

信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国 2026 RSA 热点研讨

暨第十八届信息安全高级论坛

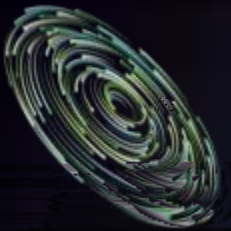
INFORMATION SECURITY HIGH LEVEL FORUM 2026





信息·趋势·感悟
THE POWER OF COMMUNITY STARTS WITH YOU
美国2026 RSA 热点研讨
暨第十八届信息安全高级论坛
INFORMATION SECURITY FUTURE 2026





信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国 2026 RSA 热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY 2026



Security must become ambient and autonomous

Ambient + Autonomous

Using agents for security for scaling defense

Agentic Defense Platform

Threat briefing, Alert triage, App lifecycle management, Red teaming, Data security posture, Conditional access, Policy configuration, Device offboarding, Access review

Agents must be secured with the same vigilance that we secure people

- 80% Of the Fortune 500 have active agents built using low- or no-code tools
- 29% Of employees have turned to unsanctioned AI agents for work tasks
- 47% Of organizations have security controls in place around GenAI use

We need to reimagine security for the agentic workforce

Protect the agents from the world

Protect the world from the agents

Detect & respond at machine speed

INTRODUCING DefenseClaw

Secure framework for AI agents



Threats in the AI Era

Speed Scale Sophistication

What Disruption Is (And Isn't)

- Active Defense & Hacking Back
- Imposing Costs On Adversaries
- Bringing Partners & Authorities Together

Four Pillars of Disruption

- Civil Legal Action
- Public Disclosure
- Technical Takedowns
- Product Hardening



信息·趋势·感悟

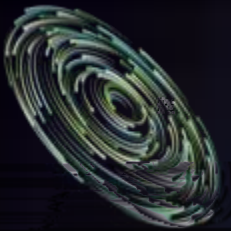
THE POWER OF COMMUNITY STARTS WITH YOU

美国 2026 RSA 热点研讨

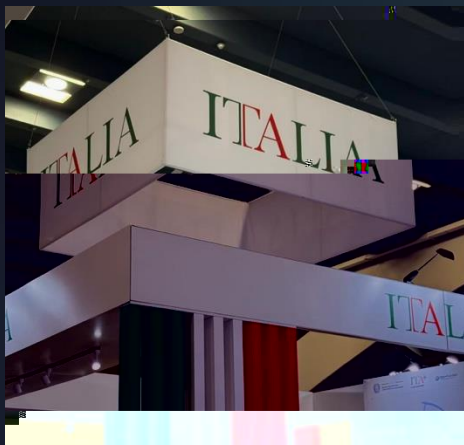
暨第十八届信息安全高级论坛

INFORMATION SECURITY FUTURE 2026





信息·趋势·感悟
THE POWER OF COMMUNITY STARTS WITH YOU
美国2026 RSA 热点研讨
暨第十八届信息安全高级论坛
INFORMATION SECURITY FUTURE 2026





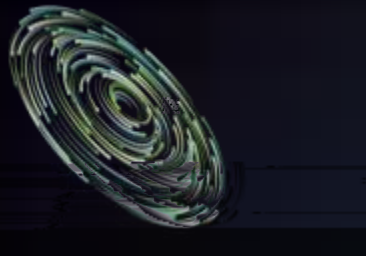
信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国 2026 RSA 热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY HIGH LEVEL FORUM 2026



