Deloitte.

Google Cloud Security

Cyber Surakshit Bharat:
Protecting the digital frontier for Viksit Bharat

September 2024

Table of contents

Foreword

India, on its inexorable march towards becoming a Viksit Bharat, is well poised to benefit from the government's focus on infrastructure development and digital transformation as the twin engines of progress. This focus aims to drive India to the third-largest economy by 2027. As these twin engine drive growth, an entire-nation approach must be taken to deal with cyber insecurities and/or threats. This approach might impede the rapid pace at which digital transformation will be embraced by the sectors, states, agencies and departments, including citizens.

The high frequency and intensity of cyberattacks, coupled with an expanding attack surface and cross-border networks of threat actors, make it necessary for the government to consolidate knowledge, resources and capabilities. This response will help combat cybercrime. To enable a robust and self-reliant Viksit Bharat, building a Cyber Surakshit Bharat proves to be a fundamental step towards it.

This whitepaper outlines our commitment to creating a cybersecure ecosystem. It explores critical aspects of safeguarding our digital infrastructure, nurturing a cyber-aware citizenry and fostering a robust digital ecosystem. By synergising our efforts, we can create a vibrant and cyber-safe digital India.

Let us embark on this journey towards a Cyber Surakshit Bharat, an integral part of our vision for a Viksit Bharat.

साइबर सुरक्षित भारत, विकसित भारत की नींव है।

Gaurav Shukla
Partner,
Deloitte India

Sandeep Patil
Partnerships Leader,
Google Cloud Security
Asia Pacific & Japan

Cyber Surakshit Bharat: The foundation for a Viksit Bharat (New India)

The government plays a crucial role in achieving a Viksit Bharat through various policy interventions and initiatives. Digital India stands out as a major one. As digital transformation accelerates, so do the cyber threats targeting government entities. A robust and adaptive cyber defence strategy is imperative to safeguard sensitive data, critical systems and national security.

This whitepaper explores the transformative potential of a new-age cyber defence platform, powered by Artificial Intelligence (AI), global threat intelligence and generative AI to bolster the capabilities of a national cyber defence centre specifically for the government and public sector.

Unique cybersecurity challenges

The nation and public sector face a unique set of cyber threats due to the sensitive nature of their data, the complexity of their technology infrastructure and the constant public scrutiny. These challenges include the following:

Extensive and evolving attack surface: Government agencies manage a vast array of systems, networks and applications, increasing the potential attack surface.

Data sensitivity: Government data, such as citizen records, classified information and national security secrets, is a prime target for cybercriminals and nation-state actors.

Regulatory compliance: Government agencies must adhere to strict compliance standards, such as GDPR, DPDPA, NIST CSF, ISO 27001, PCI DSS, IT Act 2000 Cert-In, etc., adding complexity to cyber defence efforts.

Public trust: Cyberattacks on government agencies can erode public trust in government services and institutions.

> **30%**
> surge observed in global cyberattacks in Q2 2024, with India hit hard.[1]

- Indian organisations faced an average of 3,201 attacks per week, the second highest in the Asia Pacific region.
- Government and military institutions followed, facing 2,084 attacks per week.

> It is easier and cheaper to launch a cyberattack than to defend it.

