Google Cloud

Google Cloud Whitepaper
September 2018

Data incident response process

The content contained herein is correct as of June 2018 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 data protection for our customers.

Introduction

Maintaining a safe and secure environment for customer data is Google Cloud's highest priority. To protect customer data, Google runs an industry-leading information security operation that combines stringent processes, a world-class team, and multi layered information security and privacy infrastructure. This paper focuses on Google's principled approach to managing and responding to data incidents for Google Cloud.

Incident response is a key aspect of Google's overall security and privacy program. We have a rigorous process for managing data incidents. This process specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of customer data.

At Google, a data incident is defined as a breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, customer data on systems managed by or otherwise controlled by Google. While Google takes steps to address foreseeable threats to data and systems, data incidents do not include unsuccessful attempts or activities that do not compromise the security of customer data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

We have a rigorous process for managing data incidents. This process specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of customer data.

How Google helps secure customer data

The security of customer data is of the utmost importance, but security is the outcome of the collaboration between Google and the customer. While Google secures the underlying cloud infrastructure and services, the customer secures their applications, devices, and systems when building on top of Google's Cloud infrastructure. Google provides customers with guidance and multiple security features to enable Google-grade security practices:

- Identity and access management
- Data encryption at rest and in transit by default, i.e., without any additional effort from customers
- Multi factor authentication, including phishing-resistant hardware second factor key
- A range of network security options including virtual private cloud (VPC) and shared VPC, built-in DDoS protection for software-as-a-service (SaaS), platform-as-a-service (PaaS) solutions and the option to use these for infrastructure-as-a-service (IaaS) solutions as well
- Detailed audit logging

To learn more about how Google secures the cloud, see Google's Infrastructure Security Design Overview paper and the associated NEXT '18 security presentation or visit Google Cloud Security Site.

Google provides customers with visibility across the services they use on Google Cloud; customers can use the security center for G Suite to prevent, detect, and remediate issues with Gmail, Drive, Devices, OAuth, and User Accounts. Similarly for GCP, customers can use Cloud Security Command Center to gain visibility into their assets, vulnerabilities, risks, and policy across their organization.

On their end, customers must properly configure security features to meet their own needs, install software updates, set up networking security zones and firewalls, and ensure that end users secure their account credentials and are not exposing sensitive data to unauthorized parties.

Figure 1 provides an illustrative example of how the responsibility shifts between the customer and Google based on the extent of managed services leveraged by the customer. As the customer moves from on-premises solutions to IaaS, PaaS, and SaaS cloud computing offerings, Google manages more of the overall cloud service, and the customer has fewer security responsibilities.

For more information on cloud security configurations, customers should reference the applicable product documentation.

