Houlihan Lokey



Generative AI: The Next Frontier in Cybersecurity

July 2023

Table of Contents

I Houlihan Lokey Advises Armorblox in Generative AI Deal

II Generative AI: The Past and Present

III The Emerging Generative AI Market

IV Industry-Wide Adoption of Generative AI Tools

V About Houlihan Lokey

Houlihan Lokey Advises Armorblox in Generative AI Deal

Houlihan Lokey

Case Study: Houlihan Lokey Advises Armorblox Through High-Profile Cisco Acquisition

Armorblox

has been acquired by

Cisco

Sellside Advisor

Quick Facts

- Headquarters: Sunnyvale, CA
- Management:
  - CEO/Co-Founder: DJ Sampath
  - CPO/Co-Founder: Anand Raghavan
  - Chief Architect/Co-Founder: Arjun Sambamoorthy
  - Chief Data Architect/Co-Founder: Chetan Anand
- Customers: 58K+
- Total Funds Raised: $60M

Profile

- Armorblox, founded in 2017, secures enterprise communications over email and other cloud office applications and protects critical business workflows from compromise.
- Armorblox leverages deep learning algorithms, ML models, data science approaches, computer vision, and LLMs like GPT to understand the context of communications.
- Cisco (NASDAQ:CSCO) delivers innovative software-defined networking, cloud, collaboration, and security solutions.
- The Security Business Group continues to grow and is focused on cloud-based security, AI-driven threat detection, and end-to-end security architectures.

Armorblox

Rationale

- This transaction will allow Cisco to leverage Armorblox's use of predictive and generative AI across its portfolio, unlocking broad security use cases beyond email and changing the way its customers understand and interact with its security control points.
- The Armorblox team will join the Security Business Group, where they will work closely to bring generative AI-powered experiences to Cisco's Security Portfolio.
- Raj Chopra, SVP and Chief Product Officer of Security Business Group, highlighted how Cisco is taking an exciting step forward in executing its plans for an AI-first security cloud with its acquisition of Armorblox, a company that has pioneered the use of LLMs and natural language understanding in cybersecurity.

Our Role

- Houlihan Lokey served as the exclusive financial advisor to Armorblox.
- This transaction underscores the team's deep domain expertise and continued success advising clients in the cybersecurity sector.
- Houlihan Lokey worked collaboratively with management to strategically position the business, including developing materials on the expansive potential of Armorblox's technology within the Cisco security portfolio in support of Cisco's internal business case that was instrumental in securing the requisite buy-in.

Houlihan Lokey

Sources: Cisco Newsroom; PitchBook.

Case Study: Cisco Bolsters Generative AI Toolkit Through Armorblox Acquisition

Cisco's Platform-as-a-Service Cybersecurity Solution

Reduce Policy Complexity

AI-Powered Assistant

- The Cisco Security Cloud will leverage a generative AI-powered policy assistant that enables administrators to describe granular security policies and reason with the assistant to evaluate and produce more efficient firewall policies.
- The product will leverage customers' existing rulesets in Cisco Firewall Management Center to drive a tailored balance of efficiency and granular control.
- Armorblox's natural-language-understanding-based AI tools will improve the assistant's ability to contextualize user prompts against the Security Cloud's proprietary corpus of data.

Quickly Detect and Remediate Threats

SOC Assistant

- Cisco's SOC Assistant will support analysts as they work to detect and respond to threats faster.
- The assistant will contextualize events across the enterprise to generate comprehensive reports for SOC analysts.
- Armorblox's best-in-class AI-powered email security technology and contextualization capabilities will boost assistant efficacy, empowering SOC analysts to ensure network-wide security with a higher degree of certainty than ever before.

Cisco Live Technology Announcements



Generative AI Security Capabilities

New capabilities in the Security Cloud remove complexity, simplify policy management, and improve threat response.



Security Enhancements

Cisco Secure Access, Firewall 4200, and Multicloud Defense products lead the way to security in any environment.



Cloud Native Application Security

Enhanced capabilities provide full lifecycle protection in today's distributed, multi-cloud environments.



Full-Stack Observability

The FSO platform allows customers to develop and grow a robust application ecosystem on an open, extensible architecture.



Networking Cloud

The platform proactively manages the network, eliminates silos, assures performance, and reduces human workload.

Source: Company website.

II

Generative AI: The Past and Present

Houlihan Lokey

A Brief History of AI: From Machine Intelligence to Large Language Models…

1950
- Alan Turing introduces the concept of machine intelligence and proposes the "Turing test" as a measure of machine intelligence.

1961
- Ray Solomonoff lays the foundation for generative AI with algorithmic probability.

2006
- Geoffrey Hinton introduces deep learning that utilizes neural networks.

2016
- Google's DeepMind develops AlphaGo, an AI program that defeats world champion Go player Lee Sedol.

2018
- NVIDIA introduces StyleGAN, a generative model capable of producing high-quality synthetic images with diverse styles.

2020
- OpenAI introduces GPT-3, a massive language model with 175B parameters, demonstrating remarkable language understanding and generation capabilities.

2022
- DeepMind introduces AlphaFold2, an AI system that solves the protein folding problem, a longstanding challenge in biology.
- OpenAI introduced ChatGPT using GPT 3.5 as part of a free research preview.

1950s–1960s | **1980s–1990s** | **2000s–2010s** | **2020s–present**

1956
- John McCarthy organizes the Dartmouth conference—considered the birth of AI as a field of study.

1997
- IBM's Deep Blue defeats Kasparov in chess, showcasing the potential of AI in complex problem-solving tasks.

2014
- Ian Goodfellow publishes a groundbreaking paper on generative adversarial networks (GANs).

2017
- OpenAI releases the generative pre-trained transformer (GPT) model.
- Armorblox is founded.

2019
- OpenAI unveils GPT-2, a language model that generates coherent and contextually relevant text.
- Armorblox emerges from stealth with natural language understanding (NLU) platform.

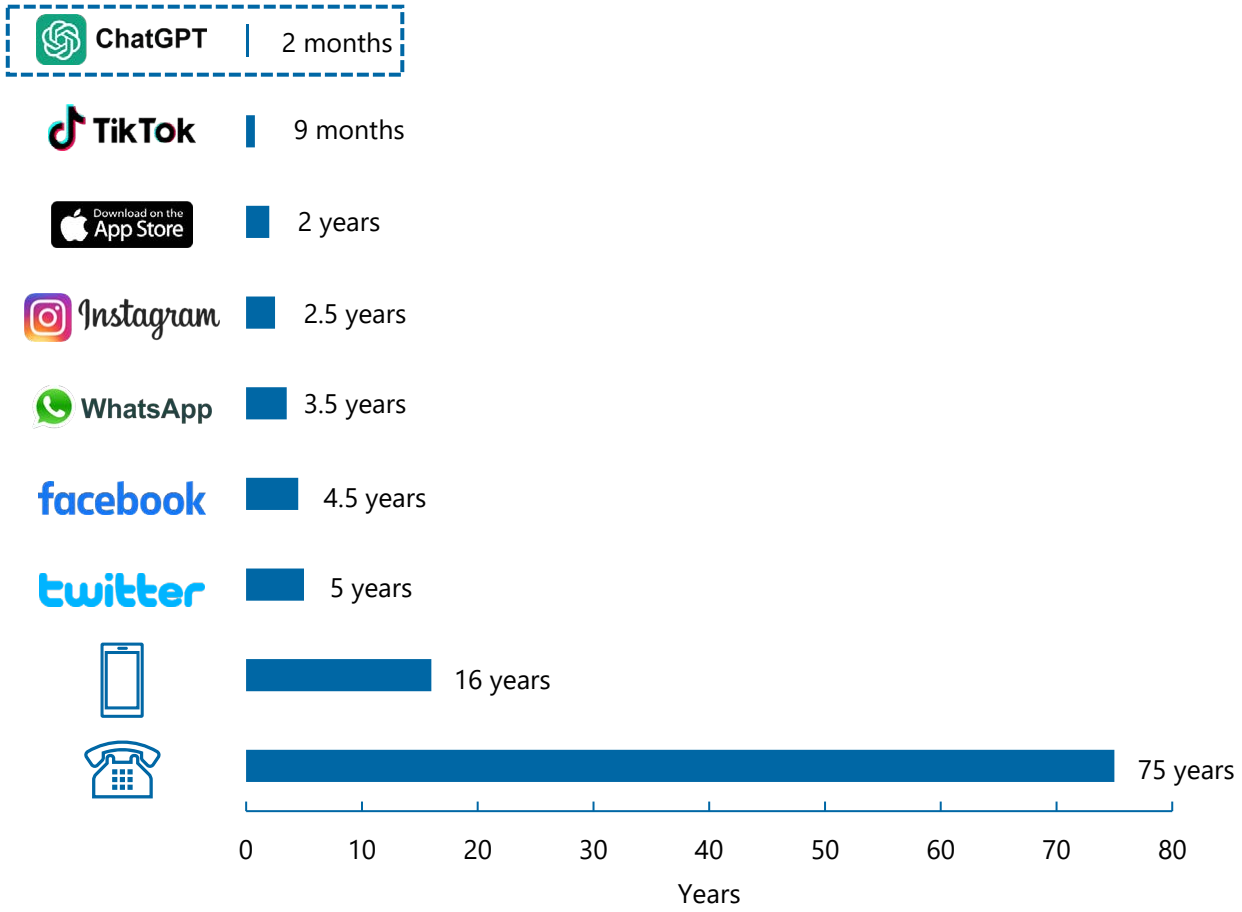
2021
- OpenAI develops DALL-E, an AI model capable of generating unique images from text.
- OpenAI launches ChatGPT API for developers, marking initial availability for external use.

