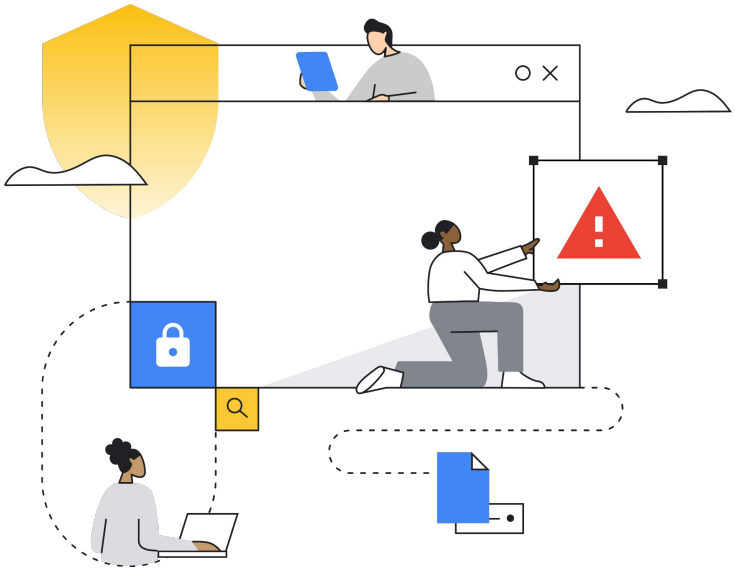
Google Cloud

10 questions CEOs should ask about cloud security



Solution Value Advisory Team, Google
Monisha Deshpande, Global Director
Joyeeta Banerjee, Head of Security & Data Analytics
Usman Chaudhary, Security Solution Value Advisor
Touraj Tehrani, Senior Principal, Security & Data Analytics

10 questions CEOs should ask about cloud security

01 Why is cybersecurity a priority for CEOs and their boards of directors?

02 What's changing in security?

03 Why do CEOs consider cyber threats a top risk to growth?

04 How do I make security a business differentiator vs. a cost center?

05 Why are security challenges so hard for organizations to address?

06 With the recent investments in cloud, is the cloud more secure?

07 What business value can I expect from a modernized security program?

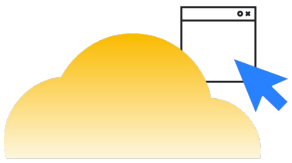
08 How is Google proactively investing in security?

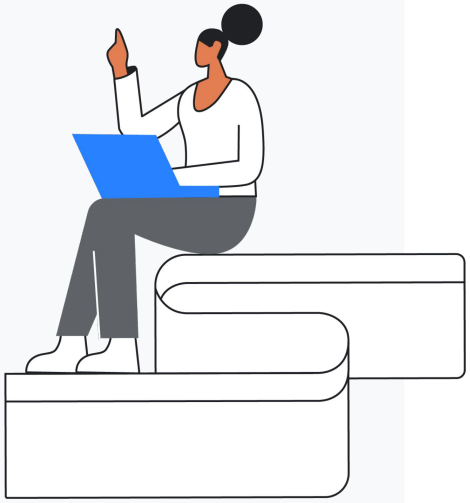
09 How is my company positioned against security threats?

10 How do I get started?

Section 1

Introduction





"Trust no one" is the mantra of the year according to technology executives recently surveyed.[1] This is warranted given the increasingly complex geopolitical environment, the shift to hybrid and workers logging in from remote locations, the investment in modernizing technology platforms, and the migration to cloud infrastructure and platform services.

The main priority for companies' IT security departments over the next two years is to improve information protection and data classification.[2] For additional context, the average data breach cost increased from $4.24 million in 2021 to $4.35 million in 2022, representing a 12.7% increase from the 2020 average cost of $3.86 million.[3] Therefore it is no surprise that cybersecurity is a priority. Drawing from our own experience, Google Cloud blocked the largest Layer 7 DDoS attack at 46 million rps in 2022 – a large scale attack that was like receiving all the daily requests to Wikipedia (one of the top 10 trafficked websites in the world) in just 10 seconds.

