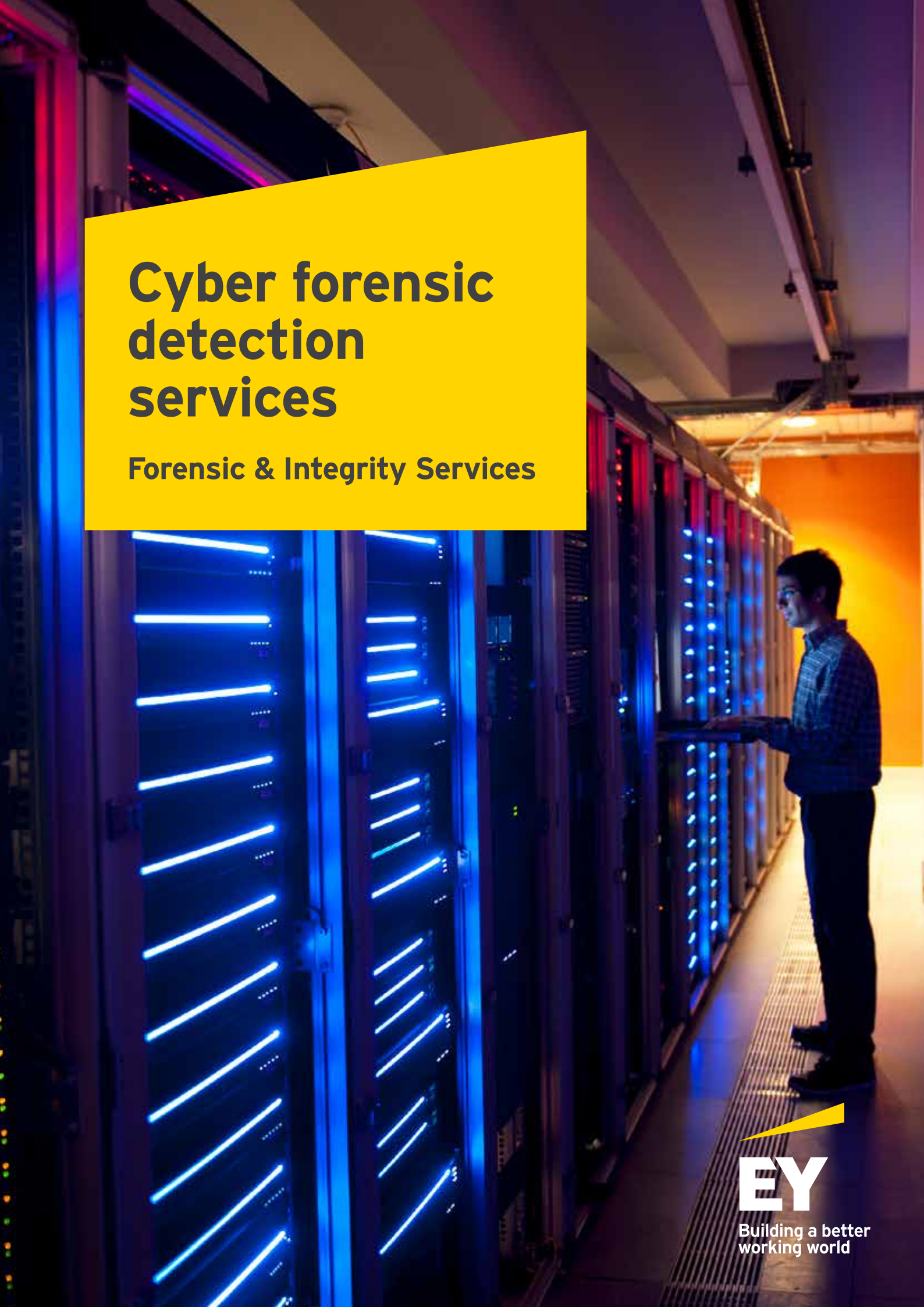


Cyber forensic detection services

Forensic & Integrity Services

EY
Building a better working world

Introduction

Threats and risks

- A **cyber breach** is only detected in average after **205 days**

  Source: Gartner

- Approximately **US$800 billion** of **cybercrimes** are committed globally every year