2023
- Jan. 23: MSFT announces $10 billion multi-year investment into OpenAI.
- Feb. 2: ChatGPT reaches 100 million users, making it the fastest-growing consumer app in history.
- Feb. 7: MSFT releases AI Co-Pilot and Chat for Bing and Edge.
- Mar. 14: Anthropic introduces Claude, its ChatGPT alternative; OpenAI introduces ChatGPT-4 with 1T parameters.
- Mar. 21: Google introduces Bard, its ChatGPT alternative.
- May 16: OpenAI CEO Sam Altman appears in a Senate subcommittee hearing on the oversight of AI; discusses the need for AI regulation that doesn't slow innovation.
- May 31: Cisco announces intent to acquire Armorblox.

...Spurred on by the Launch of ChatGPT

Fastest-Growing Consumer App in History

Time to 100M Users



ChatGPT Stats

$14B
Total Invested Capital

$29B
Valuation

$100M+
Monthly Active Users

1.8B+
Monthly Website Page Views

60M
Average Daily Active Users

18–34
Most Popular Demographic

Countries Leading Adoption

Sources: PitchBook, Reuters, World of Statistics.

III

The Emerging Generative AI Market

Houlihan Lokey

Large and Rapidly Growing Market Driving Significant VC Investment

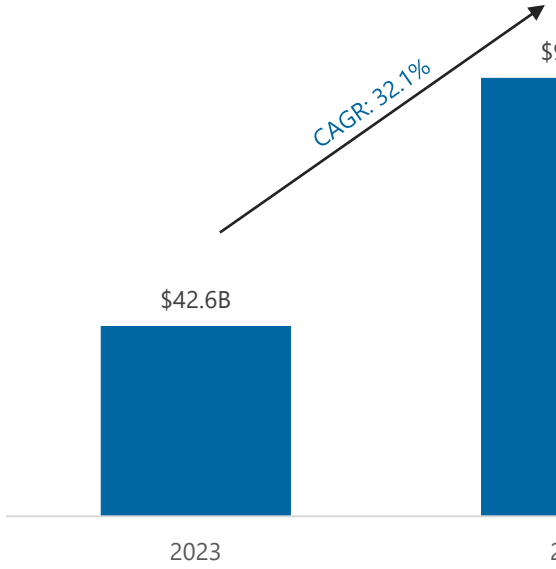
Generative AI Represents Massive Potential

- Already a large market opportunity, the generative AI market is expected to grow at a 32.1% CAGR between 2023 and 2026 based on current enterprise use cases.
- Generative AI-relevant use cases already present a significant enterprise opportunity—estimated to reach $42.6 billion in 2023—with natural language interfaces offering the largest market due to customer service and sales automation use cases.
- The potential of generative AI to expand the total addressable market of AI software to consumers and new user personas in the enterprise represents an additional upside to current forecasts.

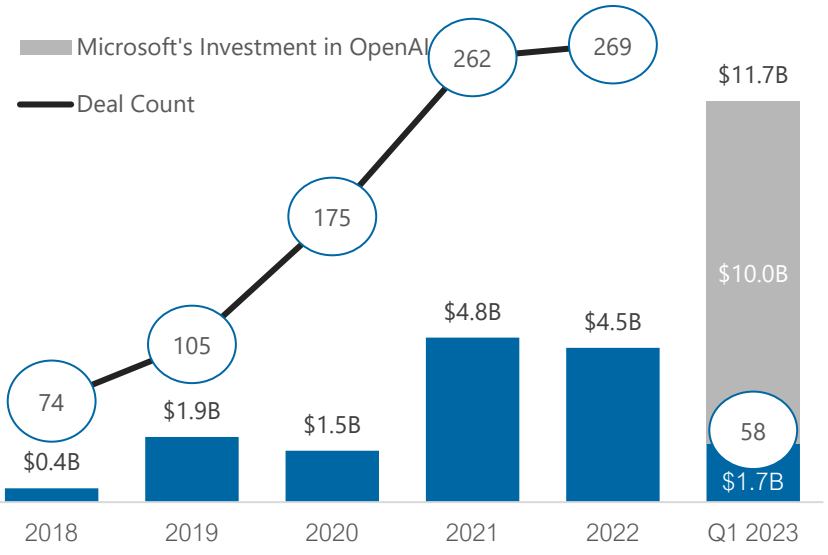
VC Funding of Generative AI Remains Robust Despite Macroenvironment

- VC investment activity in generative AI startups continues at a frenzied pace, despite an otherwise challenging environment for early-stage investment firms as an emphasis on efficient growth has emerged.
- The immense potential for generative AI and wide-ranging applications create a highly attractive secular opportunity for VC investors.
- With relatively low barriers to entry and plentiful funding, the space is becoming increasingly competitive as nascent startups seek to capitalize on the enthusiasm for the sector and tackle new and existing problems.
- The highly technical nature of generative AI, the rapidly evolving landscape, and a plethora of startups entering the market are driving investors to put significant weight on underwriting the knowledge and vision of founders when considering which companies to back.

GENERATIVE AI MARKET SIZE*



GENERATIVE AI VC FUNDING ACTIVITY



MOST ACTIVE VC INVESTORS IN GENERATIVE AI

Alumni Ventures · Amplify Partners · andreessen horowitz · Bloomberg BETA · Index Ventures · khosla ventures · SEQUOIA · SOMA CAPITAL · South Park Commons · TIGERGLOBAL

SELECT VC ACTIVITY IN CYBERSECURITY AI

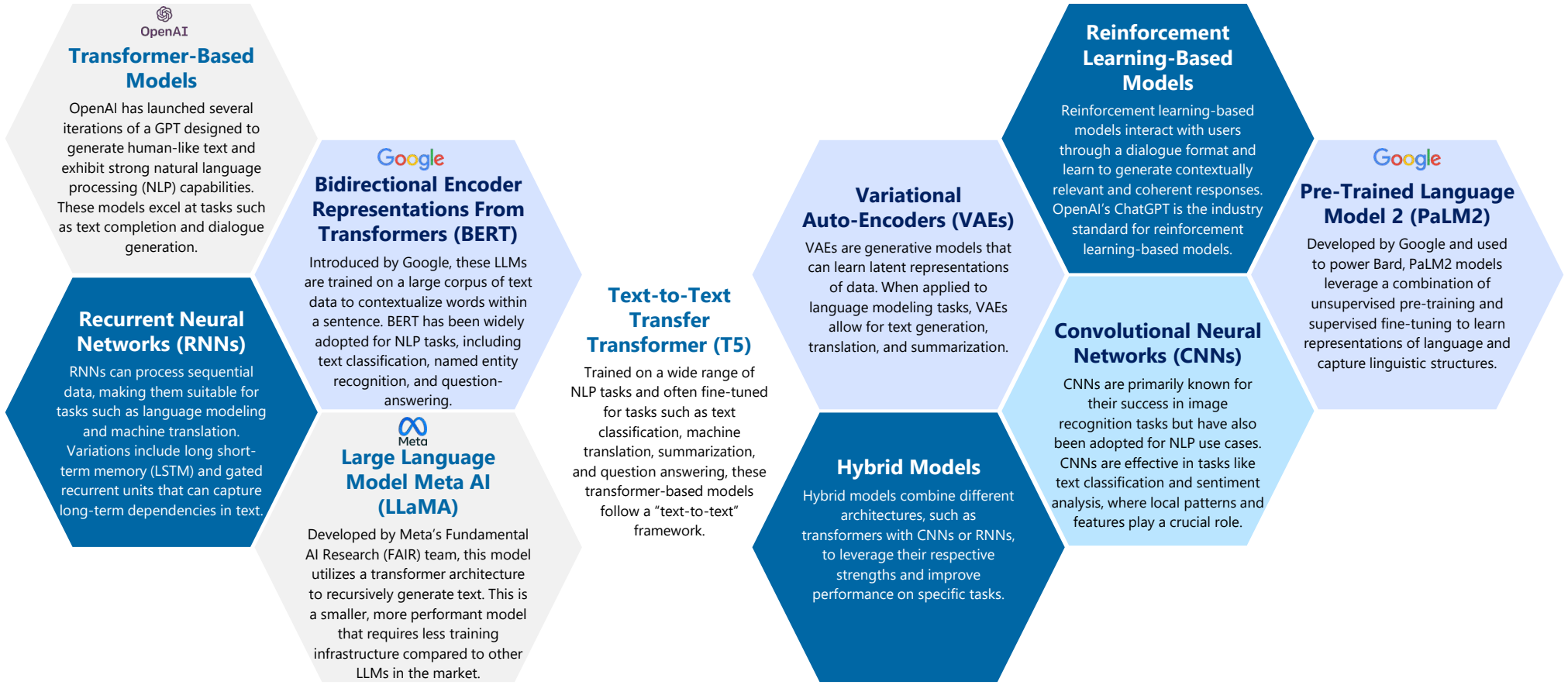
(Date and Amount Raised)