All of these reasons reinforce the need for a strong enterprise security posture, and **CEOs and Boards are increasingly prioritizing security investments to protect revenue, preserve brand equity, and keep operations secure and resilient.** This eBook uncovers the critical questions that the C-Suite and Boards are asking as they make these decisions across the enterprise.

[1] The Wall Street Journal, "CIO 2023 Priorities: Cybersecurity," December 2022
[2] Statista, "What are the top priorities for your organization's IT security department over the next two years?" January 2023
[3] IBM, "Cost of a data breach 2022," January 2023

Section 2

What's changing in security?

The cyber threat landscape continues to evolve, and it is not just sophisticated adversaries who are getting better. In the old world, high-damage attacks were limited to elite organizations such as nation states with a significant amount of resources. They targeted governments and critical infrastructure to advance their cyber espionage agenda.

But in today's new world, it is easier for "commercial" actors to develop cyber attack skills at a lower resource cost and to use them regularly. This means that their targets have now broadened to include enterprises and companies of all sizes. Moreover, these attacks are now driven by financial gain which is evident from Google's observation of crypto mining in infected cloud instances.

The top malware used for short-term infections will be cryptominers in 2023, but other forms of monetization, such as phishing or ransoming customer environments, could grow as well.[4]

Other examples include the ransomware attacks against Colonial Pipeline and the supply chain attacks against SolarWinds. Organizations are under tremendous pressure today to secure themselves against these threats. At the current rate of growth, damage from cyberattacks will amount to about $10.5 trillion annually by 2025 – a 300 percent increase from 2015 levels.[5]

Old world

- Limited number of highly advanced attackers
- Nation-state level resources required
- Targeting governments and critical infrastructure
- Cyber-espionage focus

New world

- Numerous well-funded "commercial" threat actors
- Broad knowledge of advanged TTPs (Tactics, Techniques, and Procedures), exploits, tooling
- Targeting enterprises of all sizes and sectors
- Financial gain, business disruption focus

Google Cloud

[4] Google Cloud, "Threat Horizons Report," January 2023
[5] McKinsey & Company, "New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers," October 2022.

Section 3

Why do CEOs consider cyber threats a top risk to growth?

Security breaches have significant lasting impacts on key business levers, making them a top threat to growth as identified by CEOs.[6] Boards are also shifting their focus to cybersecurity in light of new developments such as the proposed rule issued by the U.S. Securities and Exchange Commission.[7] This rule will require companies to disclose their cybersecurity governance capabilities, the frequency of discussion on the topic, and how they consider this integral to their business strategy, risk management, and financial oversight.

Risk, resiliency, and reputation are the three top areas where cybersecurity ultimately impacts the top and bottom line of an enterprise:

Risk

Tying the technical nuances of an extremely complex topic to the financial risk of the enterprise is increasingly important for CEOs and Boards to understand. A CEO / Board agenda on this topic should include: understanding the main security threats, the impact of cloud adoption, the implications of hybrid work, employee awareness, and compliance with regulatory frameworks are all critical components.