  Source: McAfee and the Center for Strategic and International Studies Study

- **Attacks and breaches** cost businesses **US$445 billion** every year

  Source: http://www.ey.com/giss

- Estimated **16.7 million identities** of U.S consumers were stolen last year

  Source: Javelin Strategy & Research's 2018 Identity Fraud Report

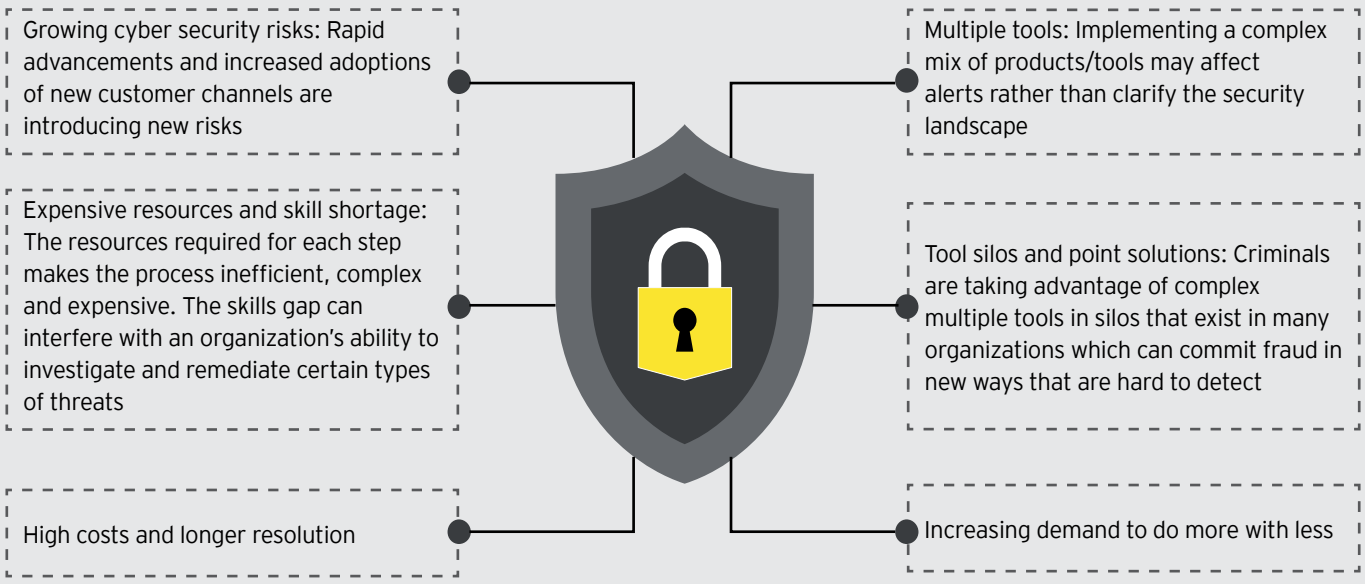
As many organizations have learned, often the hard way, cyber-attacks are unavoidable and breaches are prone to happen. Attackers are increasingly relentless: when one tactic fails, persistent adversaries will try other tactics until they breach an organization's defense. It is a real challenge when companies do not realize they've been breached and fail to react in a planned and co-ordinated manner.

Traditional security audits are no longer enough as sophisticated attackers are consistently finding ways to by-pass current cyber-defenses, stay dormant inside the network for long periods of time and execute the motive while being in camouflage.

Today, in an organization's perspective there is a need for both, quick on demand assessments and year-long continuous monitoring to understand integrity of the network and end points to have a better visibility on current state of compromise, before investing heavily on cyber.

As technology takes a major role in cybersecurity, it will become the foundational element for economic transactions. Each industry would need to develop its applied cybersecurity capability based on a common standard.