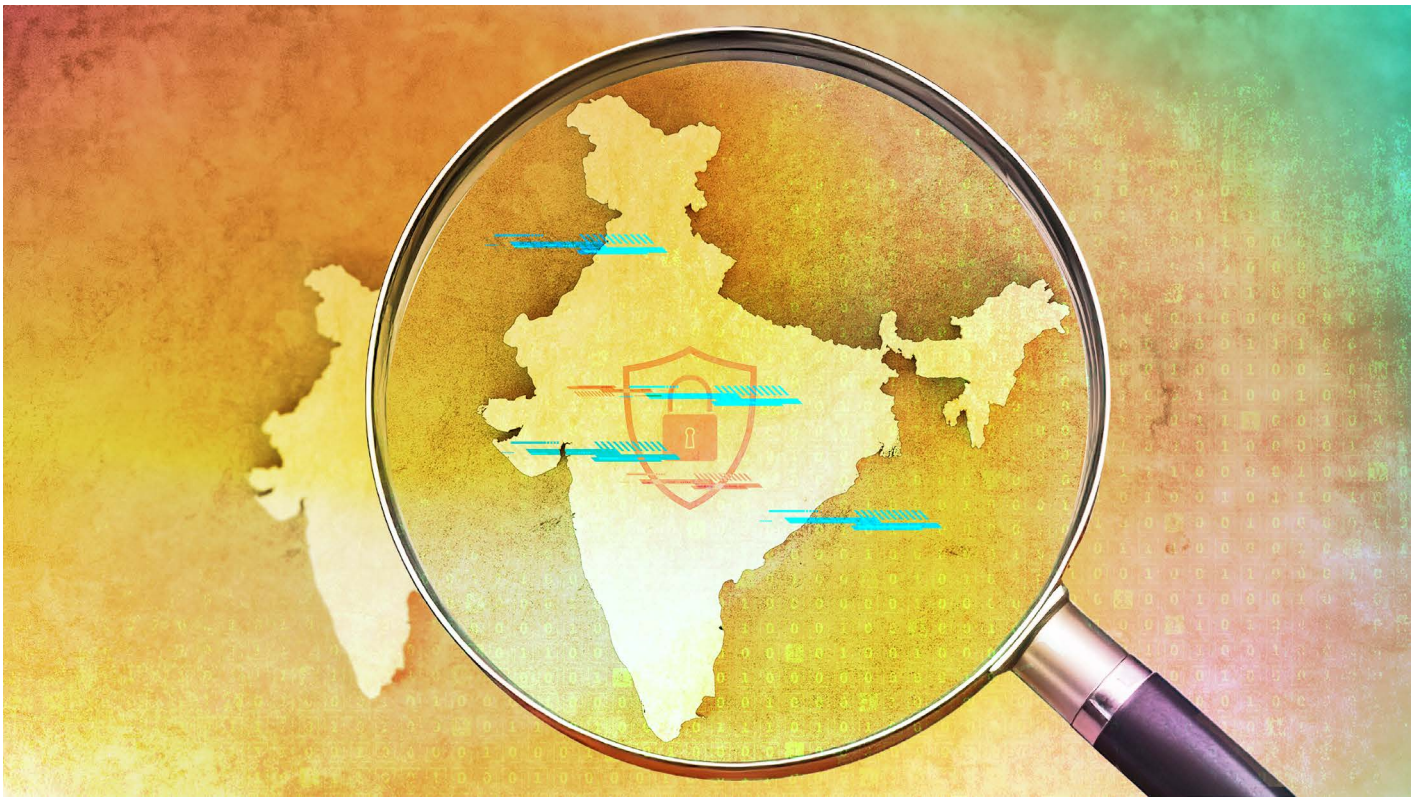
[1] Industry Targeting - Source: Times of India

The cyber threat landscape is characterised by increasing complexity, sophistication and velocity. Cyber adversaries are employing advanced techniques, such as AI, automation and human-operated ransomware groups, to launch highly targeted and persistent attacks. These threats pose significant challenges to traditional cyber defence approaches, necessitating a more proactive and intelligent defence strategy.

Vision for governments and public sectors

- Cultivate a collaborative culture of enhanced cybersecurity and threat awareness with **cyber governance at scale.**
- Reduce the effect and severity of cyber attacks on Critical National Infrastructure to **secure the nation.**
- Accelerate innovation and drive repeatable outcomes through a **secure and reliable Cloud.**
- Empower the government entities with advanced skills and capabilities to **defend against tomorrow's attacks today.**

> A central, secure and intelligent platform to provide nationwide cyber defence and protect what is critical to the nation



New-age cyber defence platform capabilities

A new-age cyber defence platform, powered by AI, global threat intelligence and generative AI, should incorporate the following core capabilities:

Data localisation and privacy:
Data localisation and privacy are essential to ensure that sensitive data is stored and processed in accordance with local regulations.