CALYPSOAI	hazy	Protect AI	HIDDENLAYER
June '23: $23M	Mar. '23: $9M	Dec. '22: $14M	July '22: $6M
Deepkeep ML SECURITY	credo ai	ROBUST INTELLIGENCE	
June '22: $7M	May '22: $13M	Dec. '21: $30M	

Source: PitchBook
** Based on market consensus estimates*

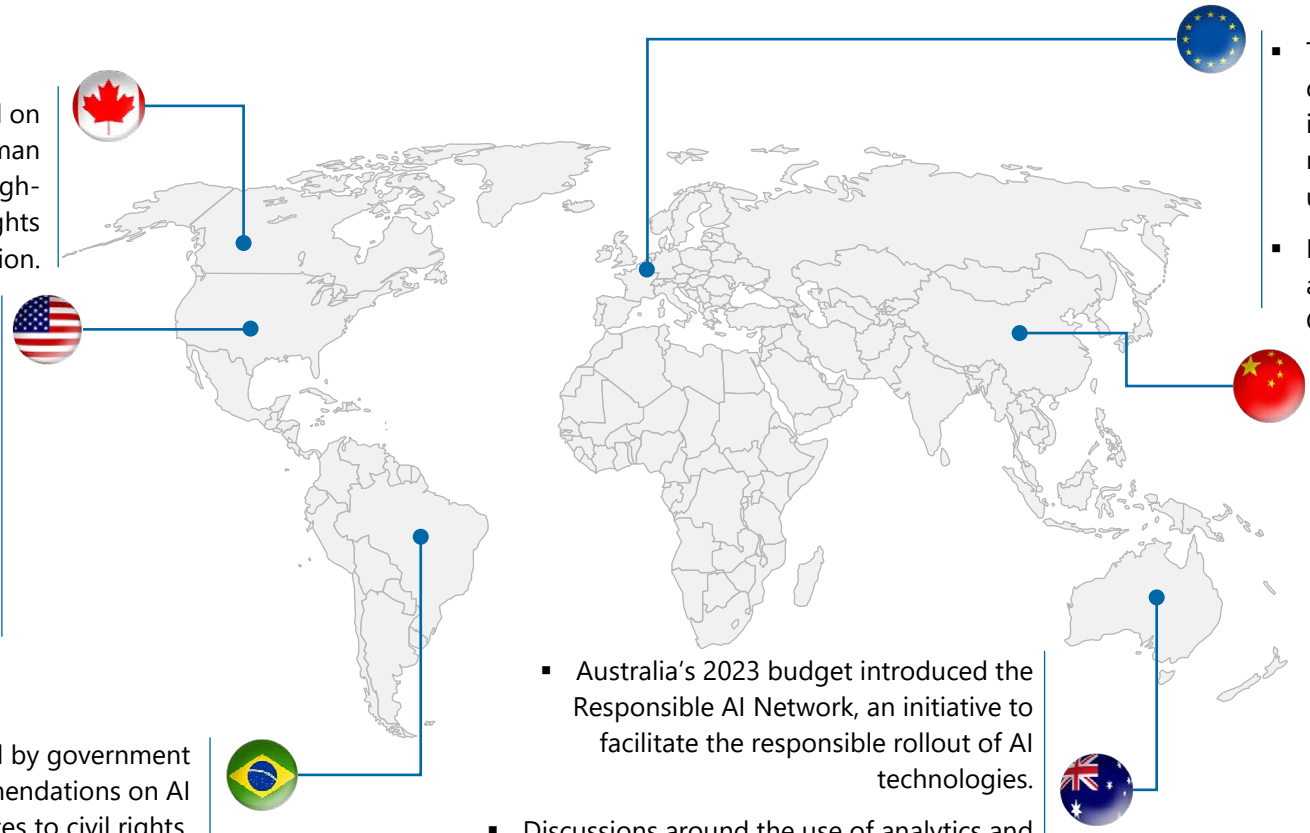
The Rapid Proliferation of Large Language Models (LLMs) in the Enterprise…

With the pace of innovation in AI (significantly outperforming Moore's Law), enterprises are rapidly integrating AI into their solutions by implementing "public" LLMs or developing their own LLMs. Securing these models and the underlying data is imperative, and while the regulatory environment is evolving, enterprises must take a proactive approach to ensure AI governance.



...Is Driving a Nascent but Evolving Regulatory Landscape

Concerns around AI are not new, but with the rapid growth of generative AI after the public launch of ChatGPT, regulators are on notice with discussions over regulation of generative AI heating up in the EU, U.S., and around the world driven by concerns over privacy, transparency, copyright/IP, discrimination, and accountability.



- Legislation planned for 2025 will build on existing consumer protection and human rights laws to recognize the need for "high-impact" AI systems to meet human rights and safety legislation.
- In Senate testimony, OpenAI CEO Sam Altman proposed creating an AI regulatory agency and requiring licensing for companies.
- Others suggest requiring transparency on training data and establishing clear frameworks for AI-related risks.
- California lawmakers are taking the lead on the oversight of AI with a bill that would monitor how industries use automated decision tools.
- Current reports debated by government officials detail recommendations on AI regulations as it relates to civil rights, categorization of risks, governance measures, and sanctions.
- The EU requires that AI-generated content be disclosed to consumers to prevent copyright infringement, illegal content, and other malfeasance related to end users' lack of understanding.
- Italy briefly banned ChatGPT before restoring access following updates made by OpenAI to ChatGPT's privacy policies.
- The Cyberspace Administration of China (CAC) is currently drafting AI-related regulations that would target services that generate text, images, video, code, and other media.
- Tech companies would have to register generative AI models with CAC before releasing products, and data used for training purposes would have to meet strict requirements.
- Australia's 2023 budget introduced the Responsible AI Network, an initiative to facilitate the responsible rollout of AI technologies.
- Discussions around the use of analytics and biometrics data to train models continue, calling for additional privacy protection.

Source: Industry.Gov, DLA Piper, NY Times, ISED, Data Guidance, LOC.Gov, CNBC, Reuters.

Leveraging Generative AI in Cybersecurity: Enhancing Defense Against Evolving Threats

Threat Landscape



NEW THREATS NECESSITATE REVOLUTIONARY SECURITY

- The cybersecurity threat landscape has continued to evolve with increasingly sophisticated and dynamic threats.
- This new environment requires proactive defense mechanisms that can adapt and counteract emerging risks, enabling intelligent, automated responses to threats.

AI-Enhanced Defense Capability



OUTSMART THE ATTACKER

- Generative AI algorithms train on vast amounts of historical data related to cyber threats, attack patterns, and vulnerabilities.
- Models trained on relevant data generate synthetic examples of potential cyber threats, helping security teams proactively identify and mitigate vulnerabilities.

Untapped Potential and New Investment



RAPID RATE OF CHANGE

- The rush to incorporate generative AI into cybersecurity products was evident at the RSA Conference, with many vendors showcasing the technology.
- The efficacy of these products depends on the availability of high-quality, diverse data rather than the choice of underlying LLMs.

