practical lessons, measurable outcomes, and the leadership strategies required to build a more intelligent, efficient, and competitive organization.

DISRUPTOR

Innovations from Google: Defending Against Tomorrow's Threats, Today

3:00 PM-3:15 PM

Let's dive into the intersection of AI, the cyber arms race, and ransomware resilience. Ransomware attacks continue to escalate, inflicting substantial financial losses, data breaches, and tarnished reputations across sectors. As we navigate through 2024, businesses must comprehend the true implications of these attacks within their operational context. Despite achieving cybersecurity compliance, vulnerabilities persist, necessitating a deeper understanding of ransomware's impact and broader strategies for mitigating overall cyber risk exposure. Advanced AI technologies are shaping both offensive and defensive cyber strategies, offering proactive threat detection, comprehensive risk management frameworks, and insights to fortify cybersecurity posture against ransomware and beyond. Don't miss this opportunity to fortify your defenses and stay ahead in the AI-powered cyber landscape.

Networking Break

3:15 PM-3:35 PM

PANEL

AI Security From a Startup Perspective

3:35 PM-4:15 PM

Startups are moving fast to harness AI, but speed comes with unique security challenges. This panel brings together founders and security leaders from high-growth companies to share how they're protecting data, securing models, and building trust while scaling rapidly. Hear candid insights on balancing innovation with risk, tackling resource constraints, and shaping security strategies that can keep pace with startup agility.

Closing Remarks

4:15 PM-4:30 PM

Cocktail Reception

4:30 PM-5:30 PM

TOGETHER WITH

Google Cloud