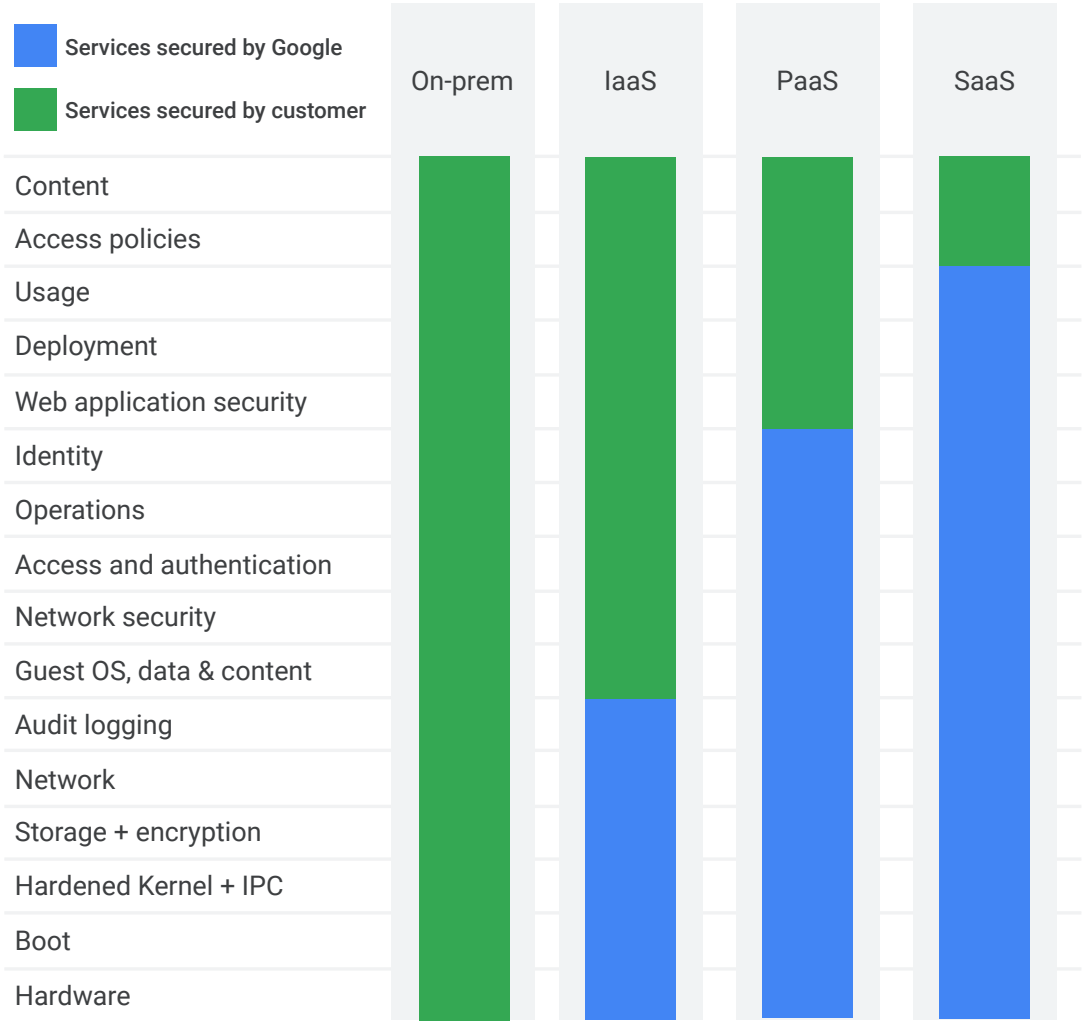

Figure 1: Responsibility chart

Data incident response

Google's incident response program is managed by teams of expert incident responders across many specialized functions to ensure each response is well-tailored to the challenges presented by each incident. Depending on the nature of the incident, the professional response team may include:

- Cloud incident management
- Product engineering
- Site reliability engineering
- Cloud security and privacy
- Digital forensics
- Global investigations
- Signals detection
- Security, privacy, and product counsel
- Trust and safety
- Counter abuse technology
- Customer support

Subject matter experts from these teams are engaged in a variety of ways. For example, incident commanders coordinate incident response and, when needed, the digital forensics team detects ongoing attacks and performs forensic investigations. Product engineers work to limit the impact on customers and provide solutions to fix the affected product(s). The legal team works with members of the appropriate security and privacy team to implement Google's strategy on evidence collection, engage with law enforcement and government regulators, and advise on legal issues and requirements. Support personnel respond to customer inquiries and requests for additional information and assistance.

Team organization

When we declare an incident, we designate an incident commander who coordinates incident response and resolution. The incident commander selects specialists from different teams and forms a response team. A typical response organization appears in Figure 2 below. The incident commander delegates the responsibility for managing different aspects of the incident to these professionals and manages the incident from the moment of declaration to closure. Figure 2 depicts the organization of various roles and their responsibilities during incident response.