Current Use Cases



Threat Intelligence and Prediction

- Models can analyze massive amounts of historical data and generate insights that aid in predicting and understanding emerging threats.
- By identifying patterns, these models help security analysts prioritize defense strategies.



Malware Detection and Analysis

- Algorithms can be trained on large datasets of malware samples to recognize common features, behaviors, and characteristics.
- This enables the creation of advanced malware detection systems that can identify and neutralize new malware strains.



Anomaly Detection

- LLMs aid in anomaly detection by modeling normal system behavior and identifying deviations from established patterns.
- By continuously learning from network traffic, user behaviors, and system logs, generative AI models can flag suspicious activity.



Detecting Generative AI Text in Attacks

- Identifying AI-generated text in attacks can help to detect phishing emails, polymorphic code, and atypical email address senders, checking if underlying links in text lead to known malicious websites.



Autonomous SOC

- SOC teams can hand off repetitive tasks to AI assistants while focusing on hunting, investigating, and responding to threats.
- Automation is not designed to replace humans but to maximize the human potential to think critically about systemwide defense.

Leveraging Generative AI in Cybersecurity: Advantages Drive Improved Security Outcomes

Scalability and Efficiency



- Generative AI algorithms can process and analyze massive amounts of data quickly, making them ideal for large-scale cybersecurity operations.
- Automating time-consuming tasks such as threat analysis and pattern recognition empowers security professionals to focus on higher-level tasks.

Reduces False Positives



- By learning from real-world data, generative AI can significantly reduce false positives and improve the accuracy of threat detection.
- This results in more efficient incident response and reduced response times.

Adaptability to Threats



- Generative AI models, with their ability to learn from data and generate new insights, can adapt and respond rapidly to emerging threats.
- Implementing generative models increases the agility of security teams as adversaries leverage generative AI tools to generate unique attacks.

Leveraging Generative AI in Practice

Problem:

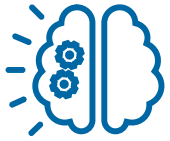
Signature-based network intrusion detection systems (NIDS) fail to stop malicious shellcode due to **false positives**.



- NIDS are essential for monitoring and identifying malicious network traffic.
- Shellcode patterns can be difficult to distinguish from benign network traffic, and this threat vector, if successful, allows attackers to access conventional computer systems and cyber-physical systems, such as smart grid infrastructure.
- Shellcode is frequently used as a payload in system penetration tools due to the enhanced access and further leverage they offer to an attacker.

Solution:

An updated IDS is built using a **recurrent neural network (RNN) LLM**.



- RNNs are inspired by the behavior of biological neurons and can capture long-term dependencies in text.
- Researchers at De Montfort University proposed the use of RNNs to combat malicious shellcode by monitoring the dataset and flagging any activity identified as malicious.
- The ability of RNNs to be adaptively tuned and capture highly complex and nonlinear relationships between both dependent and independent variables without prior knowledge makes the model a strong potential solution to this problem.

Results:

An **RNN-based IDS** that flags shellcode with **more frequency and reduced false positives** compared to a signature-based IDS.



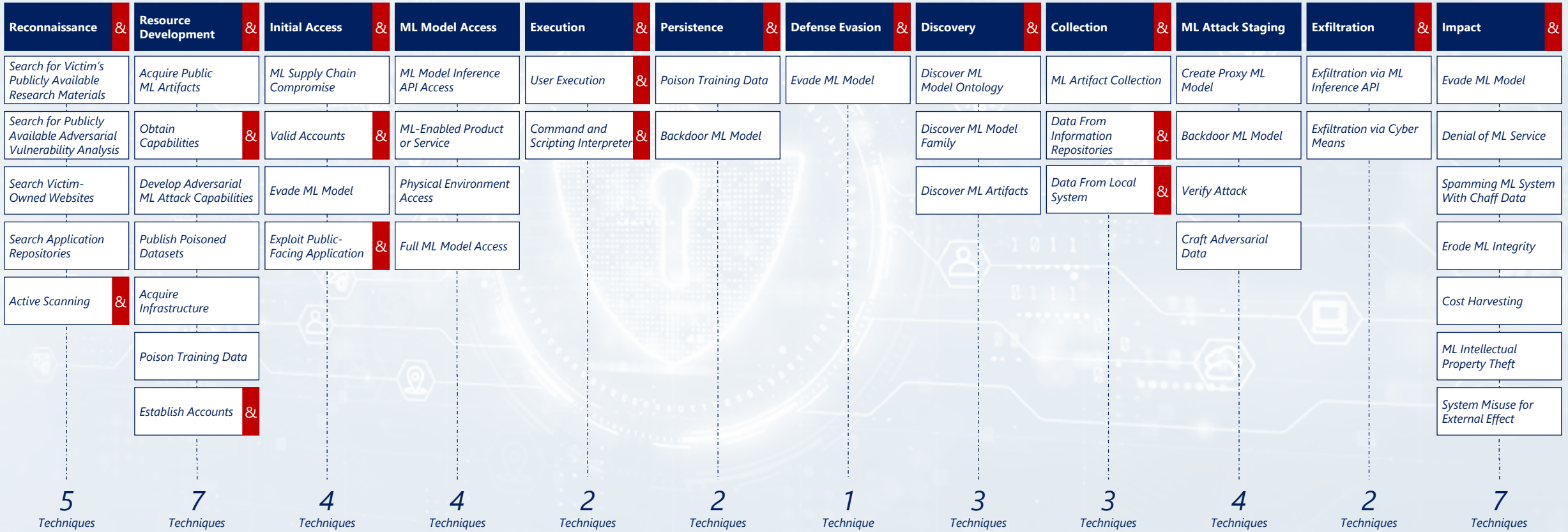
- Researchers tested the new detection methodology using repeated 10-fold cross-validation for accuracy on a dataset of 400,000 samples to examine the false positive rate.
- The neural network architecture was 98% accurate and produced a false positive rate of under 2%, compared to 90% false positive rates in signature-based systems.
- Findings of the study were validated by SentinelOne, supporting the efficacy of using RNNs to deliver improved outcomes.

Sources: SentinelOne Blog, "Malicious Input: How Hackers Use Shellcode"; Shenfield, Alex and Day, David & Ayesh, Aladdin, "Intelligent Intrusion Detection Systems Using Artificial Neural Networks"; Subba, B., Biswas, S., and Karmakar, S., "False Alarm Reduction in Signature-Based IDS: Game Theory Approach."

Adversarial Threat Landscape for Artificial Intelligence Systems (ATLAS)

MITRE ATLAS™ is a knowledge base of adversary tactics, techniques, and case studies used by researchers to navigate the machine learning (ML) threat landscape successfully. An evolving regulatory landscape, the growing number of vulnerabilities in ML, an expanding attack surface, and new attack vectors are driving the accelerated development of solutions focused on protecting ML models.

ATLAS



Source: MITRE.
Note: "&" indicates an adaptation from ATT&CK.

Generative AI Landscape in Cybersecurity

Hyperscalers

amazon
Google
Microsoft

ML Security

ADVERSA
ADVERUM
AIShield Powered by Bosch
CALYPSOAI
CRANIUM
Deepkeep ML SECURITY
deepki
HIDDENLAYER
preamble
Protect AI
ROBUST INTELLIGENCE
TROJ.AI

Endpoint/EDR

CROWDSTRIKE
DARKTRACE
SentinelOne

Security Operations

ANVILOGIC
CISCO

ML Data Privacy

BigID
EDER LABS
gretel
hazy
inpher
Opaque
PRIVATEAI
Sarus

ML Governance and Compliance

calvinrisk
credo ai
DataRobot
FAIRLY
Holistic AI
preamble
Verta

IAM

sensity

Threat Intelligence

FLASHPOINT
Recorded Future
zignal LABS

Application Security

VERACODE

ML Observability

aporia
arize
Arthur
deepchecks.
fiddler
hyperwise
Sigma Roc
SOLASAI
truera
WHYLABS

Risk and Compliance

SecurityScorecard

Email Security

Abnormal
Armorblox
SLASHNEXT

Web Security

TALON

ML Development

ANTHROPIC
cohere
Google
Hugging Face
Meta
Microsoft
OpenAI

IV

Industry-Wide Adoption of Generative AI Tools

Houlihan Lokey

Industry-Wide Adoption of Generative AI Tools

On May 30, 2023, CrowdStrike introduced Charlotte AI, a generative AI security analyst that uses the world's highest fidelity security data and is continuously improved by a tight feedback loop with CrowdStrike's threat hunters, managed detection and response operators, and incident response experts.

