



# Generative AI Adoption in Cybersecurity

June 2024

# Contents

- 03 Overview and value chain
- 04 Key business problems and challenges
- 05 Impact of gen AI
- 06 Maturity and scale of gen AI adoption
- 07 Segment wise adoption based on the study

For more information on this and other research published by Everest Group, please contact us:

**Vaibhav Bansal**, Vice President

**Kumar Avijit**, Practice Director

**Anish Nath**, Practice Director

**Divya Chandak**, Senior Analyst

**Arjun Chauhan**, Senior Analyst

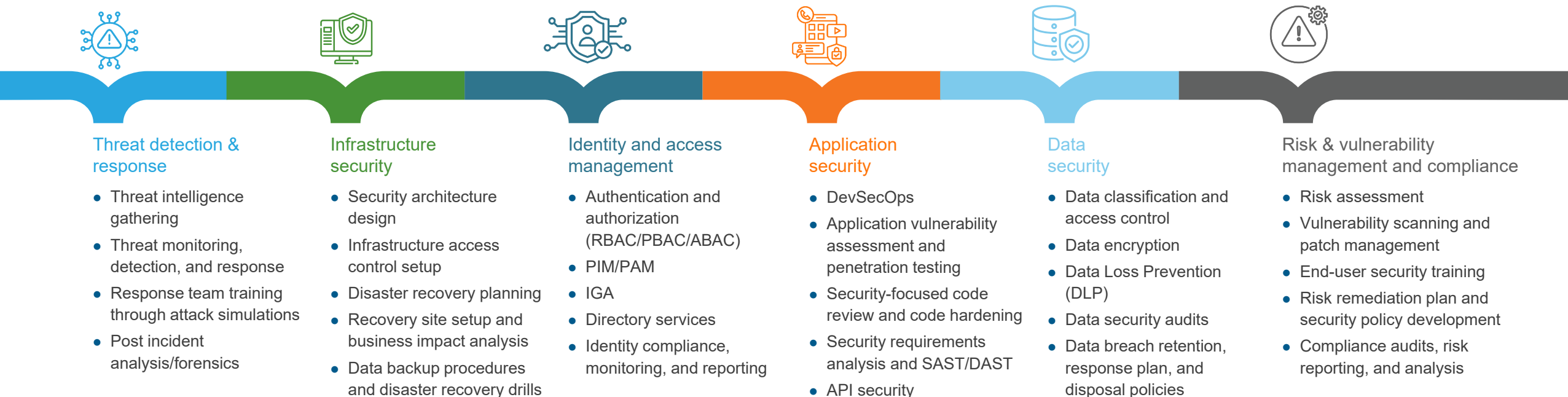
**Copyright © 2024 Everest Global, Inc.**

We encourage you to share these materials internally in accordance with your license. Sharing these materials outside your organization in any form – electronic, written, or verbal – is prohibited unless you obtain the express, prior, and written consent of Everest Global, Inc. It is your organization's responsibility to maintain the confidentiality of these materials in accordance with your license of them.







# Overview and cybersecurity value chain

## Overview

The foundational objective of cybersecurity is to protect enterprises' data, systems, and networks from unauthorized access and cyber threats. While the initial goal was to prevent breaches and ensure compliance, as threats have grown more sophisticated, cybersecurity has evolved to include continuous monitoring, risk management, and proactive defense strategies to safeguard sensitive information and maintain trust with customers and partners.