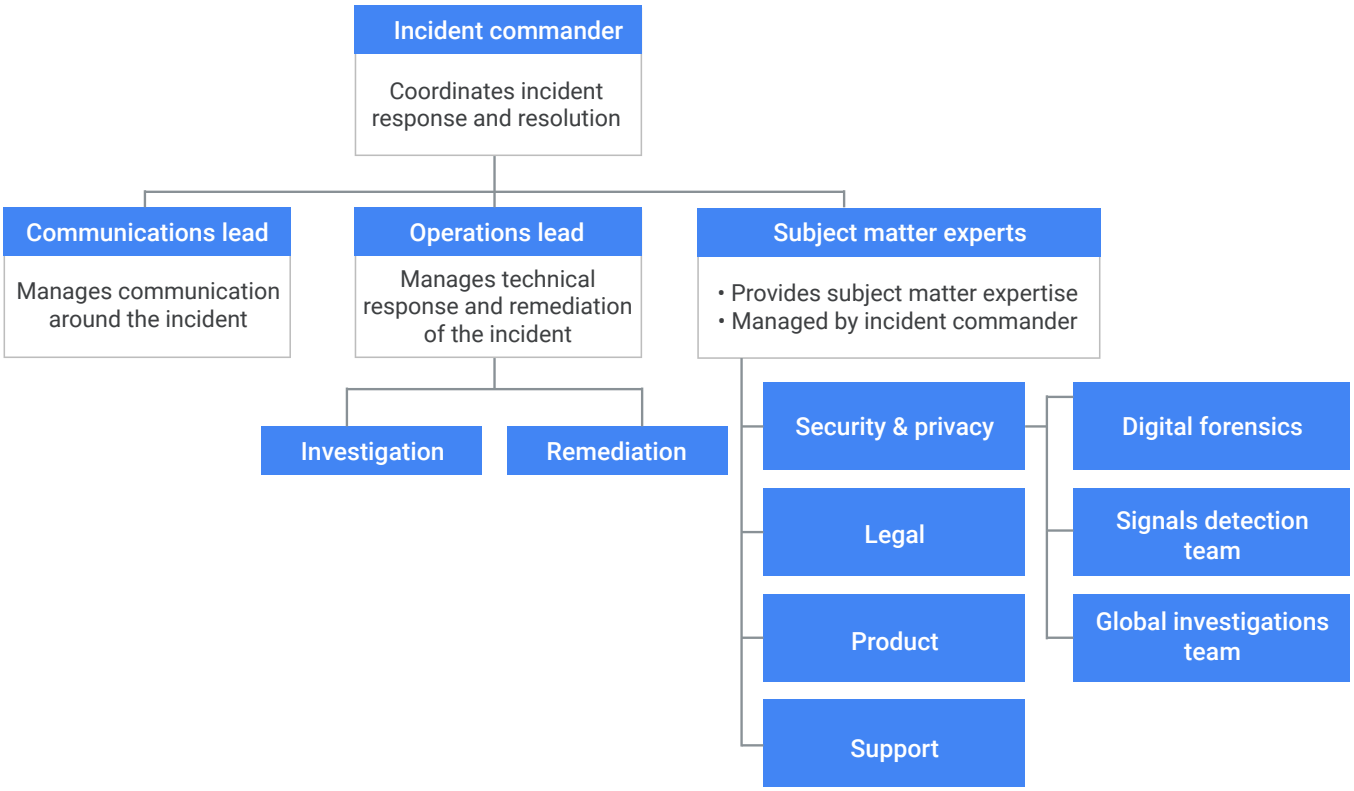

Figure 2: Data incident response team organization

Data incident response process

Every data incident is unique, and the goal of the data incident response process is to protect customers' data, restore normal service as quickly as possible, and meet both regulatory and contractual compliance requirements. Google's incident response program has the following process:

