BCG

Weekly Brief

May 13, 2026

Cybersecurity at the Speed of AI

As companies race ahead to develop AI, they are discovering that bad actors are racing even faster. AI allows attackers to hunt for vulnerabilities, generate realistic phishing content, clone voices, and impersonate executives on video.

About 60% of leaders believe they have already encountered an AI-enabled attack, according to a BCG survey of 500 senior leaders. Anthropic's unreleased large-language model, Claude Mythos, has discovered vulnerabilities in firewalls and IT infrastructure that have escaped detection for decades. It's only a matter of time before bad actors discover these and other security holes.

The Limits of Tech Solutions

Your IT and security teams are being pitched weekly if not daily by vendors with technology tools to detect and prevent attacks. But technology solutions only go so far.

The human side of cybersecurity is undervalued. Threats move at AI speed, while people figure things out in people time. Security teams are frequently brought in late to product and AI initiatives. Critical workflows, such as those involved in fixing vulnerabilities and managing access to systems, require cross-functional cooperation. Too often an urgent item for one team loses priority when it passes to a new team.

The best tools can't fix unclear ownership or clumsy handoffs. Companies need clear responsibilities and accountabilities that

define who does what and when.

A Human-Centered Approach

BCG's recent article, "Cybersecurity at the Speed of AI Requires Synchronicity" lays out a comprehensive approach to addressing this problem.It is based on our work over decades helping to protect clients and confirmed by a benchmarking study of leading companies.

Centralize authority, decentralize execution, enforce accountabilities. The CISO should be setting cybersecurity strategy, policy, standards, and risk appetite. The security team then handles specific tasks, like security architecture design, threat monitoring, security operations, and incident response.

Technology teams are responsible and accountable for implementing many of the policies and standards established by the CISO. Product and business teams operate within clear guardrails, defined by the security team.

This model works because the CISO sets the overall cybersecurity framework and is able to hold others accountable for its execution.

Start with a risk-based approach. Companies should build security into products from the start, involving security professionals continuously throughout ideation, design, build, launch, and operations.

Teams address risk tradeoffs, feasibility, and business value early on. This head start reduces late revisions that can delay launches and affect operations.

Redesign workflows before automating them. Things often fall apart when a task is handed off from one team to the next. AI cannot fix broken processes. But it can help accelerate workflows that have been redesigned around clear owners, defined service levels, and escalation rules. Automating redesigned workflows with AI ensures organizations are as hardened as possible against AI-based threats.

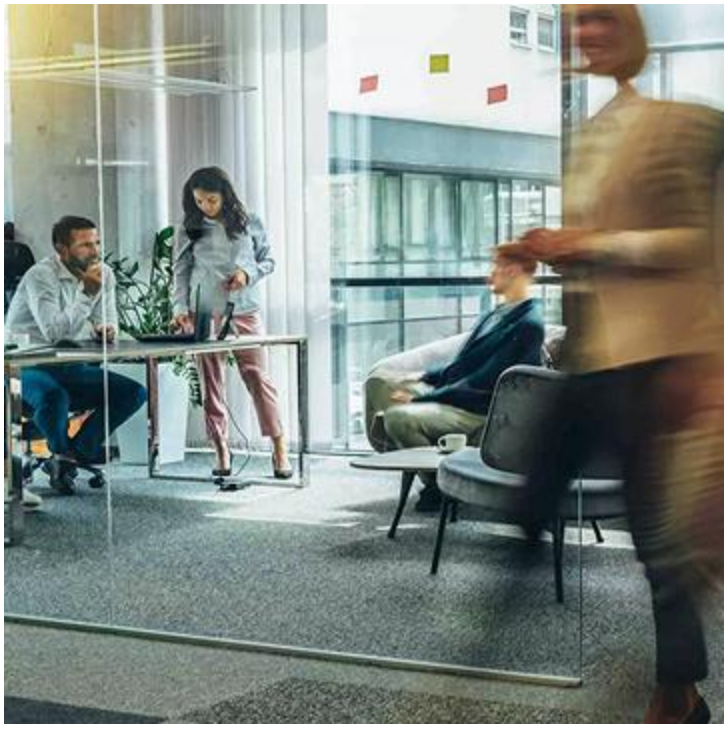
For example, AI can identify critical threats and vulnerabilities in a flood of alerts and block unsafe code the moment a developer writes it. By connecting scattered clues, AI can detect an attack and start the response without a human handoff.

***

As is true in so many areas, humans and AI working together unlocks success.

Christoph Schweizer
Chief Executive Officer

Further Insights



Cybersecurity at the Speed of AI Requires Synchronicity

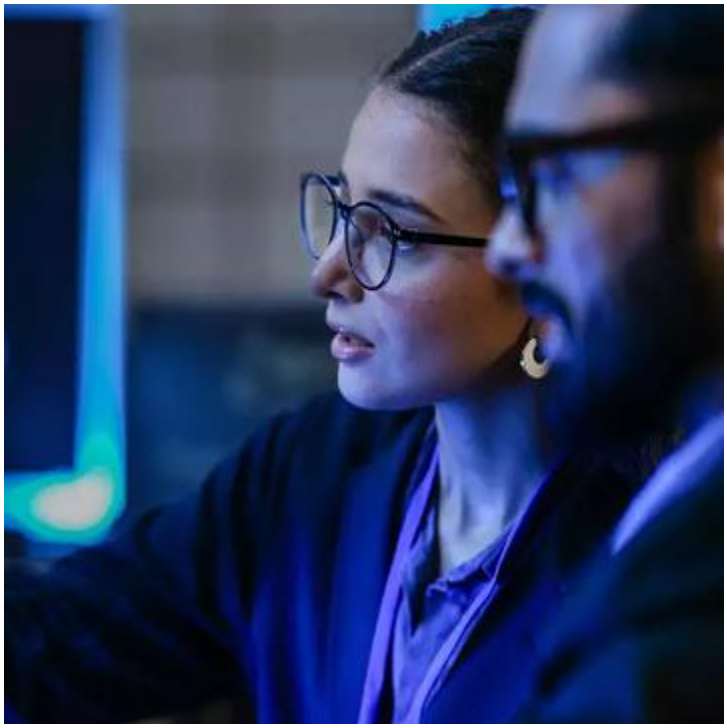
As Anthropic's Claude Mythos demonstrates, organizations need to fundamentally change how they do security. This AI model uses advanced reasoning to find vulnerabilities in firewalls and other infrastructure that have escaped detection for decades.

RETHINK CYBERSECURITY

Claude Security Is Now in Public Beta

Services partners such as BCG are now helping organizations deploy Claude-integrated security solutions.

DEPLOY AI IN SECURITY



AI Is Raising the Stakes in Cybersecurity

Bad actors are increasing their use of AI in cyber attacks faster than companies are responding. A global survey of senior leaders reveals the size of the gap.

SEE WHAT'S AT STAKE