# Key business problems and challenges in cybersecurity

	 <b>Threat detection &amp; response</b>	 <b>Infrastructure security</b>	 <b>Identity and access management</b>	 <b>Application security</b>	 <b>Data security</b>	 <b>Risk &amp; vulnerability management and compliance</b>
Key objectives	Identify and respond to cyber threats to minimize damage	Secure the IT infrastructure to ensure business continuity and protect critical assets	Ensure secure and efficient access to systems and data	Protect applications from vulnerabilities and threats	Safeguard sensitive data from breaches and unauthorized access	Identify, assess, and mitigate risks to ensure compliance and security
Key business problems and challenges	<ul style="list-style-type: none"> <li>• Difficulty in real-time threat detection and analysis</li> <li>• Lack of skilled cybersecurity professionals</li> <li>• Delays in incident response and containment</li> </ul>	<ul style="list-style-type: none"> <li>• Dealing with complex infrastructure environments</li> <li>• Ensuring consistent security policy enforcement</li> <li>• Managing and mitigating infrastructure vulnerabilities</li> </ul>	<ul style="list-style-type: none"> <li>• Managing identities and access for diverse user groups</li> <li>• Ensuring compliance with access control policies</li> <li>• Protecting against identity theft and unauthorized access</li> </ul>	<ul style="list-style-type: none"> <li>• Identifying and mitigating application vulnerabilities</li> <li>• Integrating security into the software development lifecycle</li> <li>• Ensuring consistent application security standards</li> </ul>	<ul style="list-style-type: none"> <li>• Ensuring comprehensive data encryption and protection</li> <li>• Managing data privacy regulations and compliance</li> <li>• Protecting against data loss and breaches</li> </ul>	<ul style="list-style-type: none"> <li>• Conducting thorough risk assessments</li> <li>• Keeping up with evolving regulatory requirements</li> <li>• Managing and patching vulnerabilities effectively</li> </ul>
Key results	<ul style="list-style-type: none"> <li>• Lower time to detect and respond to threats</li> <li>• Improved incident resolution rates</li> <li>• Enhanced threat intelligence and awareness</li> </ul>	<ul style="list-style-type: none"> <li>• Increased infrastructure resilience</li> <li>• Enhanced disaster recovery capabilities</li> <li>• Lower risk of infrastructure-related breaches</li> </ul>	<ul style="list-style-type: none"> <li>• Streamlined access management processes</li> <li>• Lower risk of unauthorized access</li> <li>• Increased compliance with IAM-specific regulations</li> </ul>	<ul style="list-style-type: none"> <li>• Fewer application vulnerabilities</li> <li>• Improved security in the development process</li> <li>• Enhanced protection for sensitive application data</li> </ul>	<ul style="list-style-type: none"> <li>• Improved data protection measures</li> <li>• Increased compliance with data security regulations</li> <li>• Fewer data breaches</li> </ul>	<ul style="list-style-type: none"> <li>• Enhanced risk management processes</li> <li>• Increased regulatory compliance</li> <li>• Fewer vulnerabilities and associated risks</li> </ul>

# Gen AI's impact in solving business problems in cybersecurity | gen AI use cases



Threat detection & response

- Summarize threat intelligence and provide recommendations for SoC analysts
- Automate threat detection and identify emerging threats in large datasets
- Ensure robust threat monitoring by identifying patterns, trends, and suspicious behaviors



Infrastructure security

- Assess and predict the impact of security incidents on business operations
- Optimize security architectures, identifying gaps and recommending enhancements



Identity and access management

- Automate identity governance, ensuring compliance and efficient administration of user identities
- Enhance directory services, improving access control and authentication processes



Application security

- Conduct comprehensive code reviews, identifying vulnerabilities and suggesting security enhancements
- Assess applications for vulnerabilities, providing detailed insights and proactive mitigation strategies



Data security

- Dynamically manage and enforce data access controls, adapting to evolving security policies
- Classify data by context and content, enhancing data protection and compliance efforts



Risk & vulnerability management and compliance

- Create personalized security training programs, tailoring content to user behaviors and roles
- Automate policy enforcement and ensure continuous compliance with regulatory standards