Charlotte AI Use Cases

- **Generative AI as a Democratizing Force—Every User Becomes a Power User:**
  - Charlotte AI will be available to every user of the Falcon platform, helping them to better understand the threats and risks facing their organization.
  - Charlotte AI can provide real-time insight into an organization's risk profile, including its threat landscape, risk level against critical vulnerabilities, current security posture, compliance requirements, and cybersecurity performance metrics.
- **Elevating Security Analysts With AI-Powered Threat Hunting:**
  - Charlotte AI can help less experienced IT and security professionals make better decisions faster, reducing response times to critical incidents.
- **Make Advanced Security Actions Easier and Automate Mundane Tasks:**
  - Charlotte AI is the ultimate force multiplier, automating repetitive and tedious tasks like data collection, extraction, and search and detection.
  - The product further accelerates enterprise-wide XDR use cases across every attack surface and third-party product, directly from the Falcon platform.

Darktrace, a leading provider of cybersecurity solutions, is using its advanced AI technology, including Darktrace DETECT™ and RESPOND™, to protect more than 8,400 customers worldwide from security and privacy risks associated with generative AI tools and LLMs, enabling businesses to leverage the power of AI safely and responsibly while guarding against potential threats and data breaches.

Overview

- Darktrace DETECT™ and RESPOND™ use generative AI to detect and prevent potential IP loss and data leakage, ensuring comprehensive risk management and compliance across the enterprise.
- Darktrace's risk and compliance models learn from customer data to understand day-to-day norms of users, assets, and devices, autonomously detecting and responding to subtle anomalies that can manifest in future threats.
- Informed by proprietary Self-Learning AI, Darktrace's Cyber AI Loop, an interconnected, comprehensive set of dynamically related capabilities, ensures that data, people, and businesses stay protected from cyber threats.

> "In May 2023, Darktrace Self-Learning AI detected and prevented an upload of over 1GB of data to a generative AI tool at one of its customers."
>
> **—Darktrace Blog**

Sources: Company websites, Silicon Angle.

Industry-Wide Adoption of Generative AI Tools (cont.)

On Palo Alto Networks' fiscal year 2023 Q3 earnings call, CEO Nikesh Arora announced plans to launch its own proprietary LLM "in the coming year" and ultimately sees "significant opportunity as we begin to embed generative AI into our products and workflows."

Vision for Incorporating Generative AI

- Generative AI will help the company improve core detection and prevention efficacy within its portfolio.
- Implementation of generative AI tools will provide a more intuitive and natural-language-driven user experience with products.
- Generative AI will drive significant efficiency in internal processes and operations across the platform.

Arora contended that generative AI would offer a disproportionate advantage to organizations that are large and have significant amounts of data, framing Palo Alto Networks as well positioned to benefit from the rise of generative AI in cybersecurity.

At RSA Conference 2023, SentinelOne unveiled a threat-hunting platform called Purple AI for its singularity platform, which seamlessly fuses real-time, embedded neural networks and an LLM-based natural language interface, supercharging users with AI to monitor and operate all security data, boost productivity, and scale operations.

Purple AI in Practice

- Built on the industry's most performant security data lake, the SentinelOne threat-hunting platform aggregates and correlates information from device and log telemetry across endpoint, cloud, network, and user data to deliver insight and recommend response actions that can be immediately executed—from mitigation and investigation to endpoint, cloud, and user management.
- Purple AI allows threat hunters to ask questions about specific, known threats and get fast answers without needing to create manual queries around indicators of compromise.
- Users can also leverage Purple AI to ask questions about suspicious activity they may not have been able to define themselves (unknown unknowns).
- Within seconds, Purple AI will provide insights on the identified behavior alongside recommendations, thus reducing the need to manually analyze and stitch together diverse events into one contextual story.

Sources: Company websites.

Industry-Wide Adoption of Generative AI Tools (cont.)

FLASHPOINT

Flashpoint, in partnership with Google Cloud, is deploying generative AI within the Flashpoint Intelligence Platform to revolutionize how organizations detect security threats and reduce risk, enabling more intuitive decision-making and empowering organizations to maximize the value of their intelligence investment while mitigating cybersecurity risks.

Flashpoint Intelligence Platform and the Use of Generative AI



- Flashpoint announced an expansion of its partnership with Google Cloud and will leverage Security Workbench capabilities to revolutionize threat detection and risk reduction for organizations, enabling security professionals to improve decision-making processes.



- Using NLP, the platform will transition from the traditional search-based interaction model to a conversation-based experience, enabling organizations to enhance the value of their intelligence investments, bridge the cybersecurity skills gap, and swiftly mitigate risks.



- Flashpoint's collaboration with Google Cloud utilizes AI-driven intelligence innovations such as optical character recognition (OCR) and in-platform video search to process and contextualize images and videos, resulting in significant fraud prevention and risk mitigation use cases across various industries.

> With this collaboration, we aim to empower organizations with faster and more comprehensive insights into potential cyber, physical, and fraud threats, enabling them to stay one step ahead in the ever-evolving landscape of cybersecurity.
>
> **—Josh Lefkowitz, CEO, Flashpoint**

SecurityScorecard

At the 2023 RSA Conference, Security Scorecard announced the launch of the first and only security ratings platform to integrate with OpenAI's GPT-4 system.

SecurityScorecard Overview



- Developed by ScorecardX, the innovation incubator of SecurityScorecard, this solution enables cybersecurity leaders to find immediate answers to high-priority cyber risks by leveraging its NLP capability.



- ScorecardX developed a natural language global search, enabling CISOs and practitioners to ask questions to better understand their cybersecurity exposure and where their security gaps lie.



- Customers can ask open-ended questions about their business ecosystem, including details about their vendors, and quickly obtain answers to drive risk management decisions.

> Our team members are squarely focused on driving innovation that helps our customers increase cyber resilience in the face of global threats… It's that commitment that has led us to put game-changing AI technology in our customers' hands, enabling them to be more proactive, move faster, and be more strategic for their organizations.
>
> **—Aleksandr Yampolskiy, CEO and Co-Founder, SecurityScorecard**

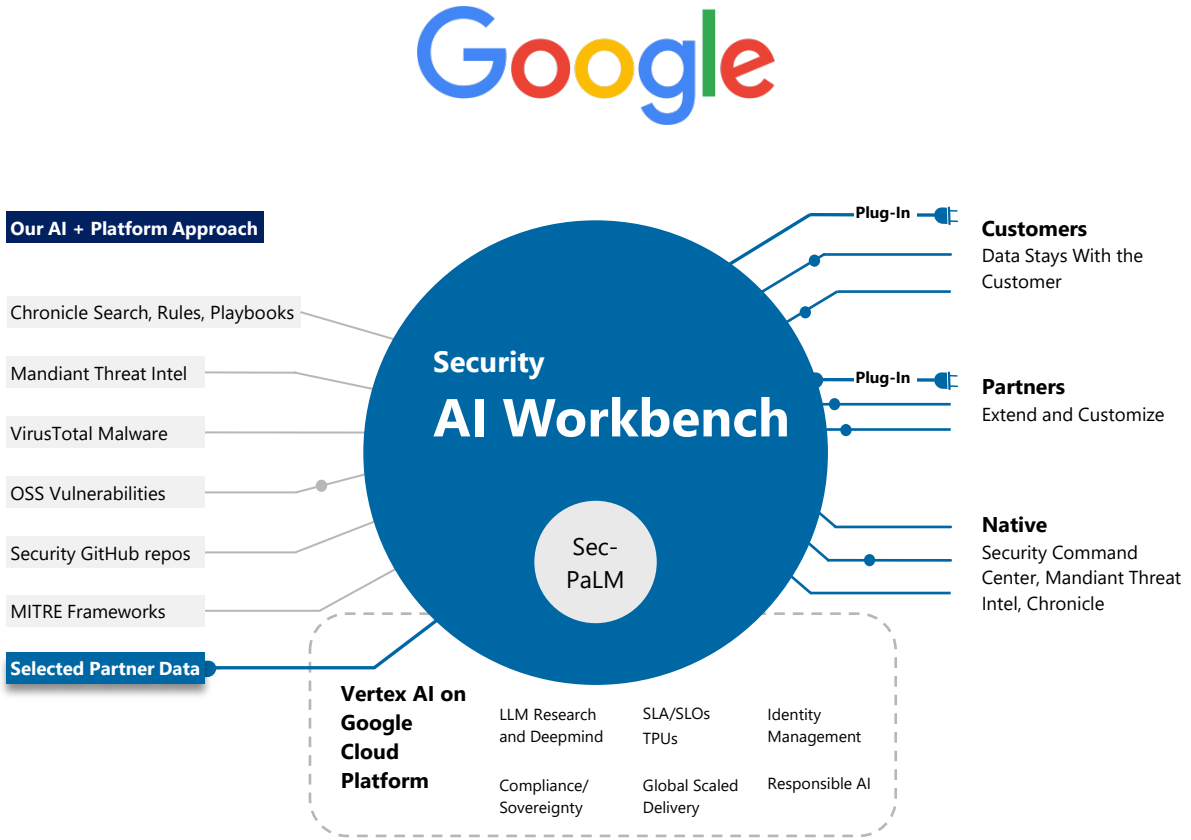
Sources: Company websites, Silicon Angle.