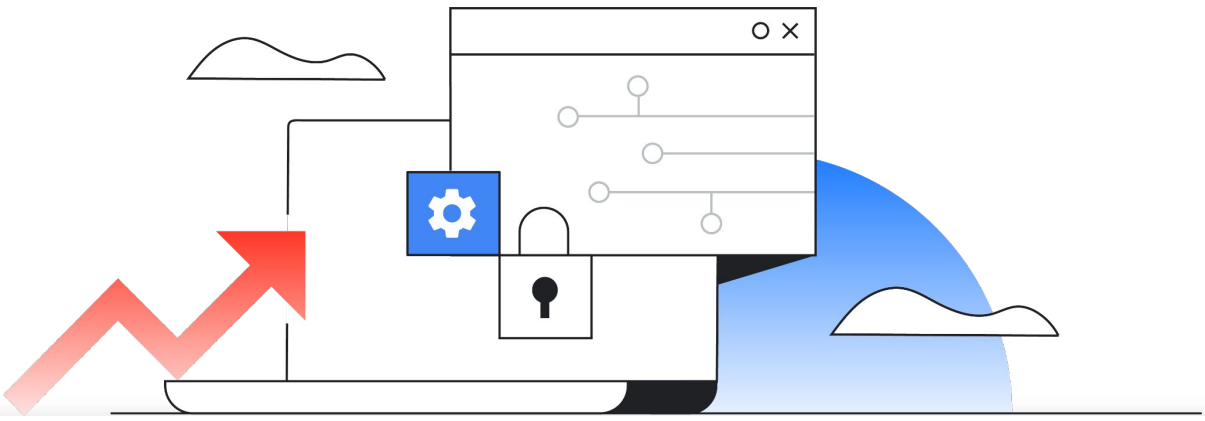
Resiliency

The ability of an organization to mitigate these risks, recover from a cyber attack, and ensure business continuity are all critical characteristics of a resilient organization. Investing in a recovery plan is as important as investing in a protection plan against cybersecurity threats.

Reputation

An organization's brand reputation is at risk when it is under a cybersecurity attack. Surveys conducted by leading security experts and Google Cloud indicate that most companies experience an impact on brand and reputation that leads to loss of customers and partners, erosion of trust, and difficulty attracting new customers.[8] This is even more relevant today with rise of consumer data – organizations need to protect a growing amount of consumer data in order to remain a brand that consumers trust.

[6] KPMG, 2021 CEO Outlook
[7] U.S. Securities and Exchange Commission, "SEC Proposes Rules to Enhance and Standardize Climate-Related Disclosures for Investors," March 2022
[8] Deloitte, "2021 future of cyber survey"



Security is a top risk that CEOs indicate as a threat to growth

Business levers impacted by cyber threats as indicated by 600 Global C-Suite responders

32%

Operational disruption

22%

Intellectual property theft

17%

Regulatory fines, loss of reputation and customer trust / negative brand

Google Cloud

Sources:
KPMG, "2021 CEO Outlook"
Deloitte, "2021 future of cyber survey"

Section 4

How do I make security a business differentiator vs. a cost center?

High-performing organizations that align their business strategy with their security requirements witness much higher business value. This is in part due to better use of security dollars on proactive capabilities rather than reactive ones. In addition, security becomes a selling factor and business differentiator rather than a cost center; this can only be achieved when security is considered an integral part of all business planning. Organizations usually fall into the below categories of security maturity:

Initial

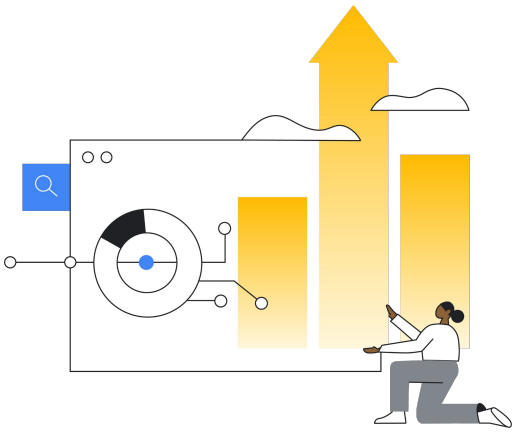
Organizations in this level often have limited security capabilities in place and are lacking in several aspects of the security lifecycle. Their security approach is ad-hoc and still in the planning phases, with less focus on transformation. They are still developing their foundational security processes and investigating security solutions.

Tactical

Organizations in this level often have foundational security capabilities in place, but a limited cloud security strategy and limited architectural framework for all aspects of the security lifecycle. Their security approach is reactive and focused on point security products and platform services without clear alignment to overarching IT transformation priorities. This short-term focus may lead to redundant products and services, with limited provision for scale.

