KPMG

Cyber Response Services

KPMG Cyber Security Services

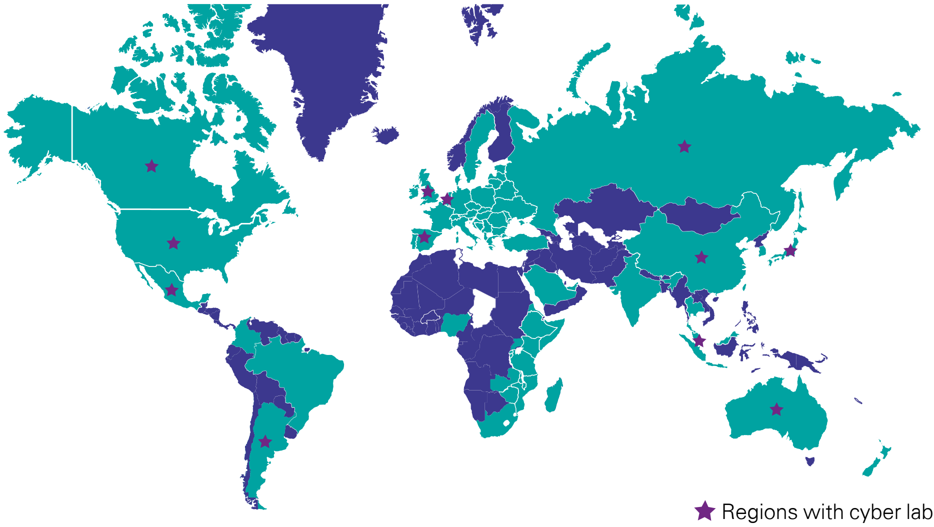
kpmg.com/us/cyber

About us

Global consistency and local capability

KPMG has over 3,500 cyber professionals in offices around the globe with cyber labs across major regions including but not limited to United States, as well as primary cyber labs in the United Kingdom, Spain, Australia, Japan, Netherlands, Russia, Singapore, Malaysia, Canada, China, Mexico, and Argentina.

- Consistent global approach, common methodology
- Rapid response through single point-of-contact and institutional strength



★ Regions with cyber labs

Why KPMG Cyber response?

KPMG Cyber has an extensive professional network within KPMG member firms across the globe that can assist organizations in transforming their security, privacy, and continuity controls into business-enabling platforms. All while maintaining the confidentiality, integrity, and availability of critical business functions. The KPMG Cyber approach strategically aligns with our clients' business priorities and compliance needs:

- Our experienced cyber response professionals possess leading technical experience and are well regarded in their specialties.
- Many of these professionals are leaders in the cyber community, helping to develop the tools and methodologies used to combat cyber crime on a daily basis.
- We have extensive experience building, delivering, and supporting cybersecurity programs for FORTUNE 500 and Global 2000 companies across a multitude of industries.

KPMG Cyber's approach—*Prevent, Improve, Detect, Respond*—is designed to be simple and effective, and most importantly aligned with your business needs.

Our professionals have experience working on various forms of cyber crime, including insider threats, data breaches, hacktivism, and advanced persistent threat-style intrusions by highly motivated adversaries. Our services include on-demand malicious code analysis, host- and enterprise-based forensics, network forensics, threat intelligence, and witness testimony.

KPMG is also heavily involved in the information security community. This involvement provides us with early insight into emerging issues, which we share with our clients and the project support teams as a component of our advisory role. The pragmatic advice and the services we can offer are shaped from the experience gained serving clients of various sizes, scopes, and complexities.

KPMG is a preferred provider of Cyber Response Services to many organizations and acts as an extension of other organizations' internal teams. Lastly, our services are tool agnostic and vendor neutral so our clients can gain comfort knowing that KPMG is entirely driven by our experience and our confidence in our ability to provide value-added assistance.

A commitment to excellence

KPMG* named a leader in The Forrester Wave™: Global Cybersecurity Consulting Providers, Q2 2019

Independent evaluation recognizes KPMG in evaluation on Global Cybersecurity Consulting Providers

KPMG is cited as a leader among Global Cybersecurity Consulting Providers, and was noted for standing out with "clear concise executive level engagement abilities."

The report recognizes that "executive engagement is a key part of [KPMG's] strategy with cybercrisis simulations, a deep metrics offering for CISOs and an initiative that helps security leaders understand the next crisis, not just the current one."

