Case Study

Lookout Protects Cloud Data of a U.S. Disaster Restoration Company Amidst Acquisitions

The Challenge

To deliver services, disaster restoration companies share sensitive information with third-party contractors and service providers all the time. While this is a mundane business operation, it unintentionally increases the risk data exfiltration.

To keep pace with technological advancement, a U.S.-based disaster restoration company had moved their operations to the cloud. And to ensure that the sensitive data they handle remained protected, it needed a robust cloud access security broker (CASB) solution.

The company chose Lookout Secure Cloud Access because of its native data loss prevention (DLP) capabilities, which ensure that sensitive data is discovered and protected with the appropriate policies. As a cloud-delivered service and part of a broader platform, Secure Cloud Access is able to easily onboard other SaaS applications and apply policies without any additional work.

This disaster restoration was able to secure both Google Workspace, including its suite of apps, and Salesforce. With integrated insights and a consistent policy framework across these apps, Lookout enabled their security team to secure their data and comply with regulations. This scalability was critical as it enabled the organization to expand its operations through a series of acquisitions without adding complexity to its security stack.

Business growth through acquisitions brings data security challenges

To keep up with the demand for disaster restoration, the company acquired several organizations over a span of just two years. As is typical, each acquisition brought its own operational challenges, among these was the integration of existing processes from the acquired companies and the enforcement of data security policies across these new environments.

Here were some of their key security objectives:

Control access to data at a granular level

To secure sensitive data and comply with regulations, the company wanted greater control over access to specific data by employees of acquired organizations and contractors who had to access their data.

Comprehensive visibility into data usage

Full control over data starts with visibility. The company also needed continuous insights into how its data was being handled so it could write the appropriate policies that are precise and don't get in the way of productivity. By having visibility into data usage, the company was then able to write appropriate policies.

Advanced data loss prevention

With its operations in the cloud, the company needed a solution with DLP capabilities that cover data residing in SaaS apps.

Focus on the business by simplifying IT security

An issue with operating in the cloud is the fragmentation of IT security management. Every app had its own controls that required dedicated management resources. The company was looking to security so its IT teams could focus on business objectives.

Results: Simplified IT security and robust data protection

With sensitive data residing in SaaS apps, and disparate systems from acquisitions that needed to be secure, the company began a search for a CASB with advanced DLP.

After a competitive bake-off and proof-of-concept analysis, they chose Lookout Secure Cloud Access for its ability to provide consistent and robust data protection for Salesforce and Google Workspace. With Lookout in place, the company could securely provide disaster recovery services while knowing their data is protected at all times.

Define and enforce access through granular control

As a disaster recovery services organization, employees and contractors in the field needed real-time remote access to sensitive data such as personally identifiable information (PII) and protected health information (PHI) of disaster victims. These data types are protected by data privacy regulations such as Health Insurance Portability and Accountability Act (HIPAA). A key part of this is ensuring only authorized personnel have access to the specific data approved for them.

Lookout Secure Cloud Access met all these requirements. With full insights into a user's behavior, the health of their device, location, and type of data requested — the Lookout CASB solution is able to enforce granular security controls. Privileges had to be restricted so that field-level employees, who generally used company-issued laptops, were only allowed to view and download information that pertained to their specific role. Policies also enforced access limitations for contractors, who typically used unmanaged devices.

With both forward and reverse proxy capabilities, Lookout is able to detect whether a device is managed or unmanaged, and applies the appropriate access policy for the device type. With this level of access in place, individual users can securely connect to the apps and data they need to be productive from any device or location.

Full visibility and actionable insights into data security

The company knew that to meet its high security standards and regulatory compliance, it needed greater visibility of how its data and apps were used. Lookout was able to provide actionable insights across the two SaaS apps all within the same management console. From a single point, its IT team was able to easily identify trends in who was accessing what types of data, which file-sharing permissions were in place, and if links to sensitive data were being shared publicly. With granular information at their fingertips, their security administrators were able to make insightful decisions on what data and compliance policies to put in place.

Prevent leakage of sensitive data

One of the biggest challenges of sharing sensitive data with contractors and service providers is data leakage. Cloud apps present a greater data security risk due to the ease and speed at which users can share data and collaborate with internal and external parties.

The company used the full Google Workspace suite as well as Salesforce and needed to ensure that PII and PHI information did not leave the company unprotected. To protect data within these apps, the IT team established DLP policies to detect social security numbers, date of birth, driver's license numbers, passport numbers, credit card numbers, and bank account information. They also authored unique policies including one to block files containing a maximum number of email addresses and phone numbers from being shared. After defining a comprehensive set of DLP policies, the company used the Lookout console to enforce them across the various apps.