Strategic

Organizations in this level have robust security architecture and engineering capabilities that govern individual security and resilience domains. Security is designed to proactively implement capabilities to mitigate the evolving threat landscape. The organization has embraced security transformation across the people, process, and technology layers. Their security teams are proactive, harnessing native cloud security capabilities for business operations.

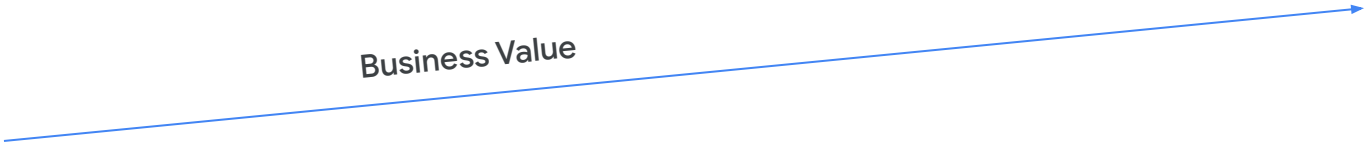


Transformational

Organizations in this level have cloud security operations functioning autonomously, and they have turned their attention to harness data and insights from their security investments. Security is consistently collected and analyzed across all information assets.

These organizations also apply predictive and prescriptive analytics of machine learning. People and processes are being transformed, which further supports technological changes. Security becomes a competitive advantage and strategic partner to the business.

Business strategy & security requirements need to be aligned for long term success



Initial

Limited controls in place, security approach is ad hoc and still in planning phases.

Tactical

Foundational security capabilities in place, but with limited cloud security strategy. Reactive and focused on point security products.

Strategic

Robust security strategy, with an eye to the evolving threat landscape and need to scale.

The organization has started to embrace security transformation.

Transformational

Functioning autonomously, applying predictive and prescriptive analytics of machine learning.

Security becomes a competitive advantage and strategic partner to the business.

Increasing alignment between business strategy and security requirements

Section 5

Why are security challenges so hard for organizations to address?

As a company aligns its business strategies to a multi-year roadmap, several challenges can prevent the successful execution of security initiatives. Broadly, we see these challenges across several areas that include: supply chain risks, data availability and protection, web threats, compliance and regulatory risks, intellectual property and business process theft, and overall operational complexity.

Google Cloud's experience working with customers indicates three opportunity areas for the adoption of broad security strategies. These are:

Strategy

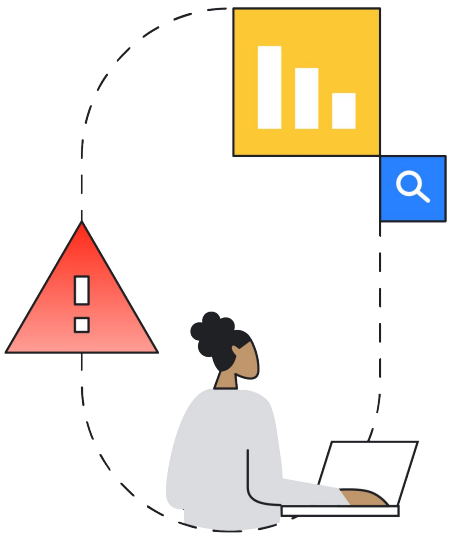
Most organizations do not have a security embedded in their strategy and business development processes.

Technology

Organizations follow a point-product approach that leads to operational complexity and redundancy, or proliferation of tools without a rationalization across the portfolio.

People

There is not just a lack of awareness of security threats and risk across the enterprise; there is also a severe shortage of security expertise and skills which is further compounded by low automation.



All of these lead to an expanded attack surface and increase the vulnerability of an organization to be exposed to a cybersecurity attack.

