SailPoint

SOLUTION BRIEF

Employing Governance for Risk Mitigation & Compliance

Europe is Not Alone in Facing Data Breaches

It's an all-too-often event that a new data breach of an enterprise is reported, and it's only becoming more frequent. Unauthorised access to data is a prominent issue, with high-profile data breaches such as Think W3 Limited and TalkTalk in the UK. In fact, from a survey of EU IT decision makers, 64% believe attacks on their own companies have increased over the past year.

To only complicate matters, cloud application usage and the rampant use of bring-your-own-device (BYOD) in organisations have made securing data even more difficult and complex. 89% of UK CIOs feel that shadow IT – employees installing and using cloud applications without knowledge or consent from the IT department – and BYOD present a long-term security risk for their company.

As these threats have grown, so too have the standards and rules associated with the security of our data. From the Data Protection Act of 1998 and ISO 27001, there have been countless standards with which organisations have had to comply. Now that the General Data Protection Regulation (GDPR) went into full effect in May 2018, the focus is to help clarify what is expected of a company to best protect itself against a breach, but also give guidance as to what to do when a data breach does occur.

On average, there are over 4 breaches per day in enterprise organisations in the UK.

This law stipulates that organisations will not only have to notify those affected by a data breach within hours of when the breach is detected, but also allow users to request exactly what information was released and give them "the right to be forgotten." These requirements are in addition to possible sanctions, fines – €20m or 4% of an enterprise's annual turnover (whichever is greater) – and, of course, loss of customer trust and negative publicity.

On top of all these requirements, it's widely accepted that the question is no longer if an organisation will be targeted in a data breach effort, but rather when. And even though GDPR mostly focuses on the data an organisation holds, one must remember the identities – the employees, contractors and other persons associated with the company – are who hold the keys to that data. While hardware measures, e.g. firewalls, network monitoring, VPNs, etc., are all important and necessary, implementing a governance-based approach to how you control access to data with the right identity program can help to mitigate the risk from data breaches.

Control Your *Users'* Access with Identity

Your employees are who hold the keys to accessing your protected information, and it is often them who let the hackers and foreign entities into your organisation, either willingly or inadvertently. Understanding who has access to your data and how that access is being used is a question that all organisations must face, solve and control.

Today, 85% of business risk can be tied to just 5% of the user population.

Identity governance can help. The right solution enables organisations to achieve both effectiveness and efficiency in meeting compliance requirements while also combating the question of securing the lifeblood of the enterprise: its data. A solution should take both efforts into account, make it possible to achieve and demonstrate successful compliance with regulatory requirements, and place the right amount of importance on ensuring users have the right access to the right data at the right time.

Protect Yourself from End-to-End

Today, the majority of business risk related to user access can be tied to a very small percentage of the user population. The difficulty usually lies with identifying and then securing against that small percentage. An effective identity governance solution must be able to pinpoint where an organisation is at risk no matter how your applications are deployed and how your identities access the relevant data.

Obtain Visibility into the Entire Organisation

To more effectively manage risk across applications, whether they are on-premises or in the cloud, an organisation's identity governance solution should provide the ability to capture the same type of intelligence on all applications. For example, to comply with separation-of-duty requirements, you must be able to detect when someone who is authorised to issue a purchase order in an on-premises application is requesting to be able to acknowledge receipt of the order in a cloud-based application. After all, if you can't see risk, you can't control it.

Increase Efficiency and Reduce Costs with Automation

By replacing slow, error-prone paper-based and manual compliance processes with automated tools, organisations can exercise more precise, real-time control over identity and access information. With automation, organisations can establish repeatable, predictable processes for compliance and respond more quickly to remediate violations. With this automation, whenever an employee joins, moves positions within or leaves your organisation, their access is automatically modified to fit the particular situation. This automation, in turn, significantly reduces the cost associated with maintaining and proving compliance.

SailPoint is Identity

To best protect the information you hold dear, you need to implement an identity governance solution with the right controls to ensure your data is and stays safe. SailPoint provides an integration solution that offers compliance, lifecycle management, identity governance for files and more, all with a proven approach to ensure compliance.

Continuously Mitigate Risk

By laying the foundation for effective governance across all identity activities, and providing a complete framework for centralising identity data, SailPoint can help organisations establish controls that support all critical compliance processes and ensure users have the right access to the right systems at the right time. Automate policy- and risk-aware access certifications to help implement uncover and prevent access risks and with SailPoint's unique, risk-based approach. With this, you can run more effective certifications and prioritise efforts on those areas of highest risk.

Reduce the Cost of Compliance

SailPoint helps organisations achieve operational efficiency and reduce the costs associated with compliance and risk mitigation. Automating access certification processes to establish repeatable practices enables a more consistent and reliable compliance effort, while also ensuring the access identities have is appropriate. These certifications can also be performed by the business managers, application owners and group owners through a friendly interface, freeing up IT.

Easily Demonstrate Compliance

Demonstrate the presence and effectiveness of controls aimed at achieving and maintaining compliance with dashboards, reports and analytics. Evidence of compliance is delivered in business language that does not require extensive understanding of the underlying technology, making the information easy for both executives and auditors to understand.

Trust in the Market Leader

SailPoint has been recognised as the leader in Gartner's Identity Governance and Administration Magic Quadrant for the past several years, a leader in KuppingerCole's Leadership Compass for Access Governance, Provisioning, and Cloud IAM/IAG, as well as top marks from Forrester Wave and Gartner in their Identity-as-a-Service (IDaaS) categorisations. You can trust in our decade plus years of experience, dedication to innovation in the identity industry, consistently high user satisfaction and proven track record.

Join Other SailPoint Successes

Companies representing a broad range of industries in a variety of locations around the world rely on SailPoint to help them achieve and maintain compliance in an effective and cost-efficient manner.

AXA Belgium

AXA Belgium, a leading financial protection organization, needed to automate their identity processes – access requests for external customers and access management for internal teams.

Working with Adinsec Identity Architects and SailPoint, AXA first focused on securing access with their own corporate customers, ensuring access rights were managed appropriately and then automated to streamline the overall processes to extend to internal users.

Through the power of identity, AXA's corporate customers were able to manage their own access requests – giving them greater control over the process and relieving some of the strain on AXA's operational load. This, in conjunction with an overall streamlined and automated system, helps AXA scale for future growth as they add more users and more applications over time.

**SAILPOINT:
THE POWER
OF IDENTITY™**

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.