Industry-Wide Adoption of Generative AI Tools (cont.)

At RSA Conference 2023, Google announced its Cloud Security AI Workbench, an industry-first extensible platform powered by its specialized security model, Sec-PaLM, which is fine-tuned for security use cases, incorporating unsurpassed intelligence through Google's visibility into the threat landscape and Mandiant's frontline intelligence on vulnerabilities, malware, threat indicators, and behavioral threat actor profiles.

Security AI Workbench Capabilities

Prevent Threats From Spreading:	
VirusTotal Code Insight	▪ Uses Sec-PaLM to analyze and explain the behavior of potentially malicious scripts and will be able to better detect which scripts are actual threats.
Mandiant Breach Analytics for Chronicle	▪ Automatically alerts users to active breaches and uses Sec-PaLM to help contextualize and respond instantly to critical findings.
Reduce Toil:	
Assured OSS	▪ Uses LLMs to help Google add more open-source software (OSS) to its OSS vulnerability management solution.
Mandiant Threat Intelligence AI	▪ Built on top of Mandiant's massive threat graph, this product will leverage Sec-PaLM to quickly find, summarize, and act on relevant threats.
Close the Talent Gap:	
Chronicle AI	▪ Searches billions of security events and interacts conversationally with the results, asks follow-up questions, and quickly generates detections, all without learning a new syntax or schema.
Security Command Center AI	▪ Provides AI-powered risk summaries for security, compliance, and privacy findings.

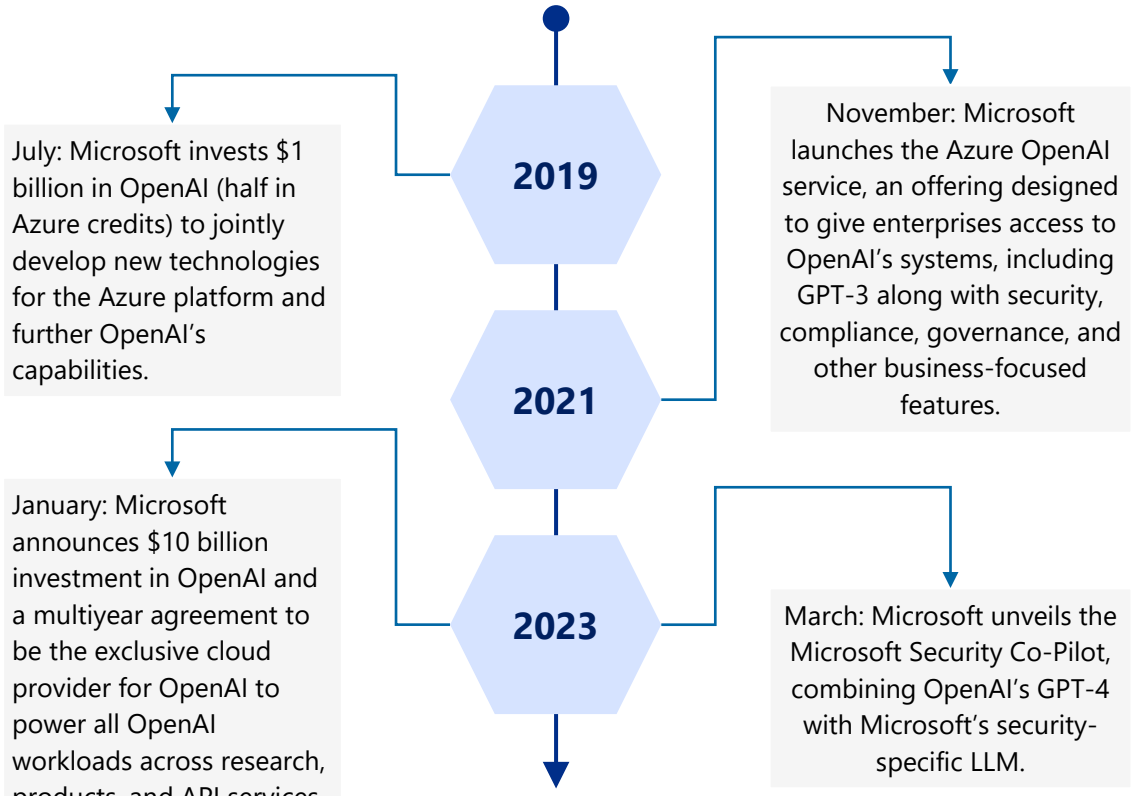


Sources: Sunni Potil, VP/GM, Google Cloud Security, via Google Cloud Blog.

Industry-Wide Adoption of Generative AI Tools (cont.)

Microsoft

Microsoft and OpenAI Collaboration



Microsoft Security Co-Pilot Capabilities

Self-Training

- Cyber-trained model adds a learning system to create and tune new skills, which translates into gains in the quality of detection, speed of response, and ability to strengthen security posture.

Threat Intelligence

- Incorporates a growing set of security-specific skills and leverages the trillions of security signals gathered as part of Microsoft's threat intelligence operation.

Threat Prioritization

- Surfaces prioritized threats in real time and anticipates a threat actor's next move with continuous reasoning based on Microsoft's global threat intelligence.

Addresses Talent Gap

- Boosts the security team's skills with its ability to answer security-related questions while continually learning from user interactions, adapting to enterprise preferences, and advising on the best course of action to achieve more secure outcomes.

User Development

- Provides users with critical step-by-step guidance and context through a natural-language-based investigation experience that accelerates incident investigation and response.

Sources: Company websites.

Industry-Wide Adoption of Generative AI Tools (cont.)

Recorded Future

At the 2023 RSA Conference, Recorded Future announced the launch of its AI platform, which incorporates its 100+ terabyte intelligence cloud and 10+ years of threat reporting experience with OpenAI's GPT LLM to provide a host of benefits for both executives and analysts.

Recorded Future AI Capabilities

- Trained on 10+ years of threat analysis data from Insikt Group, Recorded Future's threat research division, combined with the insights of the Recorded Future Intelligence Graph.
- Automatically collects and structures data related to both adversaries and victims from text, imagery, and technical sources, and uses NLP and ML to analyze and map insights across billions of entities in real time.
- Provides real-time threat landscape analysis and actionability at an internet scale, enables analyst efficiency to help compensate for skills shortages, and provides intelligence-driven insights so organizations can make decisions before adversarial activity impacts business outcomes.

VERACODE

At the 2023 RSA Conference, Veracode released Veracode Fix, a GPT-based ML model trained on Veracode's proprietary dataset that includes more than 85 million fixes over nearly two decades, excels at fixing insecure code, and dramatically reduces the time needed to remediate flaws.

Use Case: Veracode Fix

- Unlike scanning tools that only find flaws, Veracode Fix generates secure code patches that developers can review and implement to remediate security flaws without manually coding a fix.
- Developers can reduce both the introduction of flaws and vulnerabilities in code as well as the accumulation of security debt over the lifetime of an application.
- By reducing the time and effort required to fix flaws, organizations can improve security posture and lower risk, accelerate time to market and compliance, and realize operational efficiencies, with initial support for Java and C#.

Sources: Company websites.

Industry-Wide Adoption of Generative AI Tools: Startup Names to Watch

CALYPSOAI

CalypsoAI, a pioneer in AI security (AISec), raised $23 million in a Series A financing round led by the Paladin Capital Group as it continues to develop and deliver AISec solutions that empower enterprises and governments to leverage the immense potential of generative AI solutions and LLMs responsibly and securely.

Overview

- The recent $23 million Series A values Calypso at $58 million with a total of $38 million raised since the company was founded in 2018 by Neil Serebryany to help organizations accelerate their use of AI technologies.
- Built for government customers, CalypsoAI's VESPR Validate product facilitates AI-empowered decision-making by streamlining model testing timelines, stress-testing models, and using natural language to maintain performance visibility.
- Recently announced product CalypsoAI Moderator is an LLM-agnostic model security tool for enterprise users that features rapid deployment, data loss prevention, jailbreak prevention, and malicious code detection.
- CalypsoAI provides solutions to a diverse range of end users across government, finance, technology, and pharmaceuticals, delivering critical tools for multifaceted model testing in the ever-evolving regulatory environment of generative AI.