Predictive analytics and threat hunting:
By combining AI with global threat intelligence, the platform can predict potential attacks and proactively hunt for adversaries within the network. This proactive approach can significantly reduce the risk of successful cyberattacks.

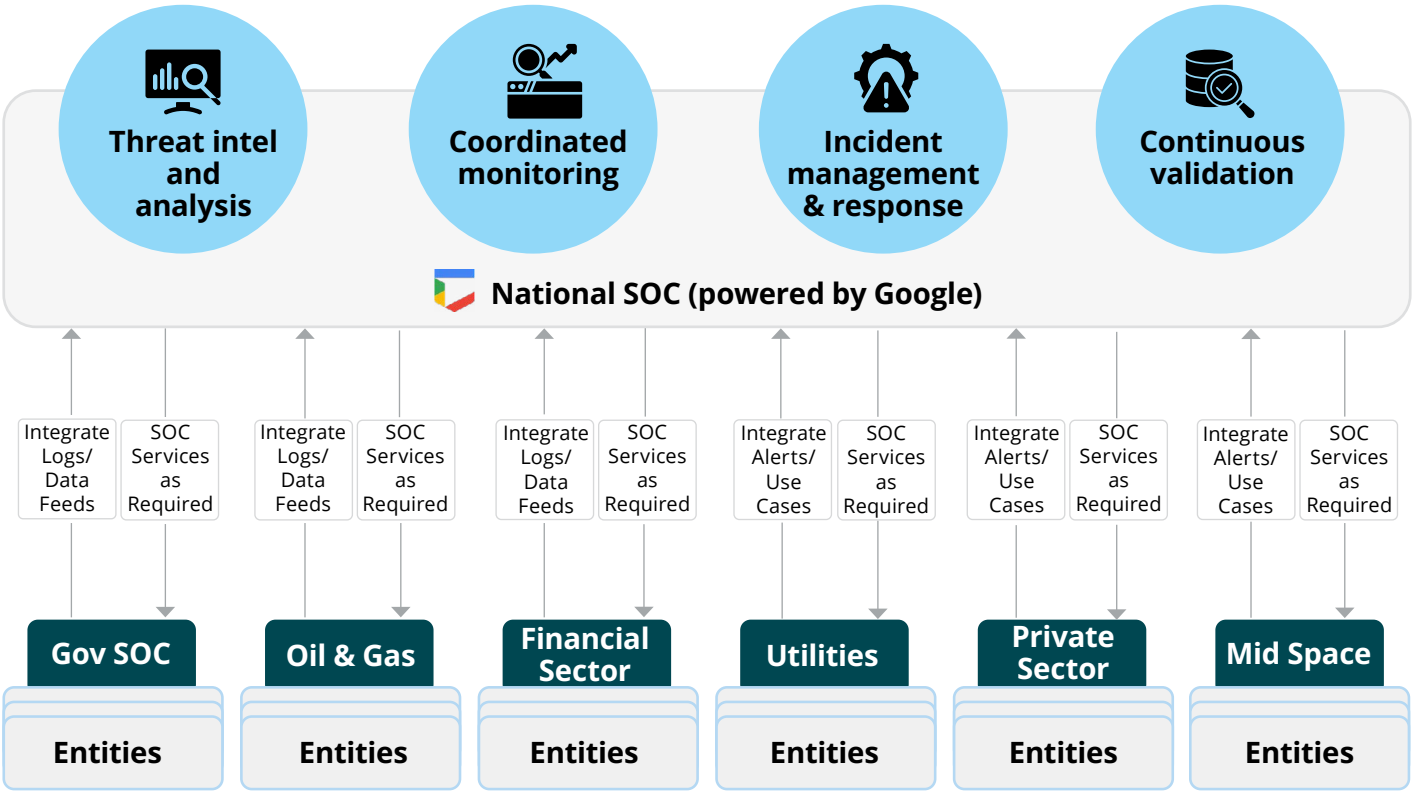
Enhanced decision making:
The platform should provide actionable insights to support informed decision making by the entity leadership. The platform can help prioritise mitigation efforts and resource allocation via modular views by correlating threat intelligence with national critical assets and vulnerabilities.