Challenges

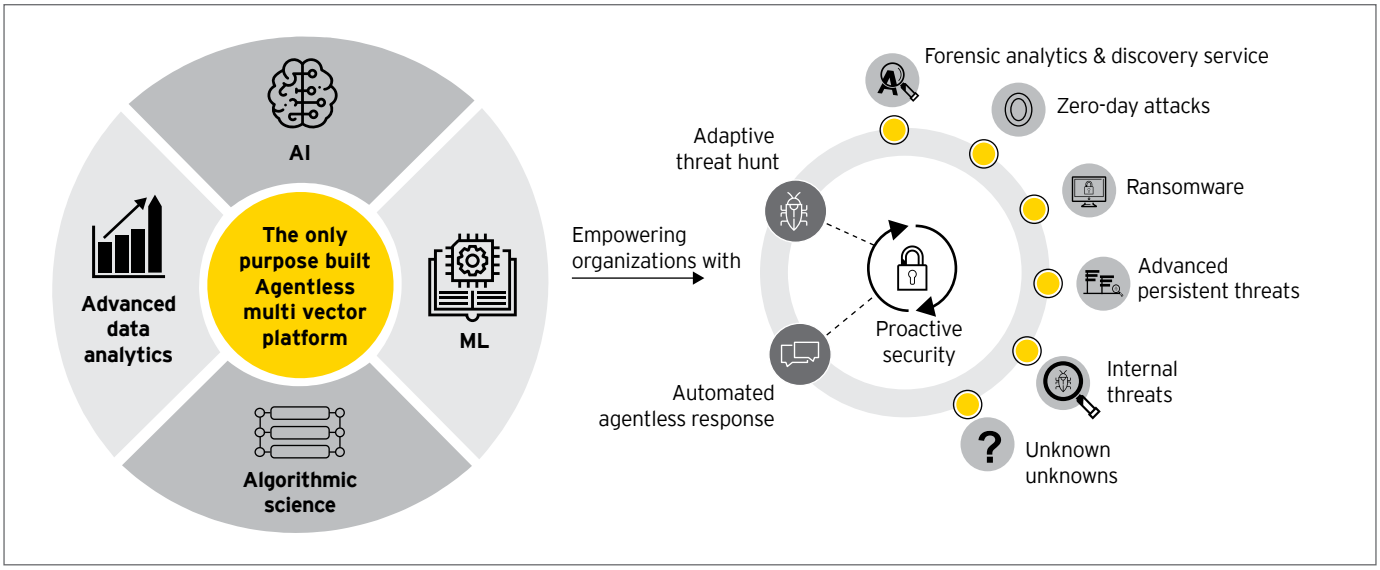


Our solution

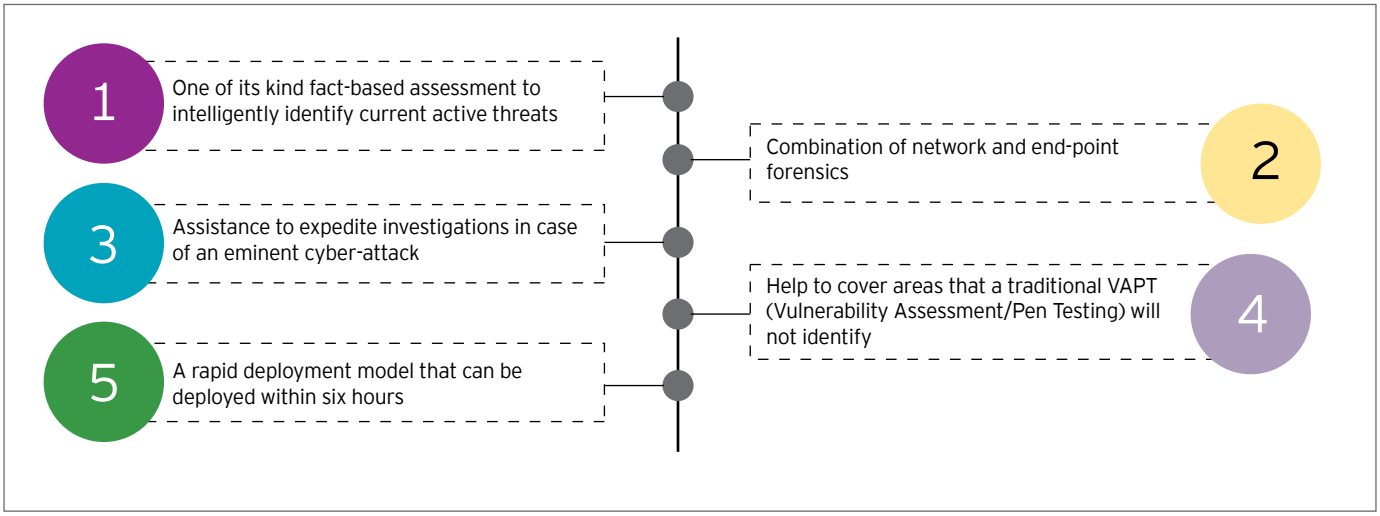
Cyber forensic detection

Unified cyber defense assessment with a combination of intelligent on-demand response automation + network forensics + end-point forensics

As a unique combination of network forensics and end-point forensics, the entire network is scanned and forensically analyzed. With the power of advance cyber defense platform to gain micro level visibility (using Artificial Intelligence and Machine Learning) in tracking existing malware/threats or any malicious activity within the environment and being able to contain it without causing any production latency or issues, a completely end-point agent less model.



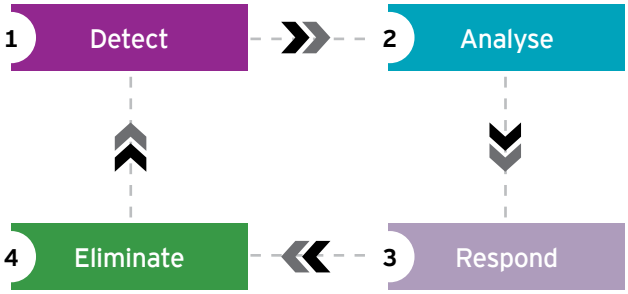
Key features



Our approach

We have sensor and master model. We would deploy sensors at the ingress points where traffic flows in/out of the network. The sensor does a deep packet inspection (DPI), static analysis, looks for any tunneling activity, etc. The master has an AI & ML model which performs binary analysis, dynamic analysis and sandboxing which helps in improved detection.

DARE Model (D –Detect, A –Analyse, R –Respond, E –Eliminate)



The assessment

1. **One-time cyber forensic assessment of the network**
2. **Adaptive threat hunt of the connected/peer networks**
3. **A forensic readiness assessment**
4. **Deliverables - Fact finding report and remediation recommendations**
   a) Current state of the cyber security – based on factual data from the network
   b) Any assets that may have been compromised
   c) Any active bots in the network
   d) Command control traffic
   e) Indicators of potential compromise
   f) Any hidden Advanced Persistent Threat's (APTs)
   g) Zero-day alerts
   h) Hidden tunneling activity
   i) Forensic imaging and reports of infected systems
   j) Malware and ransomware detection

Sr. no.	Potential risk areas	Cyber forensic detection	Penetration test	Vulnerability assessment
1	Can the current state of cybersecurity be identified?	Yes	No	No
2	Are any of assets compromised already?	Yes	No	No
3	Are there any active bots in the network?	Yes	No	No
4	Is there any command and control activity going on in the network?	Yes	No	No
5	Are there any indicators of potential compromise on the network (past/present)?	Yes	No	No
6	Using threat intelligence information, are there any APTs hidden in the network?	Yes	No	No
7	Are there any zero-days that the network is witnessing right now?	Yes	No	No
8	Is there potential outbound traffic that should cause worry?	Yes	No	No
9	Are there any hidden tunneling activity on the network?	Yes	No	No
10	Can it be authoritatively said that there are no unknown/known threats active or passive on the network?	Yes	No	No
11	Are there vulnerabilities on the network?	No	Yes	Yes
12	Are these vulnerabilities exploitable?	No	Yes	No
13	What potential damage can be done by exploiting these vulnerabilities?	No	Yes	No
14	Has an attacker exploited and gained access to the network?	Yes	No	No
15	What gaps exist in the security architecture?	Yes	Yes	No
16	Has any attacker used these gaps and is currently in the network?	Yes	No	No

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

EYIN1903-006
ED None

JG

About Forensic & Integrity Services

Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

ey.com/in

@EY_India EY|LinkedIn YouTube EY India

EY India careers ey_indiacareers

Contact us

Arpinder Singh
Partner and Head – India and Emerging Markets
Direct: + 91 12 4443 0330
Email: arpinder.singh@in.ey.com

Harshavardhan Godugula
Partner
Direct: + 91 40 6736 2234
Email: harshavardhan.g@in.ey.com

Ranjeeth Bellary
Associate Partner
Direct: +91 22 619 20172
Email: ranjeeth.bellary@in.ey.com

Venu Thotakura
Director
Direct: +91 40 6736 2234
Email: venu.v@in.ey.com