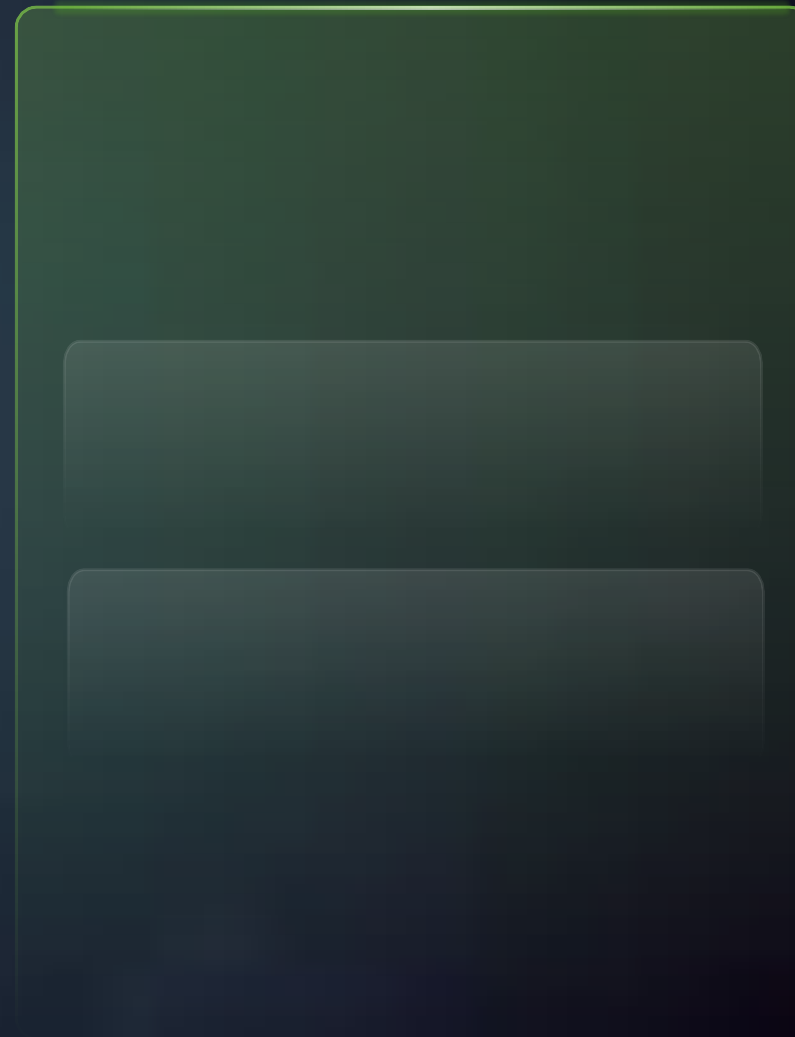
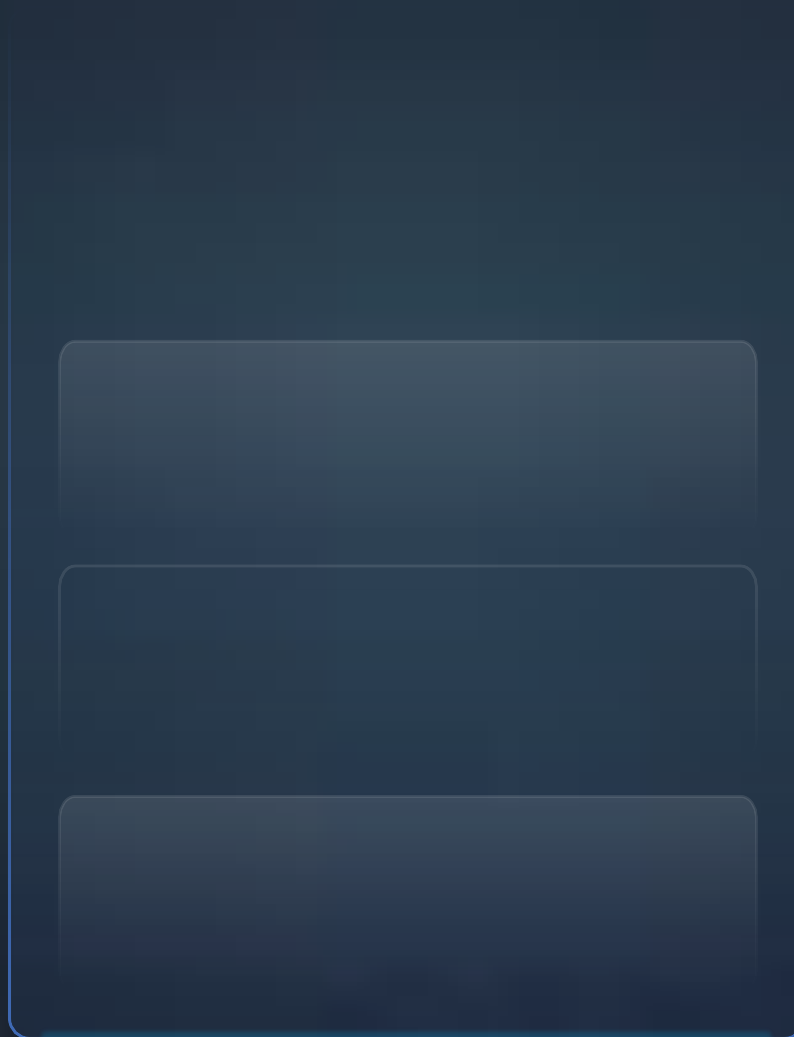
01