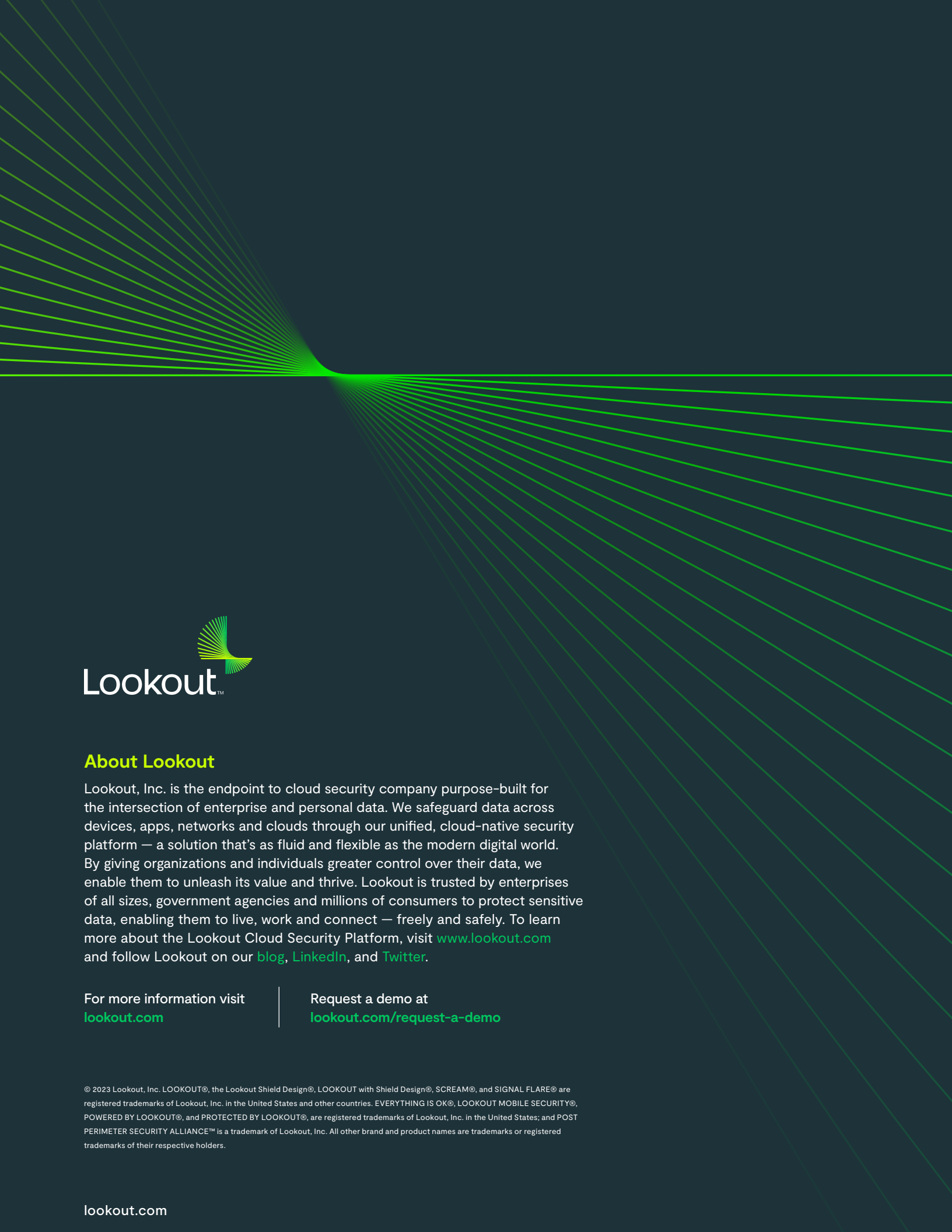
Reduce complexity and administration of IT security

As a business with a reputation for providing stellar disaster recovery services, ensuring operational efficiency of IT support was a priority. The company was initially concerned that adding Lookout Secure Cloud Access could add complexity and cost. Lookout explained how unified policies can be created once and applied across Salesforce and all Google Workspace apps including Gmail, Google Chat, and Google Drive, as well as any other cloud apps they put behind the CASB solution.

To make sure that they properly vetted this product, the company also required third-party validation. Lookout provided a reference customer who vouched that Lookout significantly reduced IT complexity by simplifying management with its unified policy framework.

Continuing the journey to the cloud with Lookout

With Salesforce and Google Workspace adequately secured, the disaster relief company's IT team is ready to extend the platform to other components. Whether it's additional acquisitions or the onboarding of new apps, Lookout Secure Cloud Access and the Lookout Cloud Security Platform, they can efficiently push existing data protection policies to new apps with confidence.



About Lookout

Lookout, Inc. is the endpoint to cloud security company purpose-built for the intersection of enterprise and personal data. We safeguard data across devices, apps, networks and clouds through our unified, cloud-native security platform — a solution that's as fluid and flexible as the modern digital world. By giving organizations and individuals greater control over their data, we enable them to unleash its value and thrive. Lookout is trusted by enterprises of all sizes, government agencies and millions of consumers to protect sensitive data, enabling them to live, work and connect — freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and Twitter.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo