MEETING THE CLOUD COMPLIANCE CHALLENGE: POLICIES ARE KEY

FORCEPOINT

MEETING THE CLOUD COMPLIANCE CHALLENGE: POLICIES ARE KEY

Cloud computing is transforming the way businesses operate. While cloud computing reduces the cost and complexity of owning and operating computers and networks, to reap the benefits of cloud computing, companies inherently give up some control over their data. This is especially true for companies using file storage Software-as-a-Service (SaaS) back-office applications Microsoft Sharepoint and OneDrive, Google Drive, Box, Dropbox and a host of others. However, even though IT teams may not control the endpoint or cloud applications, they are still responsible for protecting their company's information assets and must ensure their cloud applications are compliant with their IT policies.

EXTERNAL AND INTERNAL COMPLIANCE DRIVERS

The word "compliance" has become a catchword that has different meanings and different goals, often dictated by your role in the organization. External compliance requirements focus on following regulations, standards, and laws imposed by external governments, organizations, and industries. Two examples of notable external regulations are the Health Insurance Portability and Accountability Act (HIPAA) that governs how sensitive patient information must be handled, and the Payment Card Industry's PCI DSS standard that governs how organizations must store, process, and handle credit card information. Achieving compliance means that at a given point in time, an audit of your information technology software, processes, and workflows allowed you to conform to a set of rules, such as standards, policies, or laws. External compliance requirements, on their own, do not dictate how information security efforts must be conducted.

In contrast, internal compliance focuses on adhering to the standards and best practices embodied in internal policy and managed through corporate governance. Internal compliance is defined by the organization and focuses on protecting data such as intellectual property, strategic plans, and business records.

The drive to secure corporate data seeks many of the same outcomes as maintaining compliance with internal and external policies. However, security specifically focuses on malicious actors, which requires its own specific strategy. As a result, while the efforts to maintaining compliance and ensuring security overlap, they each require individual treatment and one cannot substitute for the other.

THE CLOUD COMPLIANCE JOURNEY

One of the biggest challenges companies face when establishing a compliance program is identifying where to begin. They realize compliance is about properly managing the interactions of people, data, and critical IP, and that they must adhere to federal and state regulations and laws. Unfortunately, few understand that good policies are the foundation of a successful internal compliance program and that it takes time to develop effective policies. Many also do not realize that the mandates for cloud and on-premises compliance are the same—data is data regardless of where it resides. However, when dealing with SaaS applications in the cloud, companies are not in control of the data environment. This critical factor must be considered when selecting tools to support and enforce compliance and security efforts.

> **It is important for enterprises to use security measures to help achieve compliance vs. relying upon compliance to drive security.**

POLICY CREATION AND ENFORCEMENT: THE FUNDAMENTALS OF A SUCCESSFUL COMPLIANCE PROGRAM

The first step to developing compliance policies is to create classifications for data, users, and applications that define how data, users, and applications can interact. Before classifications can be developed, you must determine the relative value of each asset to the organization.

Data Classifications – Determine the data classifications the organization will allow to be created, manipulated, and stored in the cloud, along with who may access data in each classification and under what circumstances.

- Establish data classifications that map to organizational impact.
- Establish data types that map to functional utilization (e.g., sales reports, intradepartmental collaboration, and marketing artifacts).
- Establish a matrix of classification types and determine eligibility of each element for use in a cloud setting, along with any required safeguards that inform eligibility, e.g., absence of public file sharing.
- Determine authorized users of the data and permissible actions, such as access, delete, and storage constraints by time, day, geography, and device.
- Determine response and remediation to actions inconsistent with policies created.
- Establish safeguards to evaluate and make a final determination of the risk/reward of that data classification residing in the cloud if theft, destruction, or corruption of data in a classification represents risk to maintaining compliance.

People/User Classifications – Determine the organization's user classifications that define the specific acts a user can perform, such as create, share, and modify, on a per data classification basis and under what circumstances.

- Establish group and user classifications that map to authorized data use.
- Establish acceptable usage parameters for each user and data matrix element considering action, (e.g., create and delete), geography, chronology, and device (including device characteristics).
- Determine policy exceptions based on organizational needs such as business travel, specific roles, and individuals.
- Identify user behavior that may indicate either unintentional risky behavior or potentially malicious activity, and determine the triggers and responses that correspond to risk levels using an "If-Then" rubric.

Application Classifications – Establish policy for sanctioned and unsanctioned application use by end users that defines the types of applications to be allowed, (e.g., collaboration, CRM, and Finance), including the application of data policy to determine those within acceptable risk bounds.

- Clearly identify what constitutes a user application in contrast to passive web sites.
- Establish acceptable application risk metrics based on regulatory requirements, industry certifications, and your own internal benchmarks. Pay attention to data manipulation capabilities like sharing, auditing, and change control over actions like deletion.
- Establish acceptable usage parameters for each user application matrix element that considers type of application, geography, chronology, device, and device characteristics.
- Establish acceptable simultaneous use of applications with additional consideration for corporate and personal accounts.
- Establish application approval policies for new applications, including the classes of applications that will NOT require approval.
- Determine response and remediation to actions inconsistent with policies created.

Compliance programs are increasingly becoming critical components of the business landscape, but they can be a significant challenge to establish and maintain. Policies form the cornerstone of an organization's compliance and security program, but developing good policies takes time. Additionally, without clearly defined policies, investments in security and compliance tools cannot be fully leveraged. Invest the time and resources necessary to get policies right or risk the exposure of critical information and the negative consequences of failing a compliance audit.

ABOUT FORCEPOINT

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit www.forcepoint.com and follow us on Twitter at @ForcepointSec.

CONTACT

www.forcepoint.com/contact

[CYBEREDGE-BRIEF-ENUS] 700015.101718