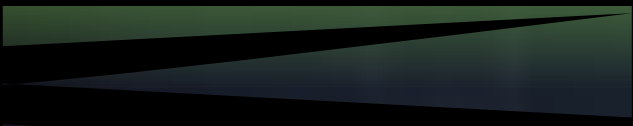
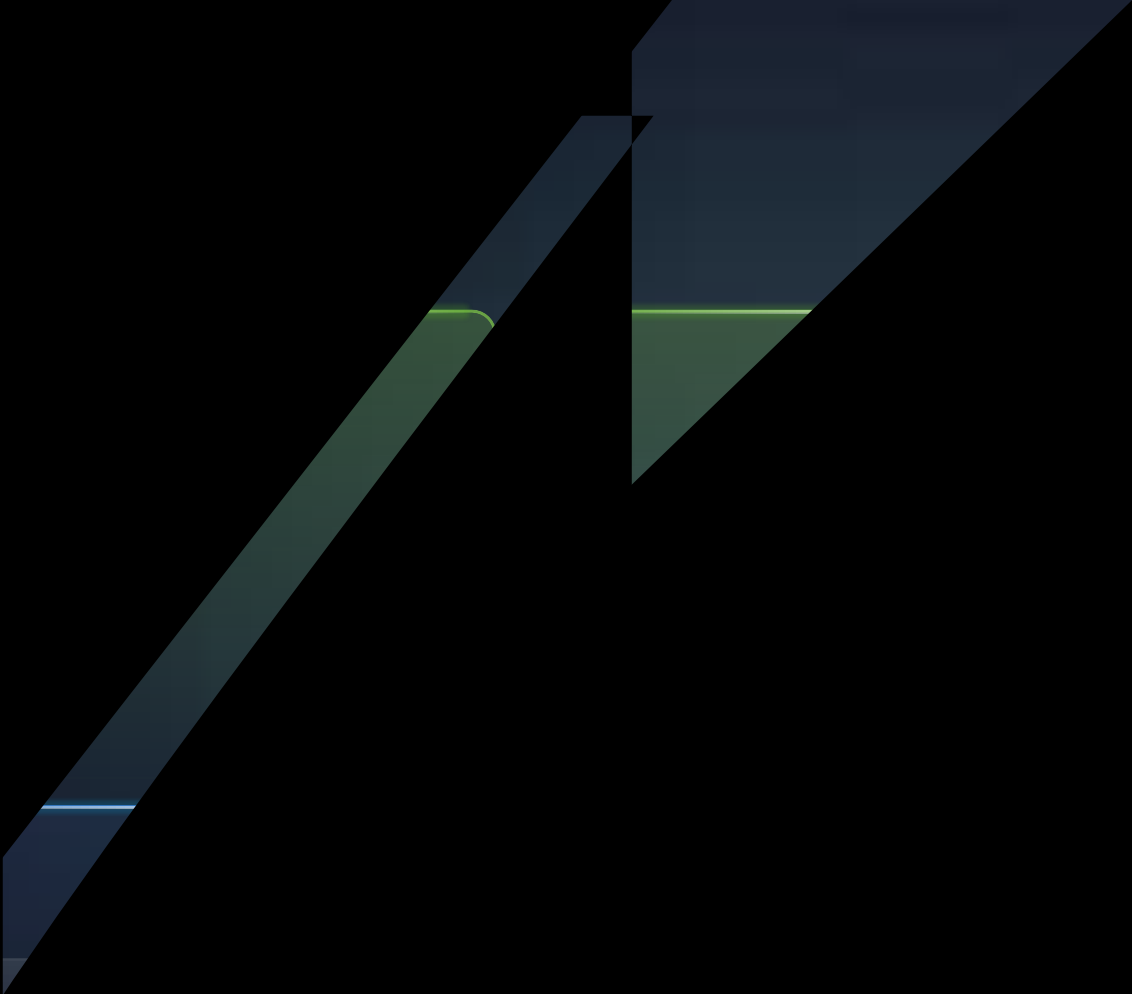
Beam 引擎