Expected impact of gen AI



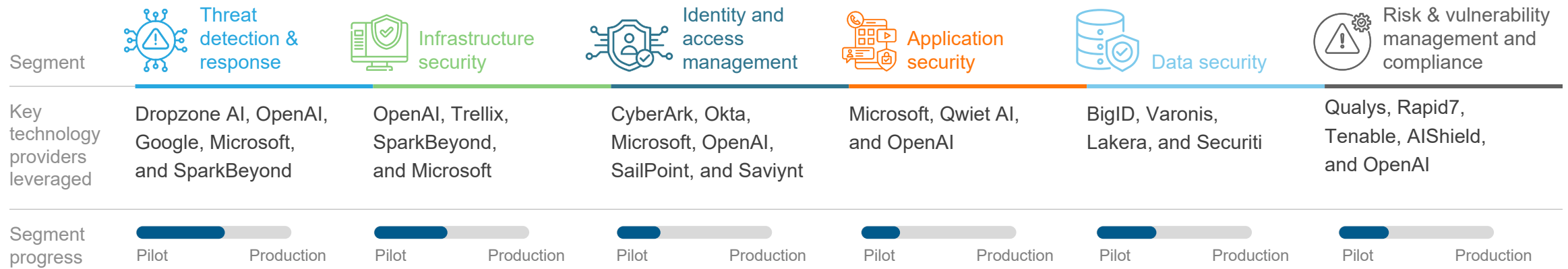
# Everest Group conducted an assessment of the market maturity of gen AI adoption across key cybersecurity services providers

● Generative AI Adoption in cybersecurity services



<sup>1</sup> The participating providers are arranged in alphabetical order

# Segment wise adoption in cybersecurity based on the study



# Stay connected

Dallas (Headquarters)

info@everestgrp.com

+1-214-451-3000

Bangalore

india@everestgrp.com

+91-80-61463500

Delhi

india@everestgrp.com

+91-124-496-1000

London

unitedkingdom@everestgrp.com

+44-207-129-1318

Toronto

canada@everestgrp.com

+1-214-451-3000

Website

everestgrp.com

Blog

everestgrp.com/blog

Follow us on



Everest Group is a leading research firm helping business leaders make confident decisions. We guide clients through today's market challenges and strengthen their strategies by applying contextualized problem-solving to their unique situations. This drives maximized operational and financial performance and transformative experiences. Our deep expertise and tenacious research focused on technology, business processes, and engineering through the lenses of talent, sustainability, and sourcing delivers precise and action-oriented guidance. Find further details and in-depth content at [www.everestgrp.com](http://www.everestgrp.com).

## Notice and disclaimers

**Important information. Please review this notice carefully and in its entirety. Through your access, you agree to Everest Group's terms of use.**

Everest Group's Terms of Use, available at [www.everestgrp.com/terms-of-use/](http://www.everestgrp.com/terms-of-use/), is hereby incorporated by reference as if fully reproduced herein. Parts of these terms are pasted below for convenience; please refer to the link above for the full version of the Terms of Use.

Everest Group is not registered as an investment adviser or research analyst with the U.S. Securities and Exchange Commission, the Financial Industry Regulatory Authority (FINRA), or any state or foreign securities regulatory authority. For the avoidance of doubt, Everest Group is not providing any advice concerning securities as defined by the law or any regulatory entity or an analysis of equity securities as defined by the law or any regulatory entity.

All Everest Group Products and/or Services are for informational purposes only and are provided "as is" without any warranty of any kind. You understand and expressly agree that you assume the entire risk as to your use and any reliance upon any Product or Service. Everest Group is not a legal, tax, financial, or investment advisor, and nothing provided by Everest Group is legal, tax, financial, or investment advice. Nothing Everest Group provides is an offer to sell or a solicitation of an offer to purchase any securities or instruments from any entity. Nothing from Everest Group may be used or relied upon in evaluating the merits of any investment. Do not base any investment decisions, in whole or part, on anything provided by Everest Group.

Products and/or Services represent research opinions or viewpoints, not representations or statements of fact. Accessing, using, or receiving a grant of access to an Everest Group Product and/or Service does not constitute any recommendation by Everest Group that recipient (1) take any action or refrain from taking any action or (2) enter into a particular transaction. Nothing from Everest Group will be relied upon or interpreted as a promise or representation as to past, present, or future performance of a business or a market. The information contained in any Everest Group Product and/or Service is as of the date prepared, and Everest Group has no duty or obligation to update or revise the information or documentation. Everest Group may have obtained information that appears in its Products and/or Services from the parties mentioned therein, public sources, or third-party sources, including information related to financials, estimates, and/or forecasts. Everest Group has not audited such information and assumes no responsibility for independently verifying such information as Everest Group has relied on such information being complete and accurate in all respects. Note, companies mentioned in Products and/or Services may be customers of Everest Group or have interacted with Everest Group in some other way, including, without limitation, participating in Everest Group research activities.