The report acknowledged that "KPMG consistently advances three messages: 1) Cybersecurity helps businesses grow; 2) cybersecurity problems now require multidisciplinary expertise; and 3) cybersecurity protects core business functions. And KPMG doesn't just say those things in its marketing; it infuses those themes into its cybersecurity services portfolio."

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgement at the time and are subject to change.

Frost & Sullivan recognizes KPMG for its innovative KPMG digital responder cyber application

Frost & Sullivan recognized KPMG with its 2017 Global New Product Innovation Award for the firm's innovative KPMG Digital Responder, an automated forensic collection, analysis, and reporting solution.

Distilled from its years of digital forensic and incident response field investigations, KPMG Digital Responder is a flat-rate cyber investigations tool that allows KPMG to automate cyber response from the point of collection to reporting—at a predictable fixed price. It can reduce costs of cyber investigations; shift time spent from collecting data to actual analysis, and provides more time to organizations to make faster, more informed strategic business decisions to manage potential cybersecurity risks.

A review of the current landscape

A cybersecurity breach can strike at any time, putting your entire organization at risk.

As many organizations are recognizing and experiencing first-hand, cyberattacks are no longer a matter of if, but when. Recent cyber breaches at major corporations highlight the increasing sophistication, stealth, and persistence of cyberattacks that organizations are facing today. These breaches result in increased regulatory oversight and may have a negative business impact.

The loss of intellectual property, customer data, and other sensitive information can cause severe financial and reputational damage.

KPMG LLP (KPMG) can help your organization effectively and efficiently respond to cyber incidents. After a breach occurs, companies need to collect breach-related data to secure evidence and support legal and law enforcement investigations. To that end, we conduct forensic analysis and detailed investigations. We have a team of experienced investigative and digital forensic specialists that can help organizations prevent and detect cyber threats and respond effectively to data breaches.

We help leading organizations worldwide effectively manage and protect their most valuable data across a broad spectrum of evolving threats and scenarios. Overall, we approach cybersecurity not as a one-time project, but rather an adaptive strategy aligned to your business goals and focused on delivering long-term value for your business.

Cybersecurity risks remain top of mind

$3.9m

Total average organizational cost of data breach in 2018[1]

More than 40% of audit committees say that risk management programs require substantial work[2]

$600b

Estimated annual cost to the global economy from cyber crime[3]

Three key trends reinforce cyber risk as “a prefect storm”

Growing threat level

From organized crime and hacktivists, as well as threats from within the organization

Changing technology landscape

Surge in digital activity, innovation, cloud, and blurring of the “perimeter”

Compliance pressure

Evolving regulatory and legal frameworks forcing organizations to do more on cybersecurity

Source: IBM, 2018 Cost of Data Breach
Study: KPMG 2017 Global Audit Committee
Source: McAfee Cyber Report, Center for Strategic and International Studies

A holistic approach for your cyber response strategy

Data insecurity is a new business reality

Few would question the importance of making sure data is secure. But having a one-dimensional, technology-focused solutions to cyber threats—focused on protection alone—is missing the bigger picture and may put your organization at greater risk.

At KPMG, we understand that cybersecurity is not just a technology problem—it is a broader business issue.