技术原理：注入式治理 (Context Injection)。不同于暴力阻断 (Kill Connection)，Beam 引擎在内向 AI 上下文窗口注入“确定性约束”。

引导 AI “自我修正”，而非强行关机

让安全成为 AI







信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国 2026 RSA 热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY FUTURE 2026

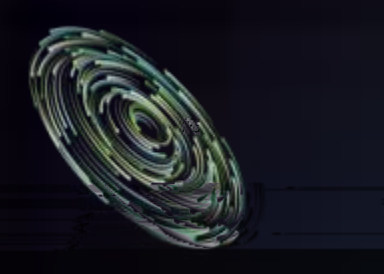
高摩擦

需要人工审核和
放行, 严重影响
效率

, 安全成为业务
阻力

低摩擦

通过上下文注入引导
AI自我修正, 而非强
制阻断



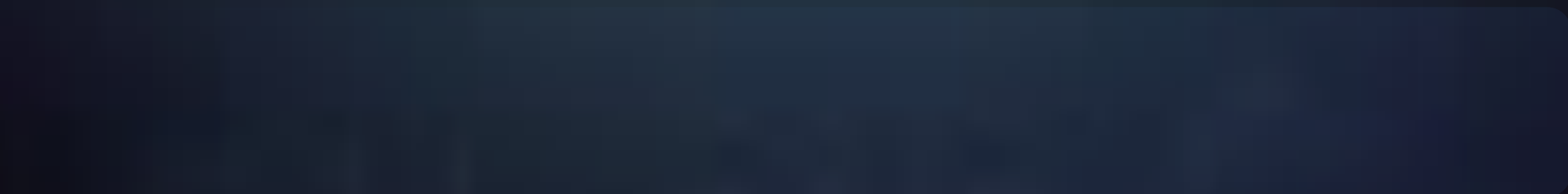
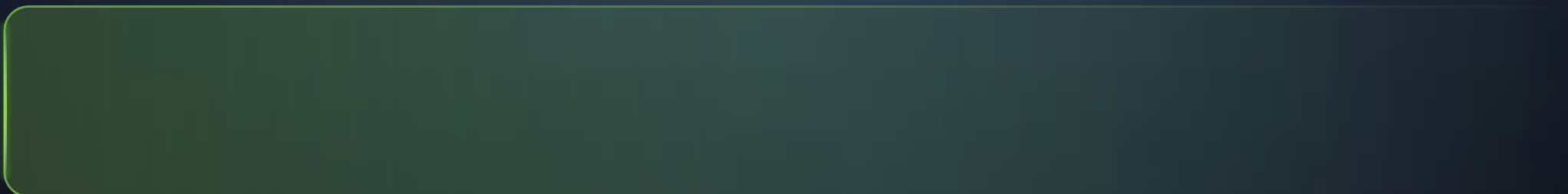
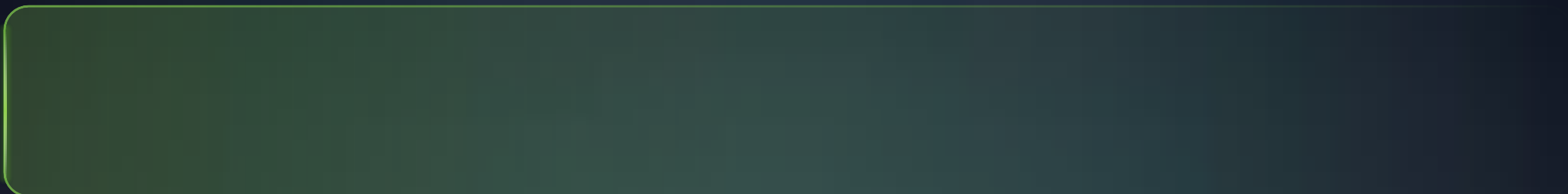
信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国 2026 RSA 热点研讨