CRANIUM

Cranium, which seeks to ensure trust and security in AI models and allows organizations to map, monitor, and manage their AI/ML environments against adversarial threats without interrupting how teams train, test, and deploy their AI models, exited stealth mode when it was spun out of KPMG Studio (KPMG's startup incubator).

Overview

- The platform detects and prevents AI attacks, such as data poisoning, model inversion, model evasion, and backdoor detection or membership interferences.
- Cranium's platform establishes an AI security framework that provides security and data science teams with a foundation for building a proactive and holistic AI security program.
- Platform also captures and quantifies AI security risk and establishes continuous monitoring.
- Cranium brings visibility, trust, and a new level of security to cybersecurity and data science teams when it comes to enterprise-level AI ecosystems.

Sources: Company websites, PitchBook.

Industry-Wide Adoption of Generative AI Tools: Startup Names to Watch (cont.)

ANVILOGIC™

Anvilogic's modern SOC platform enables efficiency by unifying and automating threat detection and incident response and has been successful in incorporating generative AI functionality throughout the platform to create a bridge between legacy security information and event management (SIEM) and next-generation security data lakes.

Anvilogic Capabilities

- Facilitates modern security data lake adoption by lowering the barrier to entry for data engineering skills, allowing SOC teams to adopt a flexible, scalable data lake strategy and eliminating language barriers to rapidly detect threats across disparate data sources.
- Identifies anomalies and potential threats in large-scale data, improving core detection and efficacy due to models being trained with behavioral data and mapped to MITRE ATT&CK.
- Reduces cost and time-to-detect by rebalancing legacy SIEM and data monoliths with a security data lake that enables teams to more efficiently collect, normalize, enrich, and deploy quality detections across modern cloud and hybrid data lake architectures.
- Increases efficiency and scale by leveraging an AI co-pilot that helps teams develop and deploy accurate complex pattern-based detections in minutes across data platforms without requiring extensive software engineering or tool expertise.

HIDDENLAYER

RSAC Innovation Sandbox 2023 WINNER

HiddenLayer has pioneered the development of Machine Learning Detection & Response (MLDR), winning the RSA Conference Innovation Sandbox contest with demonstrations of its comprehensive Machine Learning Security (MLSec) platform.

HiddenLayer Capabilities

HiddenLayer's MLSec platform consists of MLDR capabilities, model scanner technology, and security audit reporting that enable enterprises to harness the advantages of generative AI technology while ensuring the security of valuable ML assets.

- Offers an easy-to-deploy platform that stops adversarial attacks and provides visibility into the health and security of ML assets by monitoring the inputs and outputs of customers' machine-learning algorithms.
- Enables real-time defense, flexible response options, model integrity safeguarding via model scanning, and ongoing security audit reporting to provide a comprehensive view of AI/ML assets security status with flexible response options and on-demand dashboard and distributable reporting.
- Protects against both inference and extraction attacks, data poisoning, model evasion, and model injection.

Sources: Company websites.

V

About Houlihan Lokey

Houlihan Lokey

Leading Independent Global Advisory Firm

Houlihan Lokey is the trusted advisor to more top decision-makers than any other independent global investment bank.

~2,595	36	$6.5 Billion	HLI LISTED NYSE	$1.8 Billion	~25%	No
Global Employees[1]	Locations	Market Cap[2]		Revenue[3]	Employee-Owned	Debt

Corporate Finance

- No. 1 Global M&A Advisor Under $1 Billion
- Over the past two years, we raised approximately $25 billion in capital

2022 M&A Advisory Rankings Global Transactions Under $1 Billion

Rank	Advisor	Deals
1	**Houlihan Lokey**	**381**
2	Rothschild	369
3	JP Morgan	217

Source: Refinitiv.
Excludes accounting firms and brokers.

Financial Restructuring

- No. 1 Global Restructuring Advisor
- $3.0 Trillion of Aggregate Transaction Value Completed

2022 Global Distressed Debt and Bankruptcy Restructuring Rankings

Rank	Advisor	Deals
1	**Houlihan Lokey**	**58**
2	PJT Partners	30
3	Lazard	29

Source: Refinitiv.

Financial and Valuation Advisory

- No. 1 Global M&A Fairness Opinion Advisor Over the Past 25 Years
- 1,000+ Annual Valuation Engagements

1998 to 2022 Global M&A Fairness Advisory Rankings

Rank	Advisor	Deals
1	**Houlihan Lokey**	**1,232**
2	JP Morgan	1,030
3	Duff & Phelps, A Kroll Business	938

Source: Refinitiv.
Announced or completed transactions.

Financial Sponsors Coverage

- No. 1 Global Private Equity M&A Advisor
- 1,000+ Sponsors Covered Globally

2022 Most Active Global Investment Banks to Private Equity

Rank	Advisor	Deals
1	**Houlihan Lokey**	**242**
2	Lincoln International	192
3	Deloitte	190

Source: PitchBook.

Houlihan Lokey + 7 MILE ADVISORS

Houlihan Lokey has agreed to acquire 7 Mile Advisors, an independent advisory firm that provides a range of services to clients across the IT services sector.

The transaction, signed July 7, will further enhance Houlihan Lokey's deep industry expertise in IT services and expands the firm's geographic footprint.

HQ: Charlotte, NC **Employees: ~30** **Managing Directors: 5**

(1) As of June 30, 2023. Excludes corporate MDs.
(2) As of June 2023.
(3) LTM ended March 31, 2023.

Our Tech M&A Team Is No. 1 Globally With Unparalleled Reach

2022 M&A Advisory Rankings
All Global Technology Transactions

Rank	Advisor	Deals
1	**Houlihan Lokey**	**116**
2	Goldman Sachs	106
3	Morgan Stanley	79
4	Rothschild	76
5	JP Morgan	75

Source: Refinitiv.
Excludes accounting firms and brokers.

2022 M&A Advisory Rankings
U.S. Technology Transactions Under $1 Billion

Rank	Advisor	Deals
1	**Houlihan Lokey**	**49**
2	Goldman Sachs	37
3	Morgan Stanley	37
4	Rothschild	33
5	JP Morgan	32

Source: Refinitiv.
Excludes accounting firms and brokers.

No. 1
TECH M&A ADVISOR*

13
LOCATIONS WORLDWIDE

235+
TECHNOLOGY BANKERS

40+
MANAGING DIRECTORS

116
TECHNOLOGY DEALS IN CY22



AMERICAS
Atlanta
Baltimore
Boston
Chicago
Dallas
Houston
Los Angeles
Miami
Minneapolis
New York
San Francisco
São Paulo
Washington, D.C.

EUROPE AND MIDDLE EAST
Amsterdam
Antwerp
Dubai
Frankfurt
London
Madrid
Manchester
Milan
Munich
Paris
Stockholm
Tel Aviv
Zurich

ASIA-PACIFIC
Beijing
Fukuoka
Gurugram
Hong Kong SAR
Mumbai
Nagoya
Shanghai
Singapore
Sydney
Tokyo

Local Technology team

**According to data provided by Refinitiv.*

Deep Cybersecurity Experience Across the Ecosystem

Armorblox has been acquired by Cisco — Sellside Advisor

Transaction Pending: CARLYLE has agreed to acquire a majority stake in NEVERHACK formerly known as PROPHECY a portfolio company of IK Partners — Buyside Advisor

XALIENT accelerate your business has received investment from VOLPI CAPITAL — Sellside Advisor

THRIVE a portfolio company of COURT SQUARE HoldCo PIK Notes Acquisition Financing — Exclusive Placement Agent

ROHDE&SCHWARZ Cybersecurity SAS has been acquired by total specific solutions — Sellside Advisor

proov has received a growth equity investment of $70,000,000 from SEP SUMERU EQUITY PARTNERS — Financial Advisor

SVERICA has made a strategic investment in SHADOWDRAGON — Buyside Advisor

Acumera has received a strategic growth investment from PEAK ROCK CAPITAL® — Sellside Advisor*

tresorit has been acquired by SWISS POST — Sellside Advisor*

CVC has invested in Acronis — Financing Advisor*

Bridewell CONSULTING has received an investment from gcp — Sellside Advisor*

IDIQ has sold a majority stake to CORSAIR CAPITAL — Sellside Advisor*

netwrix has received an equity investment from updata PARTNERS — Financial Advisor