Beyond digital walls: A strategic approach

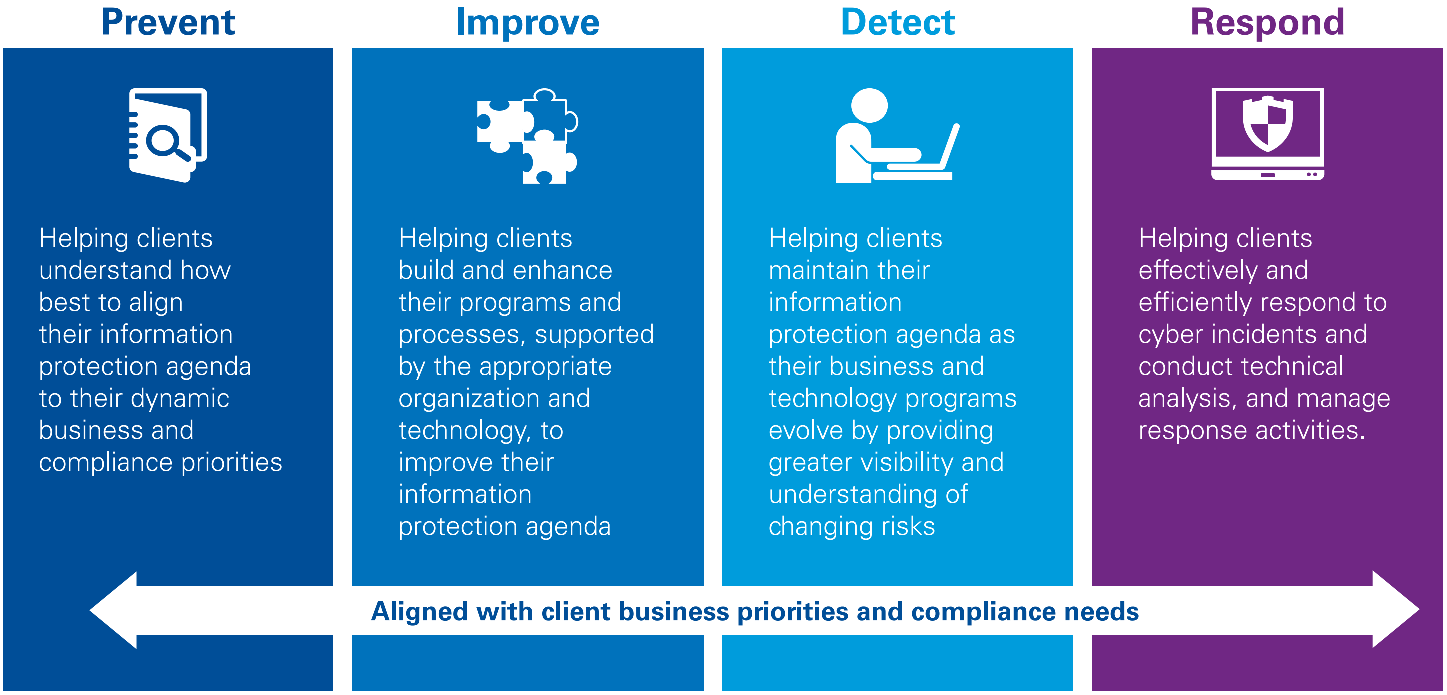
Clearly, the realities of cybersecurity today are very different from those of the past. The near inevitability of an information breach means organizations need to adjust to balance paradoxical demands for data protection and data accessibility for business growth. If success today is defined by an organization's ability to absorb a cyberattack and carry on with business-as-usual, you need a customized strategy that prioritizes business objectives while protecting critical information.

A holistic approach to cybersecurity is more effective and more realistic than simply building digital walls.

Beginning with the individual goals and operations of your enterprise, we build a customized cybersecurity strategy informed by the latest threat intelligence and leading practices that stays on top of key drivers impacting cyber:

- External threats
- Change in the way business is conducted
- Rapid technology change
- Regulatory compliance
- Threat awareness.

How we address cyber security concerns



Prevent

Helping clients understand how best to align their information protection agenda to their dynamic business and compliance priorities

Improve

Helping clients build and enhance their programs and processes, supported by the appropriate organization and technology, to improve their information protection agenda

Detect

Helping clients maintain their information protection agenda as their business and technology programs evolve by providing greater visibility and understanding of changing risks

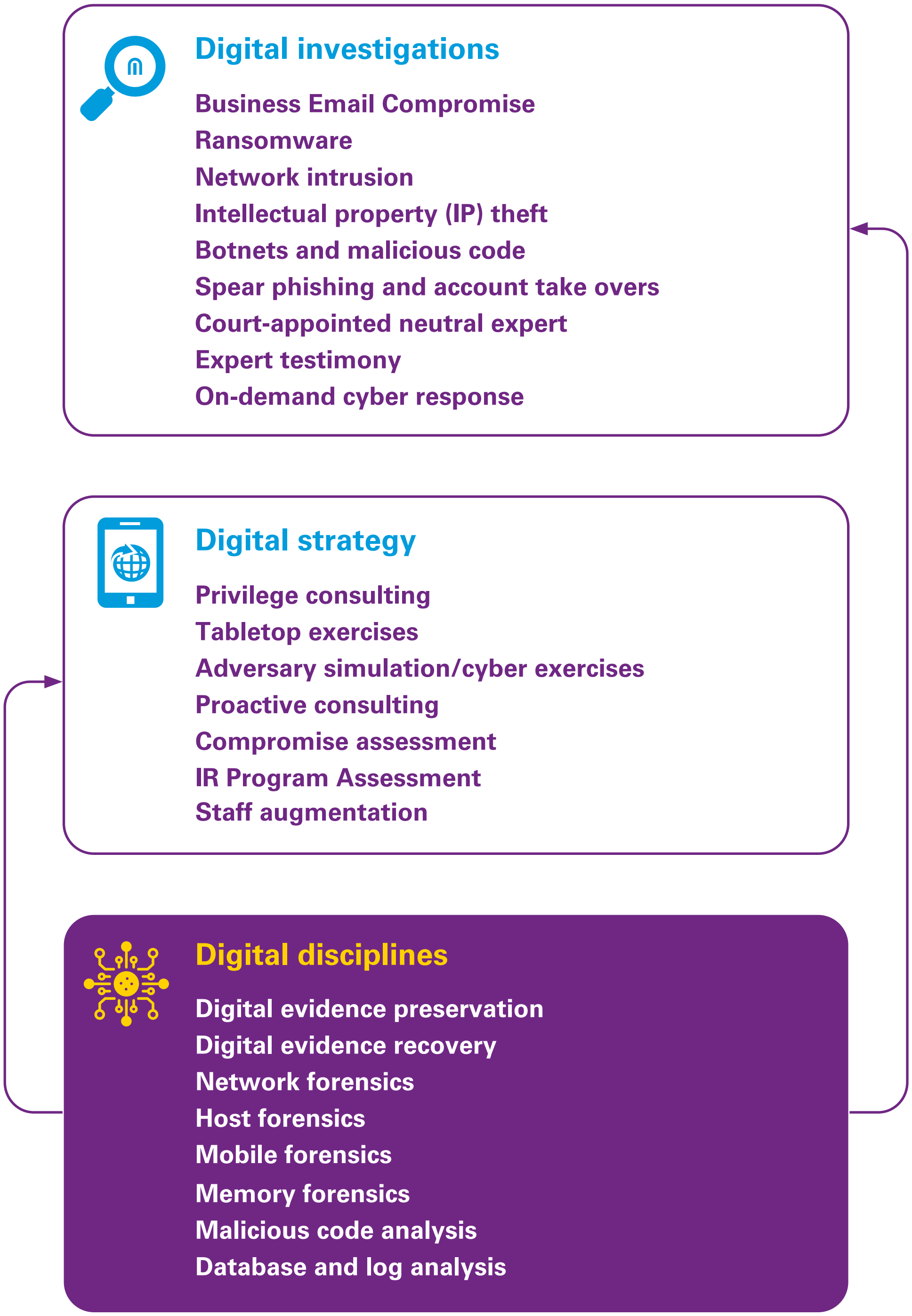
Respond

Helping clients effectively and efficiently respond to cyber incidents and conduct technical analysis, and manage response activities.

Aligned with client business priorities and compliance needs

Cyber response services

A look at our capabilities



Digital investigations

Business Email Compromise
Ransomware
Network intrusion
Intellectual property (IP) theft
Botnets and malicious code
Spear phishing and account take overs
Court-appointed neutral expert
Expert testimony
On-demand cyber response

Digital strategy

Privilege consulting
Tabletop exercises
Adversary simulation/cyber exercises
Proactive consulting
Compromise assessment
IR Program Assessment
Staff augmentation

Digital disciplines

Digital evidence preservation
Digital evidence recovery
Network forensics
Host forensics
Mobile forensics
Memory forensics
Malicious code analysis
Database and log analysis

Efficient execution

Global Evidence Management System (GEMS)

KPMG utilizes industry-leading collection, preservation, and analysis methods for every situation. Evidence acquisitions are handled in accordance with KPMG's digital evidence handling protocols, which include chain-of-custody procedures, authenticity of evidence, encryption, and tracking of physical/logical evidence.

KPMG understands the importance of simplifying evidence management for large and diverse data sets, staying in control of budgets, and maintaining project timelines, all while providing a defensible audit trail to avoid adverse rulings levied in court.

KPMG believes that evidence tracking should be integrated into the incident response process in order to help ensure accuracy, efficiency, and awareness of the data throughout the various phases of a project.