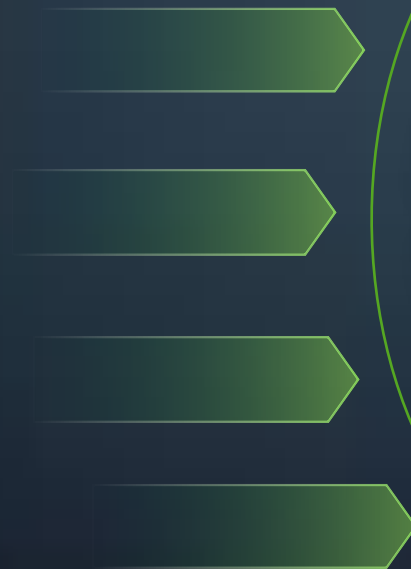
暨第十八届信息安全高级论坛

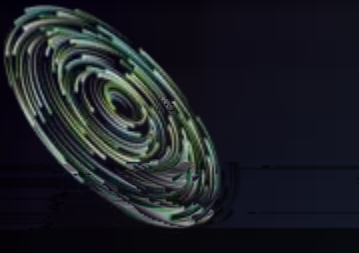
INFORMATION SECURITY FORUM 2026





信息·趋势·感悟
THE POWER OF COMMUNITY STARTS WITH YOU
美国 2026 RSA 热点研讨
暨第十八届信息安全高级论坛
INFORMATION SECURITY FORUM 2026





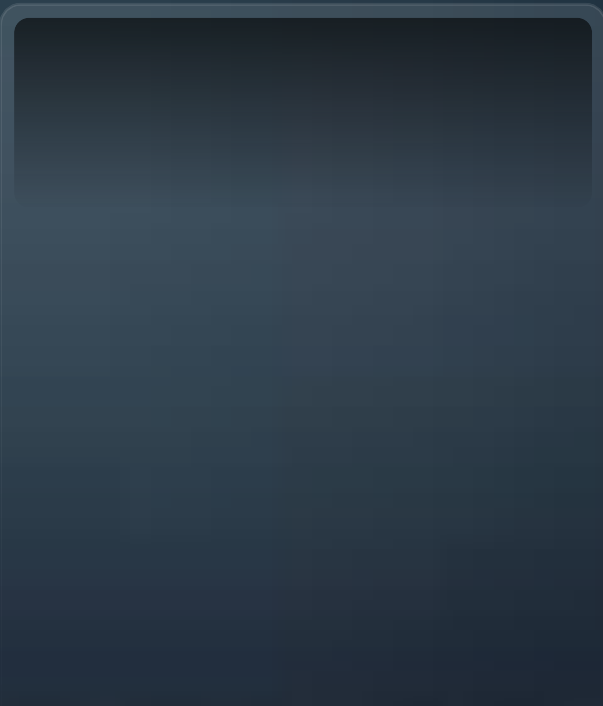
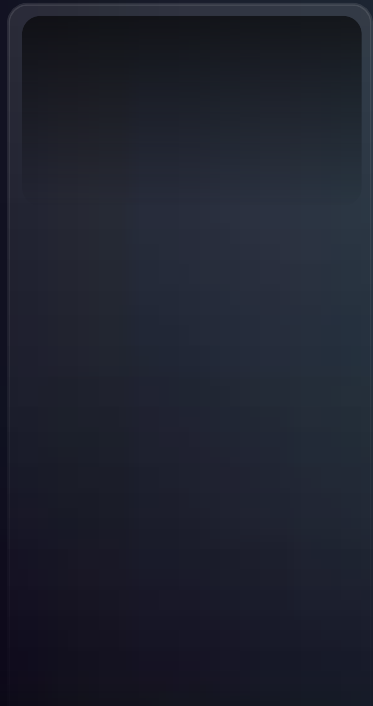
信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国 2026 RSA 热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY FUTURE 2026