Advanced threat detection and response:
The platform should use AI-driven analytics to identify and prioritise threats in real time. Automation of routine tasks, such as incident response and vulnerability management, should be prioritised to free up analysts for higher-value activities, such as threat hunting and incident investigation.

Automated threat simulation and training:
Generative AI can be used to create realistic threat simulations for training purposes. This enables cybersecurity teams to develop and test response plans in a safe and controlled environment, enhancing their preparedness for real-world incidents.

Deloitte India Touche Tohmatsu India LLP and **Google Cloud Security** have come together to suggest an approach for establishing the "**Aadhunik Cyber Raksha Pranali**" that the government and public sector entities can rely on. **Google Cloud Cybershield™**, the underlying technology platform, aligns with the vision to drive security governance at scale, secure the nation, accelerate innovation and defend against tomorrow's attacks today.

The National SOC (powered by Google) integrates with multiple sectoral Security Operation Centers (SOCs) and/or state SOCs to aggregate threats and prioritise remediation activity. Initially, the government will benefit and learn from the governement SOC-focused delivery model, identifying additional early enhancement opportunities (for example, existing technologies, Managed Security Services Provider capability and restricted-scope capability to cover the mid-space).



National SOC high-level architecture

Two core components

1. National SOC

Modernised nationwide SOC with capabilities to enhance detection, protect against major threats and automate response and incident management.

2. Expert guidance

Governance, processes and skills required to **build and operate** Cybershield, delivered through a nationwide cyber security capability.

The National capability will detect and automate responses to cybersecurity attacks affecting **Critical National Infrastructure (CNI)** and **government** entities. It will integrate with other SOCs across government entities to deliver the below outcomes:

Enhance the National Cyber Security Centre

- Augment and enhance the current National Cyber Security Centre (NCSC) with cloud-native solutions to improve the agility and scalability of security operations.
- Modernise technology and workflows to automate detection and response.

In-depth security analytics

- Perform **s**ub-second queries on large data sets and analyse historical data at scale.
- Aggregate and enrich data with threat intelligence and additional context to get faster insights.

Continuous feedback loop

- Share information upstream with entities and developers to fix vulnerabilities based on threat intelligence and red teaming exercises.

Centralise data visibility

- Ingest and centralise logs, events and user behaviour analytics in near, real-time from across government entities into the NCSC, to gain deeper visibility into advanced persistent threats and indicators of compromise.

Coordinate response

- Centralised alert triage, case management and response automation will ensure coordination across multiple government entities.

Engineering talent

- Trained analysts with engineering skills to write detection rules and work upstream with DevOps team.
- Analysts create use cases and own the end-to-end lifecycle of threats and spend the majority of time doing engineering/automation vs. operations.

Conclusion

The government sector faces a complex and evolving cyber threat landscape. A new-age cyber defence platform, powered by AI, global threat intelligence and generative AI, is essential for protecting critical national infrastructure, citizen data and national security. Government agencies can significantly enhance their cyber resilience and protect against future threats by investing in this technology and building a skilled cybersecurity workforce.

Detect and analyse

Monitor and detect cyberattacks on IT infrastructure.

Identify threats that can target critical infrastructure, government entities, the private sector or personal user data.

Automate defence against any cyberattacks and provide multiple layers of protection against the full range of digital threats.