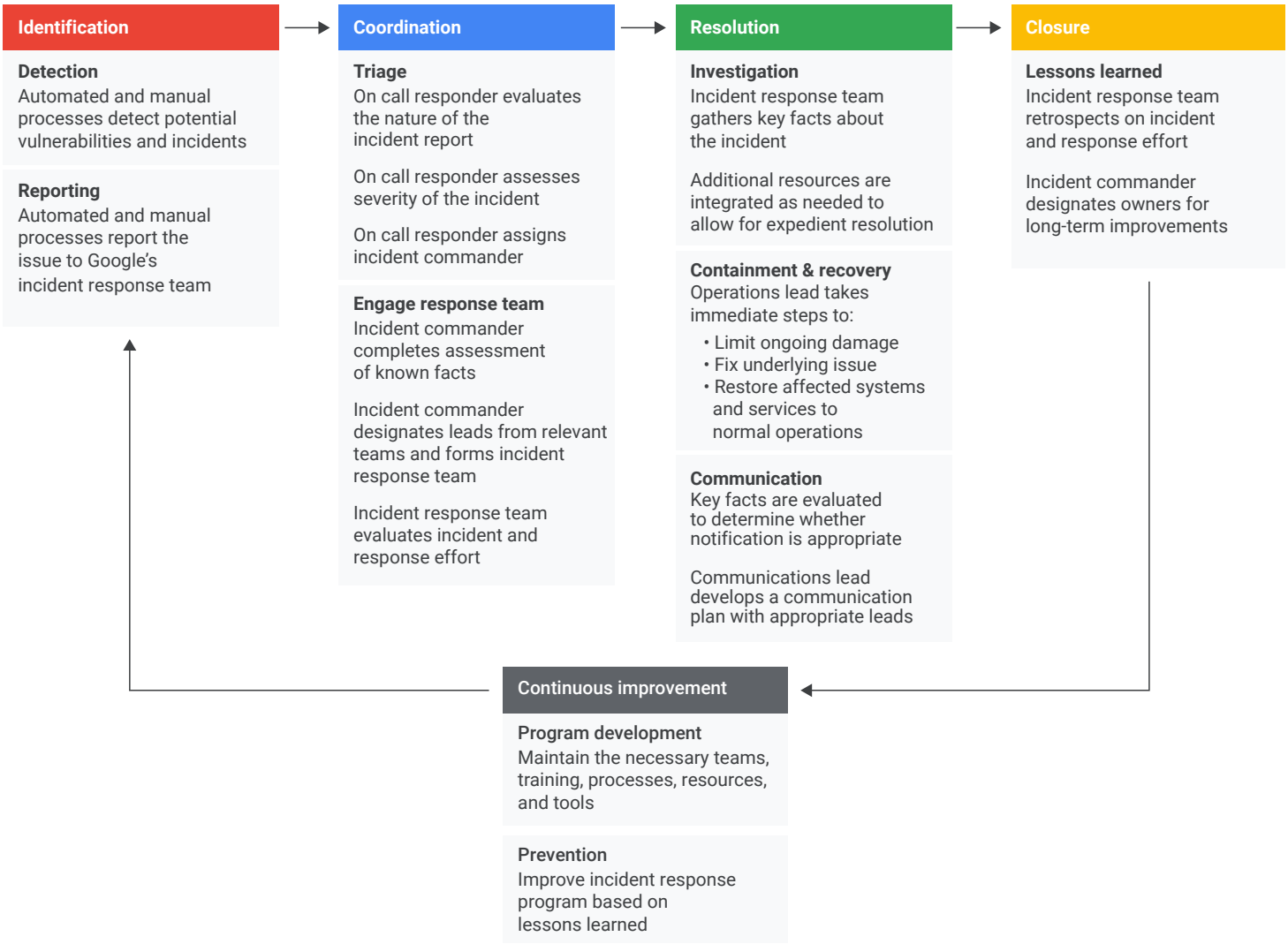

Figure 3: Incident response workflow

Identification

Early and accurate identification of incidents is key to strong and effective incident management. The focus of this phase is to monitor security events to detect and report on potential data incidents.

Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents.

Google's sources of incident detection include:

- Automated network and system logs analysis — Automated analysis of network traffic and system access helps identify suspicious, abusive, or unauthorized activity and escalates to Google's security staff
- Testing — Google's security team actively scans for security threats using penetration tests, quality assurance (QA) measures, intrusion detection, and software security reviews
- Internal code reviews — Source code review discovers hidden vulnerabilities, design flaws, and verifies if key security controls are implemented
- Product-specific tooling and processes — Automated tooling specific to the team function is employed wherever possible to enhance Google's ability to detect incidents at product level
- Usage anomaly detection — Google employs many layers of machine learning systems to differentiate between safe and anomalous user activity across browsers, devices, application logins, and other usage events
- Data center and / or workplace services security alerts — Security alerts in data centers scan for incidents that might affect the company's infrastructure
- Google employees — A Google employee detects an anomaly and reports it
- Google's vulnerability reward program — Potential technical vulnerabilities in Google-owned browser extensions, mobile, and web applications that affect the confidentiality or integrity of user data are sometimes reported by external security researchers

Google's incident detection team employs advanced detection tools, signals, and alert mechanisms that provide early indication of potential incidents.

Coordination

When an incident is reported, the on-call responder reviews and evaluates the nature of the incident report to determine if it represents a potential data incident and initiates Google's Incident Response Process.

Once confirmed, the incident is handed over to an incident commander who assesses the nature of the incident and implements a coordinated approach to the response. At this stage, the response includes completing the triage assessment of the incident, adjusting its severity if required, and activating the required incident response team with appropriate operational/technical leads who review the facts and identify key areas that require investigation. We designate a product lead and a legal lead to make key decisions on how to respond. The incident commander assigns the responsibility for investigation and the facts are assembled.