KPMG uses a proprietary evidence management solution called Global Evidence Management System (GEMS).

Tool agnostic

KPMG is tool agnostic and vendor neutral. KPMG is entirely driven by our experience and our confidence in our ability to provide value-added assistance using tools including but not limited to the following.

Network forensics

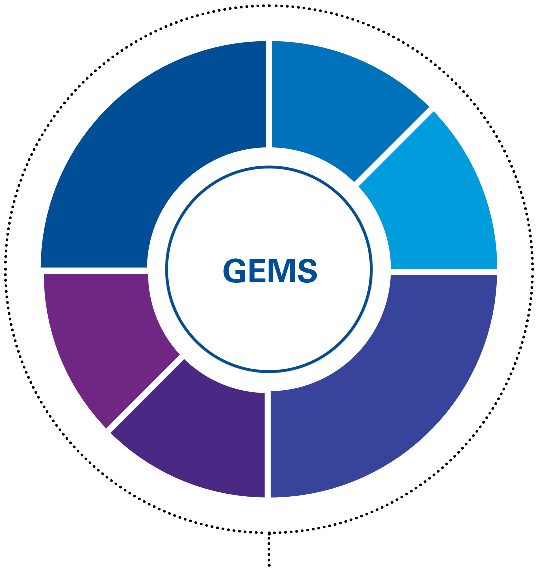
- Fidelis Cybersecurity™
- RSA NetWitness™
- Suricata™
- Wireshark™

Log data

- ArcSight™
- Elasticsearch, Logstash, Kibana™
- LogRhythm™
- Plaso™
- QRadar™
- Splunk™

Endpoint detection & response

- Carbon Black™
- Crowdstrike Falcon™
- Cylance Optics™
- FireEye HX™
- Google Rapid Response™
- Microsoft Defender ATP™
- Sysmon™



KPMG's Global Evidence Management System

Host forensics

- AccessData Forensic™
- F-Response Enterprise™
- NUIX™
- Axiom Forensics suite™
- TZworks™

Memory forensics

- Volatility Framework™
- Rekall™

Malware analysis

- Cuckoo Sandbox™
- Falcon Sandbox™
- Ghidra™
- IDA Pro™
- REMnux™
- Threat Analyzer™

KPMG Digital Responder

KPMG Digital Responder is a sophisticated application that can help information security, compliance, forensic, and legal groups reduce spend, maintain integrity, and increase the effectiveness of response to internal investigations and cyber incidents. The following is an example workflow (see Figure 1).

1. KPMG Digital Responder allows for the targeted collection of forensic artifacts from a live computer or existing disk image, eliminating the need to capture a complete copy of a hard drive.
2. Subsequently, the collected data is securely transferred to KPMG. The data is automatically processed, leveraging leading forensic and incident response techniques.
3. KPMG's specialists review an automated output and deliver a tailored report, which can provide early insights to indicators of uncovering new incidents, who was responsible for an incident, what systems and people were impacted, who may still be at risk, and much more.

This solution can also help supplement EDR products such as Carbon Black™, and Cylance™.