+

Respond and recover

Respond to attacks with a swift response to prevent and limit widespread impact.

Resolve existing vulnerabilities to continue to enhance the existing cyber defence capabilities.

Gather cyber threat intelligence on an international scale to better protect and secure the nation.

Aware and secure

Raise awareness and improve the security level across the nation to a level comparable to leading global governments.

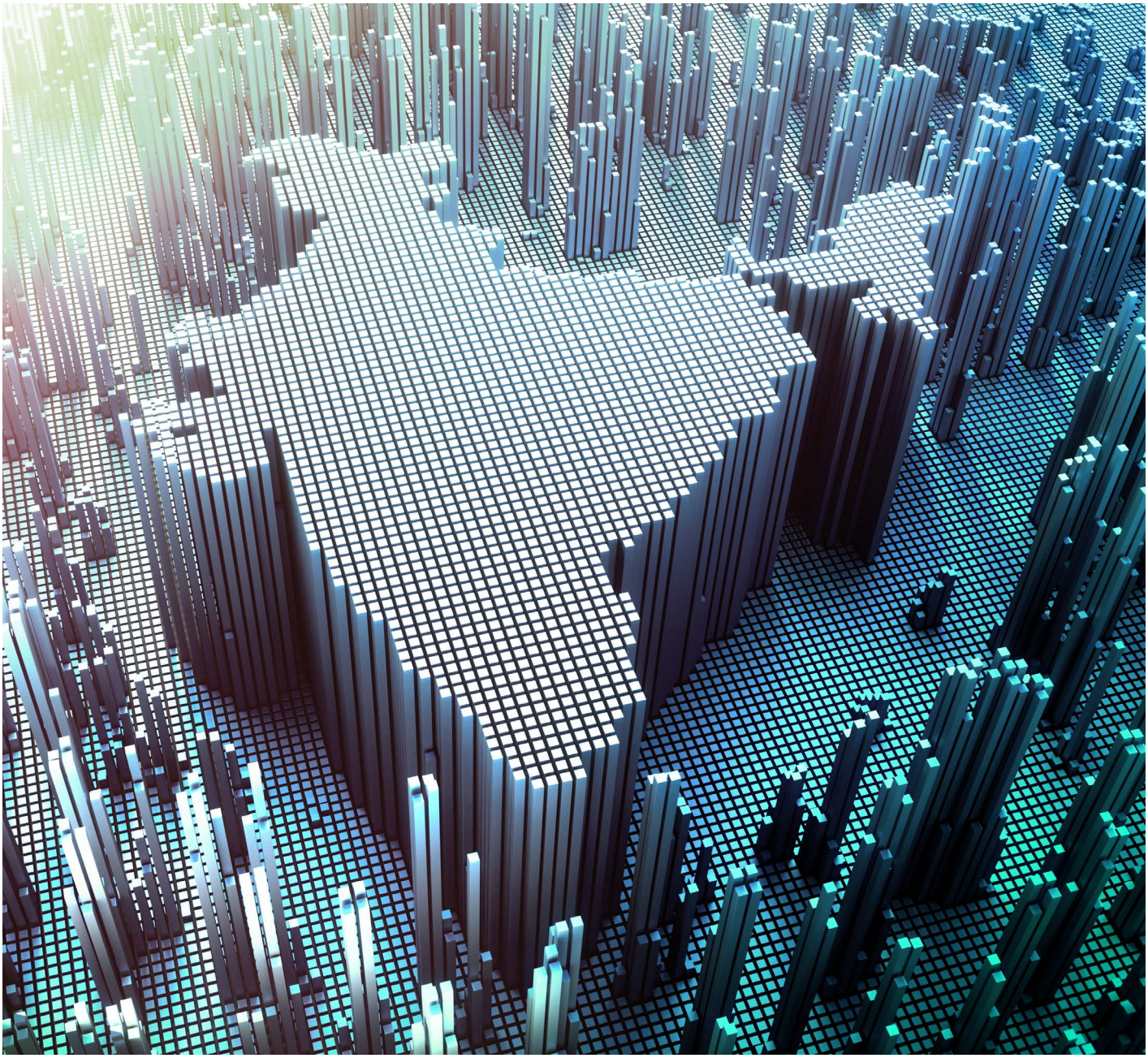
Enable the nation with the necessary governance, skills and knowledge to continue being able to defend and have the best-in-class cyber defence capabilities.