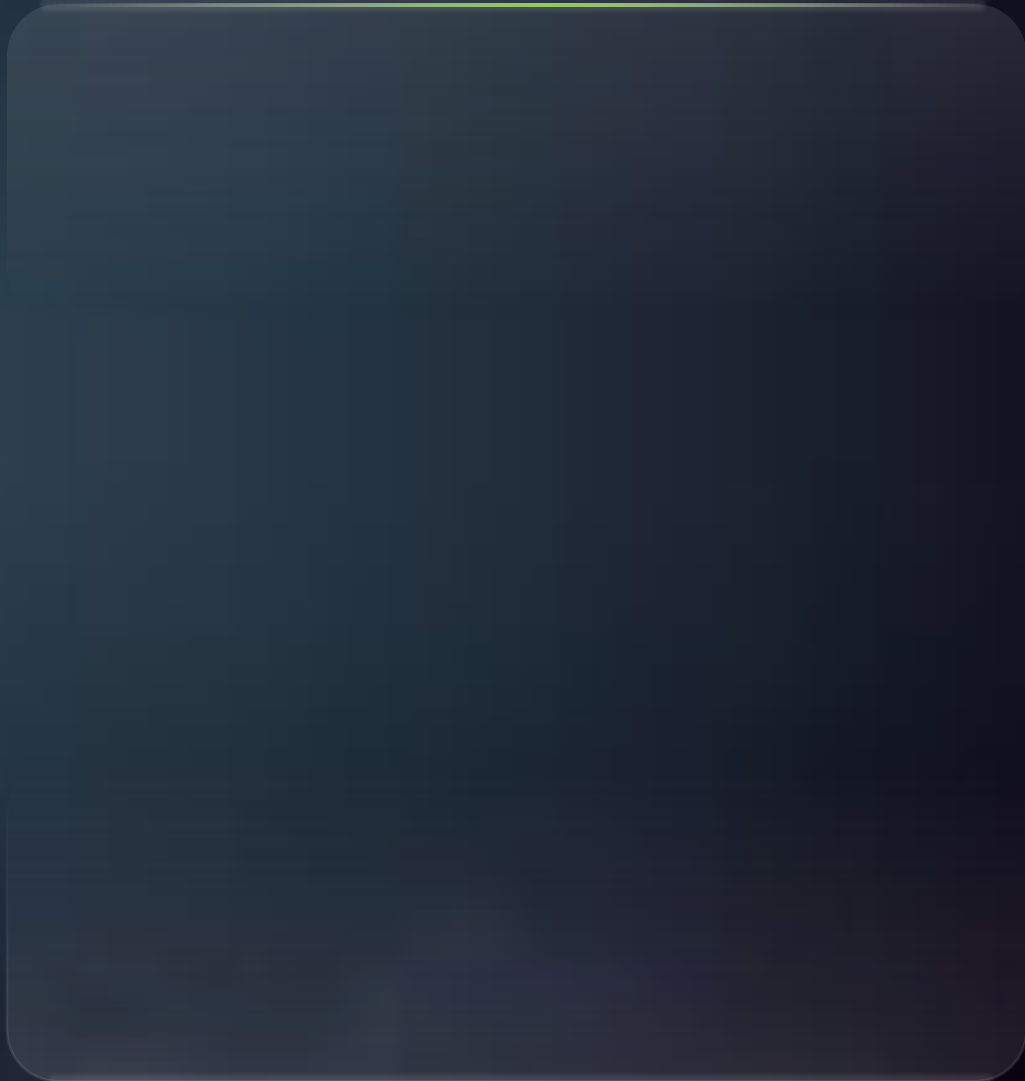
信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国 2026 RSA 热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY FUTURE 2026





信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国2026 RSA 热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY FORUM 2026



NSA



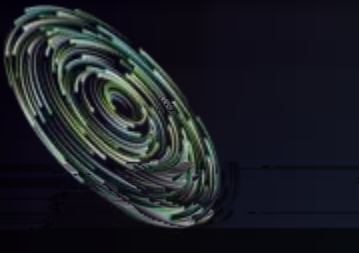
CISA





FBI



Jen Easterly



信息·趋势·感悟
THE POWER OF COMMUNITY STARTS WITH YOU
美国 2026 RSA 热点研讨
暨第十八届信息安全高级论坛
INFORMATION SECURITY FUTURE 2026

 **Claude** 
@claudeai

Introducing Claude Code Security, now in limited research preview.

It scans codebases for vulnerabilities and suggests targeted software patches for human review, allowing teams to find and fix issues that traditional tools often miss.