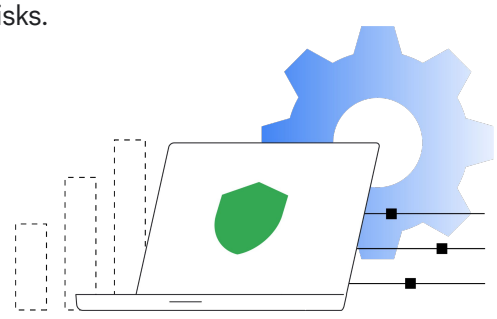
Section 6

With the recent investments in cloud, is the cloud more secure?

As enterprises make significant technology investments to modernize their infrastructure to the cloud, Google Cloud security experts believe that a well-configured cloud environment, or on-premise cloud-like modernized IT environment, can be more secure than typical on-premise environments, especially legacy on-premise.[9] Adopting cloud technologies and adjusting business practices and processes can allow organizations the opportunity to step change their management of operational risk.

For example, cybersecurity risks can be addressed and mitigated using cloud in ways that are not viable with traditional on-premise technologies. Cloud providers typically have global scale infrastructure designed to provide security throughout the entire information processing lifecycle – and this scale drives down the unit cost of that security.[10] These capabilities include: pervasive and sometimes by-default encryption of data, internet-scale capacity to deflect denial of service attacks, feature-rich data loss prevention technologies, etc.

With these growing investments in the cloud, CISOs and CIOs are working closely together to ensure that there is a tight feedback loop across IT, Product, Operations, and other cross-functional teams to ensure continued operations and deliver on business outcomes without compromising security risks.



[9] Google Cloud, "What is Cloud Security?"

Section 7

What business value can I expect from a modernized security program?

Boards are requiring CEOs, CIOs, and CISOs to justify their spending based on quantifiable levers. It is increasingly important to understand the value that security investments create to optimize decisions, gain internal approvals, and validate the realized value post-implementation. We believe every organization should evaluate the business value of investing in security solutions across these three broad dimensions:

Reduced risk

An elevated security posture means reduced risk: fewer breaches, less costly business disruption, reduced loss of intellectual property, reduced loss of reputation, and the avoidance of legal fees and lawsuits as examples.

Risk quantification is becoming a critical lever for C-level executives as they balance the security investments for risk mitigation vs. cyber risk insurance, where this risk quantification can help with negotiations.

Enhanced productivity

There is a severe shortage of cybersecurity professionals, so a modernized security program helps organizations do more with fewer resources—such as reduced FTE headcount and less time needed to plan and implement—as well as enhance their security automation.

Optimized financials

A modernized security program can result in lower total cost of ownership (TCO), increased revenue for the business (improved software development life cycle times), and reduced costs associated with audits. And, it helps organizations gain a deeper understanding of their security capabilities for the associated costs.

Expected business value from a modernized security program

Reduced risk

- Reduced cost of data breach and disruption
- Reduced cost of response
- Reduced incident response cost

Optimized financials

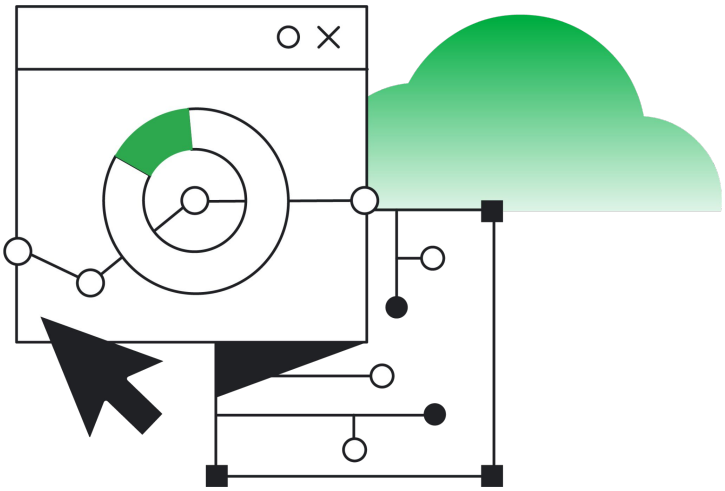
- Consolidated cloud point product vendors
- Reduced external audit costs
- Improved app release frequency

Enhanced productivity

- FTEs repurposed through vendor consolidation efficiency
- Reduced security planning and implementation time
- Reduced information security cost
- Improved software development life cycle agility

Section 8

How is Google proactively investing in security?