Threema. has entered into a partnership with Afinum — Sellside Advisor*

LIVINGBRIDGE has invested in TitanHQ — Buyside Advisor*

DSwiss has sold a minority stake to Verium — Sellside Advisor*

Acronis structured equity investment led by Goldman Sachs — Financing Advisor*

NC4 has been acquired by everbridge® — Sellside Advisor

MARLIN EQUITY PARTNERS has sold a majority stake in QUALITEST to Bridgepoint — Sellside Advisor*

NTT Security has acquired WhiteHat SECURITY. — Buyside Advisor

Acquisition Financing inside secure has acquired verimatrix — Financing Advisor*

Tintri has sold substantially all its assets, pursuant to Section 363 of the U.S. Bankruptcy Code, to DDN STORAGE — Company Advisor

dealflo has been acquired by OneSpan — Sellside Advisor*

DATA SYNC TECHNOLOGIES has been acquired by CLEAR CREEK GROUP — Sellside Advisor*

BLUECAT has been acquired by MDP® MADISON DEARBORN PARTNERS, LLC — Sellside Advisor

BOMGAR a portfolio company of THOMA BRAVO — Financial Advisor

SURGIENT has been acquired by QUEST SOFTWARE — Sellside Advisor*

TRUST DIGITAL has been acquired by McAfee® — Sellside Advisor*

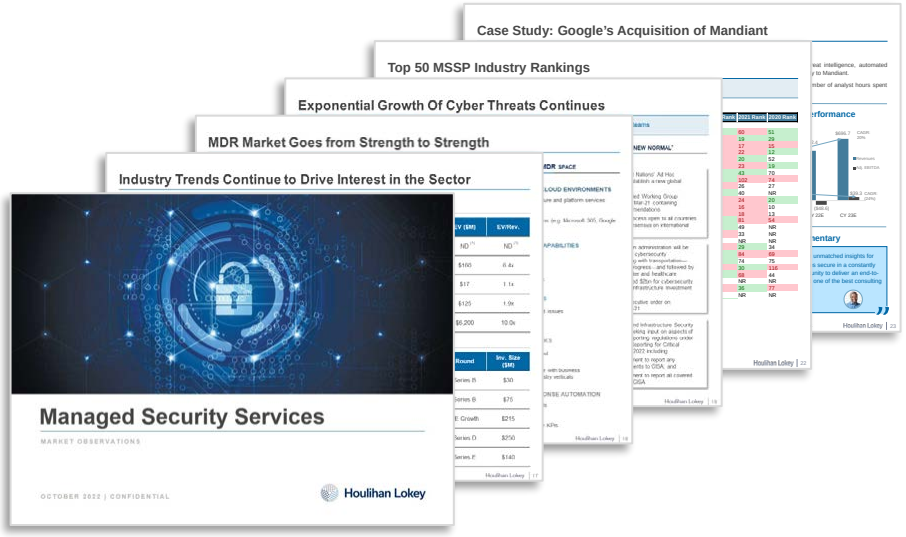
Tombstones included herein represent transactions closed from 2010 forward.
**Selected transactions were executed by Houlihan Lokey professionals while at other firms acquired by Houlihan Lokey or by professionals from a Houlihan Lokey joint venture company.*

Other Houlihan Lokey Cyber Sector Reports

Identity Sector Report



Managed Security Services Report



To gain access to these decks, please reach out to the following:

U.S. Cyber Team



Keith Skirbe
Managing Director
Co-Head of U.S. Cyber
San Francisco
Keith.Skirbe@HL.com



Bobby Wolfe
Director
Co-Head of U.S. Cyber
Miami
BWolfe@HL.com



Tyler Deck
Senior Vice President
Boston
TDeck@HL.com



Rishabh Bansal
Associate
San Francisco
Rishabh.Bansal@HL.com

Global Cyber Reach



Mark Smith
Director
Head of U.K. Cyber
Manchester
Mark.Smith@HL.com



Malte Abrams
Managing Director
Head of DACH Cyber
Frankfurt
Malte.Abrams@HL.com



Ido Zakai
Managing Director
Head of Tech
Tel Aviv
Ido.Zakai@HL.com



Sara Napolitano
Managing Director
Head of France Cyber
Paris
Sara.Napolitano@HL.com

Capital Markets



Sean Fitzgerald
Managing Director
New York
SFitzgerald@HL.com



Chris Hebble
Managing Director
Los Angeles
CHebble@HL.com

Cyber Tech Expertise



Stephen Lee
Managing Director
Tech and Cyber Due Diligence
Chicago
SJLee@HL.com



Edouard Viot
Cybersecurity Consultant
Paris

Yearly Conferences

black hat

infosecurity EUROPE

RSA Conference 2023

Disclaimer

© 2023 Houlihan Lokey. All rights reserved. This material may not be reproduced in any format by any means or redistributed without the prior written consent of Houlihan Lokey.

Houlihan Lokey is a trade name for Houlihan Lokey, Inc., and its subsidiaries and affiliates, which include the following licensed (or, in the case of Singapore, exempt) entities: in (i) the United States: Houlihan Lokey Capital, Inc., and Houlihan Lokey Advisors, LLC, each an SEC-registered broker-dealer and member of FINRA (www.finra.org) and SIPC (www.sipc.org) (investment banking services); (ii) Europe: Houlihan Lokey Advisory Limited, Houlihan Lokey EMEA, LLP, Houlihan Lokey (Corporate Finance) Limited, and Houlihan Lokey UK Limited, authorized and regulated by the U.K. Financial Conduct Authority; Houlihan Lokey (Europe) GmbH, authorized and regulated by the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht); (iii) the United Arab Emirates, Dubai International Financial Centre (Dubai): Houlihan Lokey (MEA Financial Advisory) Limited, regulated by the Dubai Financial Services Authority for the provision of advising on financial products, arranging deals in investments, and arranging credit and advising on credit to professional clients only; (iv) Singapore: Houlihan Lokey (Singapore) Private Limited and Houlihan Lokey Advisers Singapore Private Limited, each an "exempt corporate finance adviser" able to provide exempt corporate finance advisory services to accredited investors only; (v) Hong Kong SAR: Houlihan Lokey (China) Limited, licensed in Hong Kong by the Securities and Futures Commission to conduct Type 1, 4, and 6 regulated activities to professional investors only; (vi) India: Houlihan Lokey Advisory (India) Private Limited, registered as an investment adviser with the Securities and Exchange Board of India (registration number INA000001217); and (vii) Australia: Houlihan Lokey (Australia) Pty Limited (ABN 74 601 825 227), a company incorporated in Australia and licensed by the Australian Securities and Investments Commission (AFSL number 474953) in respect of financial services provided to wholesale clients only. In the United Kingdom, European Economic Area (EEA), Dubai, Singapore, Hong Kong, India, and Australia, this communication is directed to intended recipients, including actual or potential professional clients (UK, EEA, and Dubai), accredited investors (Singapore), professional investors (Hong Kong), and wholesale clients (Australia), respectively. Other persons, such as retail clients, are NOT the intended recipients of our communications or services and should not act upon this communication.

Houlihan Lokey gathers its data from sources it considers reliable; however, it does not guarantee the accuracy or completeness of the information provided within this presentation. The material presented reflects information known to the authors at the time this presentation was written, and this information is subject to change. Any forward-looking information and statements contained herein are subject to various risks and uncertainties, many of which are difficult to predict, that could cause actual results and developments to differ materially from those expressed in, or implied or projected by, the forward-looking information and statements. In addition, past performance should not be taken as an indication or guarantee of future performance, and information contained herein may be subject to variation as a result of currency fluctuations. Houlihan Lokey makes no representations or warranties, expressed or implied, regarding the accuracy of this material. The views expressed in this material accurately reflect the personal views of the authors regarding the subject securities and issuers and do not necessarily coincide with those of Houlihan Lokey. Officers, directors, and partners in the Houlihan Lokey group of companies may have positions in the securities of the companies discussed. This presentation does not constitute advice or a recommendation, offer, or solicitation with respect to the securities of any company discussed herein, is not intended to provide information upon which to base an investment decision, and should not be construed as such. Houlihan Lokey or its affiliates may from time to time provide investment banking or related services to these companies. Like all Houlihan Lokey employees, the authors of this presentation receive compensation that is affected by overall firm profitability.

Houlihan Lokey



CORPORATE FINANCE

FINANCIAL RESTRUCTURING

FINANCIAL AND VALUATION ADVISORY

HL.com