Learn more: [anthropic.com/news/claude-co...](https://anthropic.com/news/claude-code-security)
介绍 Claude 代码安全，现处于有限研究预览阶段。

它扫描代码仓库并设计针对性的软件补丁供人工审核，帮助团队发现并修复传统工具常忽略的问题。

了解更多: [anthropic.com/news/claude-co...](https://anthropic.com/news/claude-code-security)

 Forbes

AI Just Hacked One Of The World's Most Secure Operating Systems

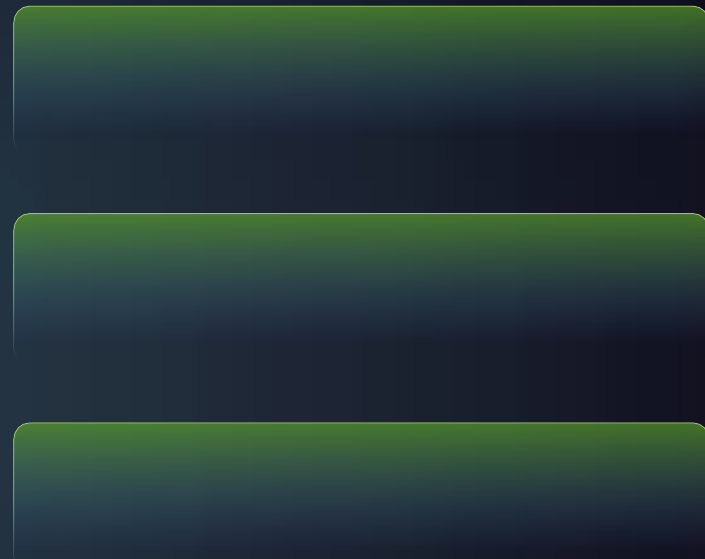
By Amir Husain, Contributor. @ Founder WQ... [Follow Author](#)

Published Apr 01, 2026, 08:38pm EDT. Updated Apr 01, 2026, 08:39pm EDT



An autonomous agent found, analyzed and exploited a FreeBSD kernel vulnerability in four hours. The implications for software security are profound.
PHOTOTEK VIA GETTY IMAGES

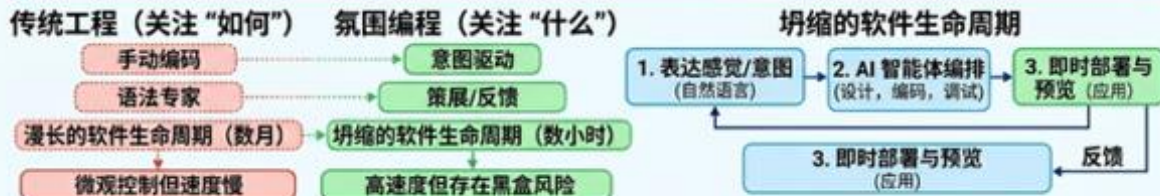
公众号·新智元





氛围编程 (Vibe Coding)：软件工程的范式转移

氛围编程：用自然语言向 AI 智能体描述“意图”和“感觉”

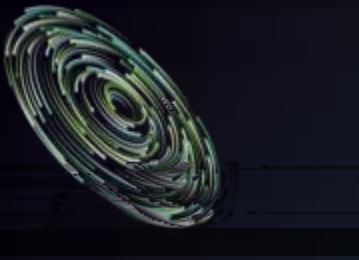


冲击

<p>技能转型</p> <p>旧程序员 vs 产品策展人</p> <p>策展优于编码。领域知识和用户体验 (UX) 至关重要。</p>	<p>民主化</p> <p>公民开发者崛起。技术壁垒降低。</p>	<p>经济转型</p> <p>开发成本趋向于零。Token 和算力优于薪资。</p>	<p>质量危机</p> <p>失去控制，可维护性，安全漏洞</p>
--	--	---	--