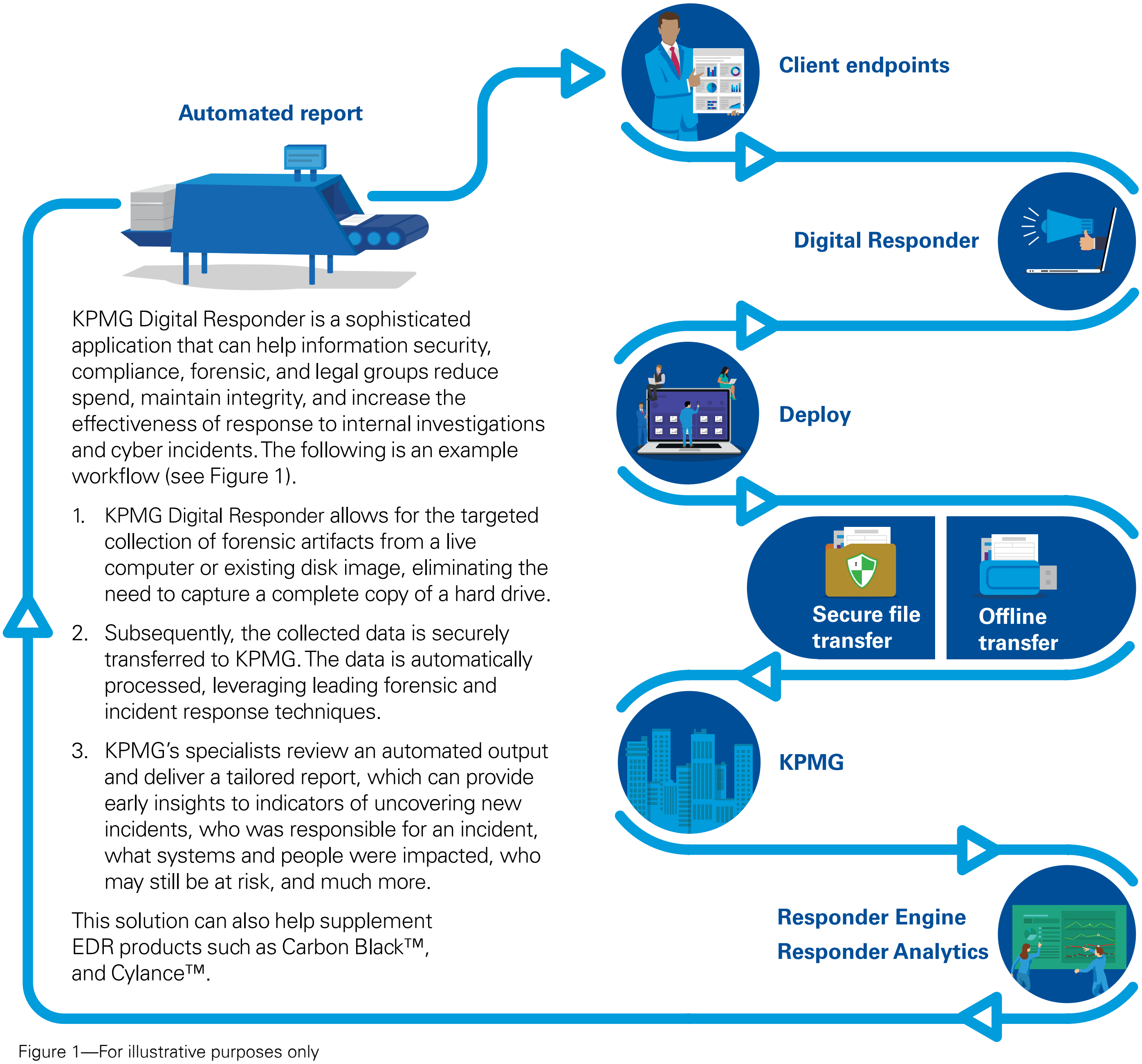


Figure 1—For illustrative purposes only

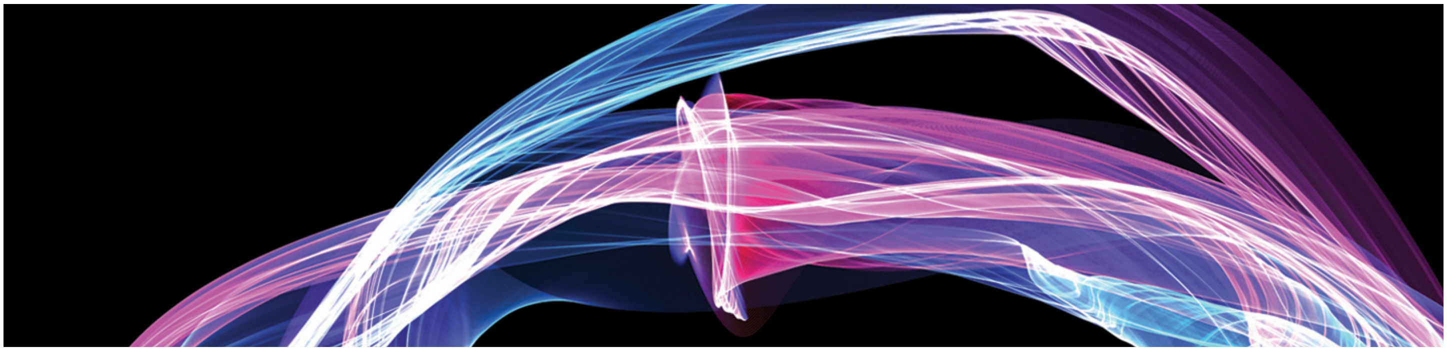
Use case examples

Use case 1—Departing employee(s)
In advance of a Human Resources exit interview, your organization's information technology team can run KPMG Digital Responder on the departing employee's computer(s). This data can then be securely transferred to KPMG in the U.S. to analyze automatically for artifacts, including, but not limited to, removable storage device connections, internet history, non-approved installed applications, mass deletion of files, and recent user activity. In totality, this can produce a standardized report that can be used in the exit interview to formulate questions, such as, "Why did you transfer 200 confidential files to a noncompany removable storage device asset?", "Why did you search how to securely delete files last week", or "What do you use third-party file sharing web services for?"

Use case 2—Malware root cause analysis
Your organization's security team identified a sensitive computer that has potentially been infected with malicious code. The same team runs KPMG Digital Responder on the computer system. This data will then be securely transferred to KPMG in the U.S. to analyze automatically for artifacts, including, but not limited to, infection vector, file execution, malware analysis, lateral movement, and indicators of compromise. In totality, this produces a standardized report that can be used for mitigation, further monitoring, and other remediation activities.

> **“The best way to put this solution into perspective is to think about how you might triage malware. Generally, you submit a file to a sandbox, and in return get a report summarizing what is known about the file, such as how it interacts with the operating system, file system changes, network connections established, and other indicators. It's an effective method for answering generally 90% of your questions. KPMG Digital Responder applies the sandbox methodology to computer system triage and forensics response.”**
>
> —David Nides,
> Managing Director, KPMG Cyber Security Services

KPMG LLP in Action—assisting clients around the globe



Global consulting institution—incident response

A large multibillion-dollar global corporation engaged KPMG to provide incident response services for a global intrusion event. KPMG coordinated and executed the global response effort involving identification, forensic analysis, and containment of over 19,000 systems in six countries. This included packet-level analysis of six months of network activity and behavior/static malware analysis of over 100 behavioral/static analysis of suspicious binaries. KPMG categorized the attack as an advanced persistent threat. KPMG quickly identified how intruders infiltrated the client's network, what activity occurred, what data was exfiltrated, and performed effective remediation. As a result of the quick resolution, KPMG was further engaged to help proactively develop a global incident response plan.