Other references

https://cloud.google.com/blog/products/identity-security/introducing-chronicle-cybershield

https://cloud.google.com/blog/topics/public-sector/cybershield-helping-governments-stand-united-against-cyber-attacks/

https://cloud.google.com/security/transparency/govt-requests/



About Deloitte

Deloitte is one of the world's largest and most diversified professional services organisations, providing assurance and advisory, tax, management consulting, and enterprise risk management services through more than 345,374 professionals in more than 150 countries. Our organisation includes a unique portfolio of competencies integrated in one industry-leading organisation. Deloitte Touche Tohmatsu India LLP (DTTI LLP) also referred as Deloitte India is a member firm in India that provides non-audit consulting services. Our experienced professionals deliver seamless, consistent services wherever our clients operate.

In India, Deloitte is spread across 12 cities with over 12,000 professionals, who are proficient at delivering the right combination of local insight and international expertise to our clientele drawn from across industry segments.

Deloitte is well-equipped to deliver solutions to the complex challenges faced by organisations across the public and private sectors. Our edge lies in our ability to draw upon a well-equipped global network and teaming this with customised services at a local office.

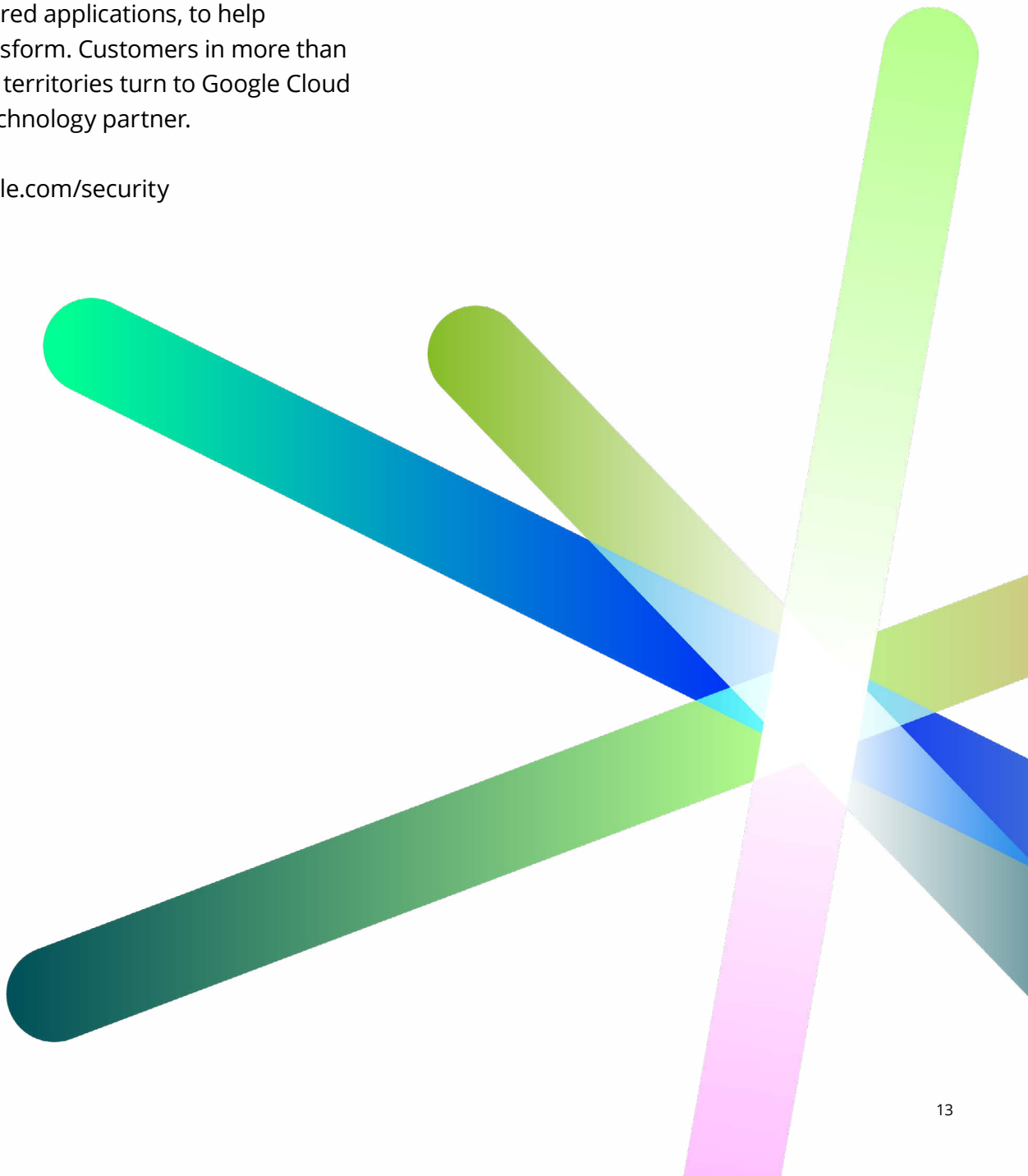
We have been consistently recognised as leaders by Gartner in Cybersecurity, the Data and Analytics space, as well for Public Cloud Infrastructure Managed and Professional Services and Oracle Cloud Application Services.