Many aspects of Google's response depend on the assessment of severity, which is based on key facts that are gathered and analyzed by the incident response team. These may include:

- Potential for harm to customers, third parties, and Google
- Nature of the incident (e.g., whether data was potentially destroyed, accessed, or unavailable)
- Type of data that may be affected
- Impact of the incident on customers' use of the service
- Status of the incident (e.g., whether the incident is isolated, continuing, or contained)

The incident commander and other leads periodically re-evaluate these factors throughout the response effort as new information evolves to ensure that Google's response is assigned the appropriate resources and urgency. Events that present the most critical impact are assigned the highest severity. A communications lead is appointed to develop a communications plan with other leads.

Resolution

At this stage, the focus is on investigating the root cause, limiting the impact of the incident, resolving immediate security risks (if any), implementing necessary fixes as part of remediation, and recovering affected systems, data, and services.

Affected data will be restored to its original state wherever possible. Depending on what is reasonable and necessary in a particular incident, Google may take a number of different steps to resolve an incident. For instance, there may be a need for technical or forensic investigation to reconstruct the root cause of an issue or to identify any impact on customer data. Google may attempt to recover copies of the data from Google's backup copies if data is improperly altered or destroyed.

A key aspect of remediation is notifying customers when incidents impact their data. Key facts are evaluated throughout the incident to determine whether the incident affected customers' data. If notifying customers is appropriate, the incident commander initiates the notification process. The communications lead develops a communication plan with input from the product and legal leads, informs those affected, and supports customer requests after notification with the help of our support team.

Google strives to provide prompt, clear, and accurate notifications containing the known details of the data incident, steps Google has taken to mitigate the potential risks, and actions Google recommends customers take to address the incident. We do our best to provide a clear picture of the incident so that customers can assess and fulfill their own notification obligations.

Closure

Following the successful remediation and resolution of a data incident, the incident response team evaluates the lessons learned from the incident. When the incident raises critical issues, the incident commander may initiate a post-mortem analysis. During this process, the incident response team reviews the cause(s) of the incident and Google's response and identifies key areas for improvement. In some cases, this may require discussions with different product, engineering, and operations teams and product enhancement work. If follow-up work is required, the incident response team develops an action plan to complete that work and assigns project managers to spearhead the long-term effort. The incident is closed after the remediation efforts conclude.

We do our best to provide a clear picture of the incident so that customers can assess and fulfill their own notification obligations.

Continuous improvement

At Google, we strive to learn from every incident and implement preventative measures to avoid future incidents.

The actionable insights from incident analysis enable us to enhance our tools, trainings and processes, Google's overall security and privacy data protection program, security policies, and / or response efforts. The key learnings also facilitate prioritization of engineering efforts and building of better products.

Google's security and privacy professionals enhance the security program by reviewing the company's security plans for all networks, systems, and services and provide project-specific consulting services to product and engineering teams. They deploy machine learning, data analysis, and other novel techniques to monitor for suspicious activity on Google's networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular security assessments. Additionally, our full-time team, known as Project Zero, aims to prevent targeted attacks by reporting bugs to software vendors and filing them in an external database.

Google conducts regular trainings and awareness campaigns to drive innovation in security and data privacy. The dedicated incident response staff are trained in forensics and in handling evidence, including the use of third-party and proprietary tools. Testing of incident response processes and procedures is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities and help us better prepare for security and privacy incidents.

Google's processes are tested on a regular basis as part of our ISO-27017, ISO-27018, ISO-27001, PCI-DSS, SOC 2 and FedRAMP programs to provide our customers and regulators with independent verification of our security, privacy, and compliance controls. A more comprehensive list of Google Cloud's third-party certifications is available here.

Summary

As detailed above, Google operates a world-class incident response program that delivers these key functions:

- A process built upon industry-leading techniques for resolving incidents and refined to operate efficiently at Google's scale
- Pioneering monitoring systems, data analytics, and machine learning services to proactively detect and contain incidents
- Dedicated subject matter experts who can be deployed to respond to any type or size of data incident
- A mature process for promptly notifying affected customers, in line with Google's commitments in our terms of service and customer agreements

Protecting data is core to Google's business. We continually invest in our overall security program, resources, and expertise, which enables our customers to rely on us to respond effectively in the event of an incident, protect their data, and maintain the high reliability customers expect of a Google service.

We continually invest in our overall security program, resources, and expertise, which enables our customers to rely on us to respond effectively in the event of an incident, protect their data, and maintain the high reliability customers expect of a Google service.