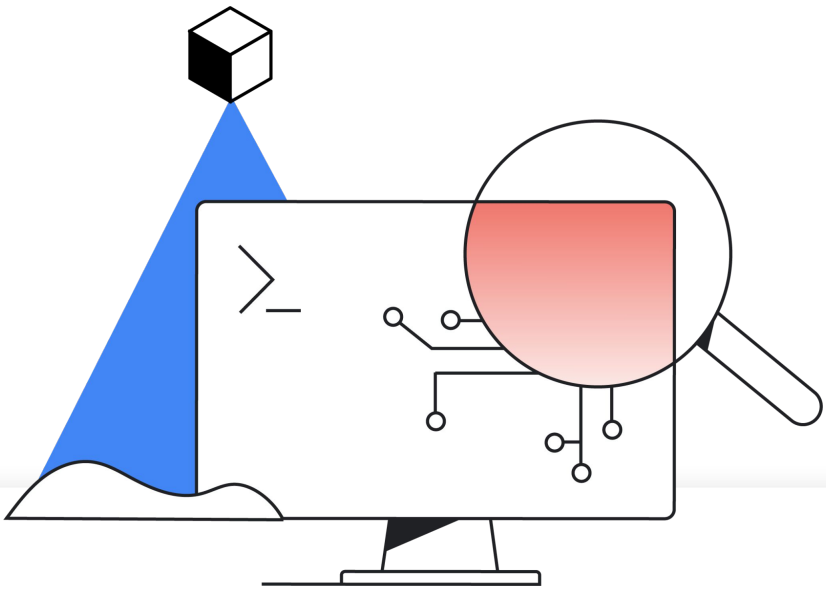
Google has invested significantly in cybersecurity and has committed to investing $10 billion to help strengthen it, including expanding zero trust programs, helping secure the software supply chain, and enhancing open source security.[10]

Additionally, Google is an active contributor to thought capital, with over 150 academic papers and active Open SSF contributions. Google is also training 100,000 professionals in cyber skills to continue investing in future talent.

Google is continuing to build security capabilities through its acquisition of Mandiant, which will help organizations improve their threat, incident, and exposure management.[11] Google has also invested in our security portfolio to protect enterprises with a focus on being secure by default, trusting nothing, and detecting threats across multiple vectors. Lastly, Google has taken the lead in reinventing data center security with the development of the Titan custom chip.

[10] Google, "Why we're committing $10 billion to advance cybersecurity," August 2021

[11] Google Cloud, "Google + Mendiant: Transforming Security Operations and Incident Response," September 2022



Section 9

How is my company positioned against security threats?

To understand where companies need to shift or increase their security investments, it is critical to get a baseline of a company's security maturity. There are several assessment frameworks that can help companies understand their security baseline.

For example, Google Cloud has developed a security and resilience framework that allows our customers to gain an understanding of their existing security posture. Our security and resilience solutions address each phase of the NIST Cybersecurity Framework.

We help our customers to assess risk, protect their businesses from threats, maintain continuous operations, and enable rapid recovery in the event of a crisis (e.g. a ransomware incident).

Section 10

How do I get started?

We would love to work alongside you to uncover your pain points, identify solutions for your security challenges, and provide recommendations for your organization's security and resilience. Our security solutions value advisory team uses the Google Cloud Security & Resilience framework to cover all components of the security lifecycle (Identify, Protect, Detect, Respond, and Recover).

Contact us to find out more.