U.S. university—incident response

A U.S. university retained KPMG to conduct an investigation of a series of IT-related incidents. Through the analysis of core network and select employee issued systems, KPMG determined the university's network had been breached, data had been compromised, and the email of top university officials was being actively monitored by an unauthorized source. While performing emergency and long-term remediation based on vulnerability and risk management assessments, KPMG traced evidence of historical and active intrusions back to a former IT employee. KPMG submitted evidence to the U.S. Attorney's office for prosecution of the responsible individual. Additionally, KPMG played a critical role in identifying personal identifiable information that was compromised during the intrusions and assisted university efforts to self-report to approximately 93,000 individuals.

U.S. hospital—Digital evidence collection

As part of ongoing litigation and anticipation of a U.S. government investigation, KPMG was retained by one of the largest teaching hospitals in the United States to coordinate the collection of digital media and hard copy documents from an active research facility. To meet the client's request to minimize disruption to the research facility and quickly complete the collections, KPMG assembled a team of 25 forensic professionals to collect over 130 TB of electronically stored information from 3,900 digital media devices and 500 boxes of hard copy documents in 108 hours.

The digital media collected was part of the hospital's infrastructure and bring your own device (BYOD) program with varying specifications and configurations, including Macintosh (MAC), Windows, and Linux systems. KPMG had to work with outside counsel, in-house counsel, IT professionals, and the medical researchers to develop the most effective way to collect the data with minimal operational disruption to the ongoing research. KPMG followed its standard operating procedures to help ensure forensic imaging and document the transfer of chain of custody per leading industry practices. KPMG also developed a customized methodology to meet the client's expectations and successfully collected data from the individual custodians, lab workstations, medical equipment, external media, network shares, personal shares, email servers, and hard copy documents leveraging the industry leading and proprietary forensic tools.

Global online retailer—incident response

A global online retailer experienced its largest breach in company history. User accounts were discovered to have exfiltrated their network due to a compromise of VPN and user credentials. KPMG was asked to assist with the investigation when the client realized they needed a holistic approach to dealing with the breach, including global digital evidence recovery/analysis, IR planning, crisis management support, data analytics, and security monitoring. Within 4 hours, KPMG had "boots on the ground," and within 48 hours, had a full team on-site.