https://www2.deloitte.com/in/en.html

About Google Cloud

Google Cloud is the new way to the cloud, providing AI, infrastructure, developer, data, security, and collaboration tools built for today and tomorrow. Google Cloud offers a powerful, fully integrated and optimized AI stack with its own planet-scale infrastructure, custom-built chips, generative AI models and development platform, as well as AI-powered applications, to help organizations transform. Customers in more than 200 countries and territories turn to Google Cloud as their trusted technology partner.

https://cloud.google.com/security



Connect with us

Deloitte India

Deepa Seshadri
Partner & Leader - Cyber
Deloitte South Asia
deseshadri@deloitte.com

NSN Murty
Partner, Deloitte India
nsnmurty@deloitte.com

Gaurav Shukla
Partner, Deloitte India
shuklagaurav@deloitte.com

Anand Tiwari
Partner, Deloitte India
anandtiwari@deloitte.com

Tarun Kaura
Partner, Deloitte India
tkaura@deloitte.com

Madhumita Mohapatra
Partner, Deloitte India
madhumitam@deloitte.com

Google Cloud Security

Sandeep Patil
Head APAC Partnerships
Google Cloud Security
sandeeppa@google.com

Ashish Wattal
Head of Gov Business
Google Cloud India
awattal@google.com

Jyoti Prakash
Sales Leader – South Asia
Google Cloud Security
jprakashjp@google.com

Vineet Parmeswaran
GSI Alliances Lead
Google Cloud India
pvineet@google.com

Enrico Risi
Sales Lead - Cybershield
Google Cloud Security
erisi@google.com

Ganesh Supekar
Partnerships Leader –South Asia
Google Cloud Security
supekar@google.com

Nikhiel Sawhney
Head of Public Sector GTM
Google Cloud Security
nikhiel@google.com

Contributors

Deloitte India

Hiten Panchal

Google Cloud Security

Ganesh Supekar

Google Cloud Security

This co-authored whitepaper applies to Google Cloud and Security products described in the Google Cloud Services Summary. The content contained herein is correct as of August 2024 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Deloitte.