2026 共识：代码是廉价的；清晰描述“氛围”的洞察力是无价的。





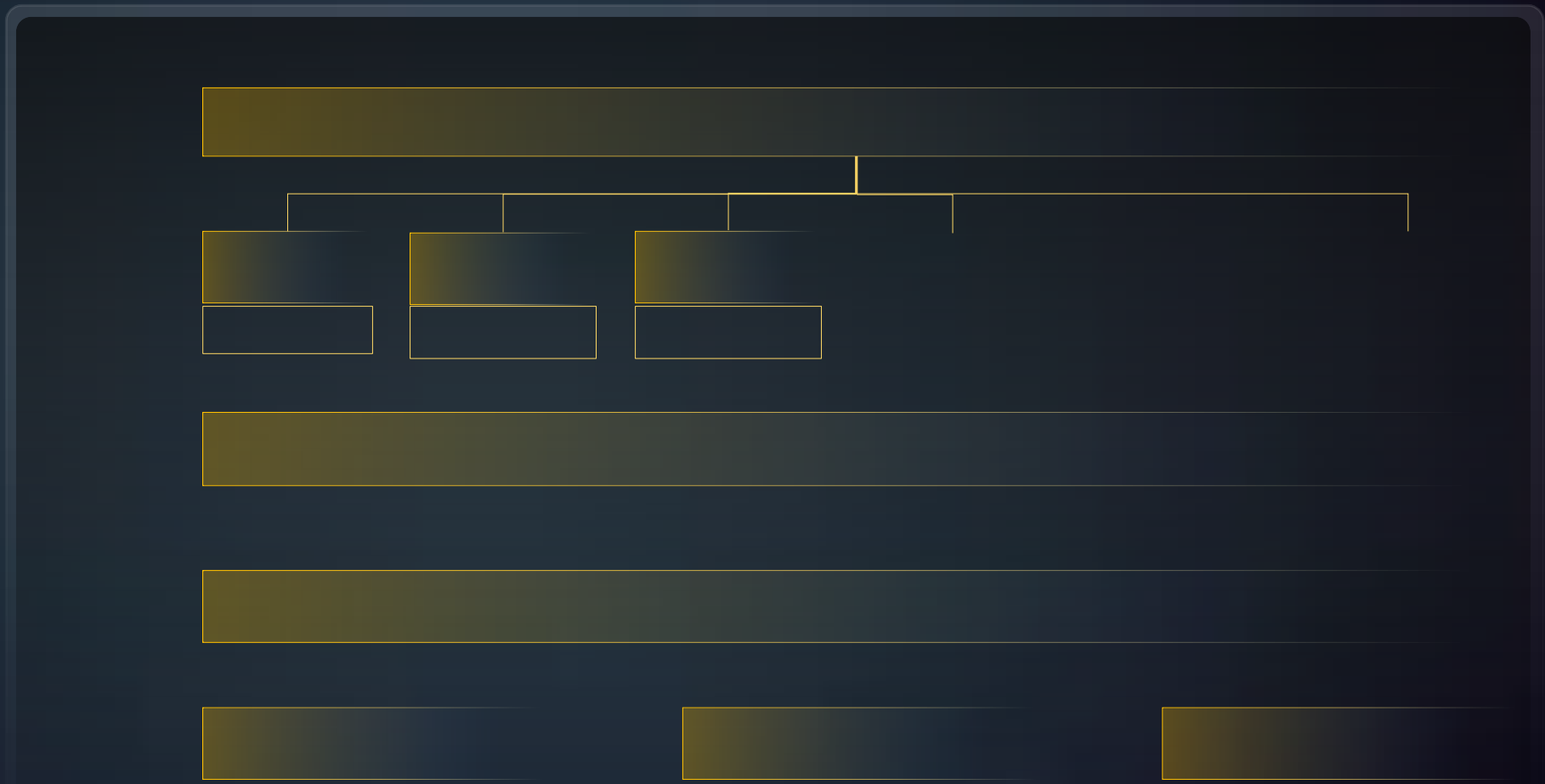
信息·趋势·感悟

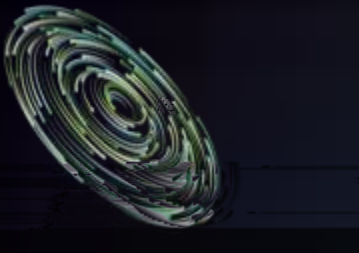
THE POWER OF COMMUNITY STARTS WITH YOU

美国 2026 RSA 热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY FORUM 2026





信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国 2026 RSA 热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY FUTURE 2026

开放性架构

构建标准化、模块化的安全原子能力，支持灵活组合与快速集成

智能体对接

实现与安全智能体的深度对接，支持自动化威胁检测与响应

信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国 2026 RSA 热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY HIGH LEVEL FORUM 2026