KPMG helped the client identify the point of exfiltration and discovered that over 100 million customer records had been stolen. Security agents were deployed to tens of thousands of computers across their enterprise to analyze the extent of the breach, and KPMG digitally preserved over 100 systems located across the United States, United Kingdom, Ireland, Germany, and India.

KPMG engaged with the client's outside counsel to maintain privilege, became the central support in the war room as well as a hub for crisis planning/management—24/7 support was provided for the duration of the crisis. KPMG worked with their security monitoring team to identify and correlate various disparate logs to enhance security monitoring for indicators of compromise (IOC) and additional attacker activity, and worked with the war room team to prepare reports for board updates, media releases, and ultimately, United States Congress. KPMG then assisted the client with remediation efforts, including developing additional monitoring and analytical capabilities, implementing identity access management platform and processes, revamping IR playbook, determining next-generation authentication options to eliminate passwords, and replanning of computer forensics lab and capabilities.

A multinational fortune 100 company—incident response

KPMG coordinated incident response to one of the most wide-spread cybersecurity incidents in healthcare industry. One of the company's business lines sold healthcare related software to hundreds of healthcare organizations across the United States—and remotely administered this software within their customer environments using a commercial remote software application. The credentials to this software were stolen and used by an attacker to subsequently access over 50 of their customer's IT environments—of which many were protected entities maintaining highly sensitive information. KPMG assisted the corporation in notifying each of their customers of the security incident including offering IR services to assist them with investigating. As a result, KPMG directly engaged with over 30 of their customers during Thanksgiving week to assist with determining the scope and depth of each individual network intrusion. While supporting 30 simultaneous network intrusion investigations, KPMG also played a key adviser role to the client that was responsible for these breaches by providing executive briefings and liasoning with law enforcement.

Global investment firms—neutral expert

In the matter involving two investment firms, KPMG was appointed as the Neutral Expert. KPMG was tasked with completing computer forensic analysis on data from both parties surrounding allegations of "source code" theft from a high-frequency financial trading platform. KPMG successfully analyzed and processed over nine terabytes of data and shared our results with both parties in accordance with the Court issued protocol. KPMG performed extensive analysis of unallocated and slack space to locate deleted information. KPMG advised and worked with both parties to develop processes for the parties to review recovered unallocated data clusters. KPMG also assisted both parties in their review of data, including the development of privilege logs and production of relevant documents.

Large public company—incident response

For a large public company, KPMG coordinated global IR to a cyberattack involving Shamoon malware. This malware was known to first target the oil and gas industry in August 2012, when reported tens of thousands of computers in the Middle East were destroyed. KPMG's client was impacted by a variant of this malware which researchers publicly attributed to the Iranian hacking group APT33. This resulted in tens of thousands of computers across the company being inoperable—and losses of millions of dollars a day in productivity. In response, KPMG helped coordinate a multinational team including U.S., U.K., and Singapore to standup a 24x7 enterprise monitoring and containment operation to isolate the propagation of malware. We further assisted with the investigation of root cause analysis and remediation.

Large hospital—ransomware

For a large affiliated hospital network, KPMG led the recovery following a ransomware attack that resulted in complete loss of access to its electronic health records database—to the point which impacted multiple hospitals from servicing patients. After another IR vendor was unsuccessful, KPMG reverse-engineered the ransomware to determine how it encrypted the data and developed an innovative approach to fully recover their data and help restore operations—an effort most would have considered impossible. KPMG was then further engaged to assist with the structured data sensitive data review to assist with notification obligations.

Contact us

Ed Goings
Principal,
Cyber Security Services
E: egoings@kpmg.com

Jim Arnold
Principal,
Cyber Security Services
E: jrarnold@kpmg.com

David Nides
Principal,
Cyber Security Services
E: dnides@kpmg.com

David Cowen
Managing Director,
Cyber Security Services
E: dcowen@kpmg.com

David Shin
Managing Director,
Cyber Security Services
E: dhshin@kpmg.com

Emergency? Can't get a hold of us?
Call KPMG's 24x7 Cyber hotline: 855-444-0087

kpmg.com/us/cyber

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.