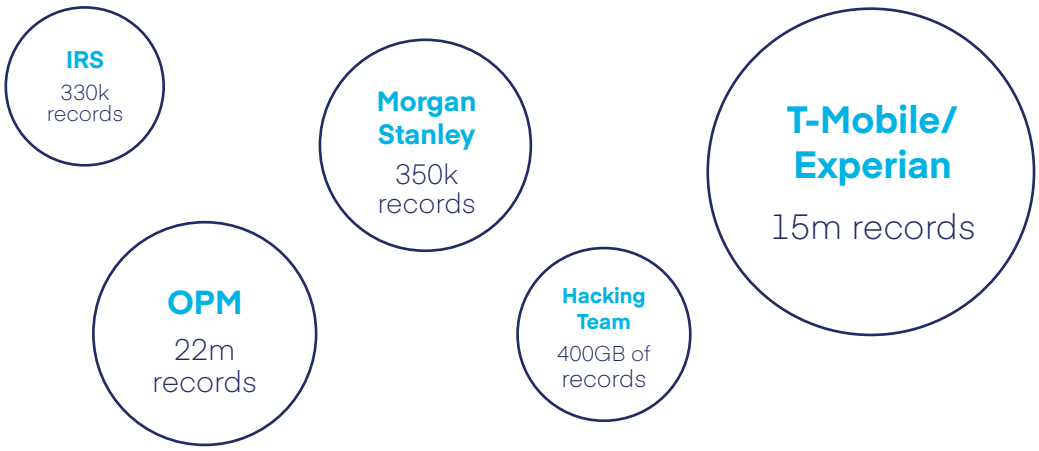
SailPoint

SOLUTION BRIEF

Identity is **Everything**

It seems as if it's every other day that we hear of a data breach. But consider the fact that we hear mostly of the big-name companies – or in the case of Ashley Madison, controversial ones. Imagine just how many we don't hear about. In fact, it's estimated that there are not only a few data breaches every week, but instead there are, on average, more than 4 breaches per day. With both small- and large-name companies in the list, it's an undeniable fact that no company is safe.

In 2015, there were at least 1400 data loss events that were recorded, releasing over 770 million records. From health and financial records to even children's account information, nothing was safe.



The common thread with all these data breaches? Someone inside the company did something they weren't supposed to do.

Exposure Points Have Evolved

It used to be that employees physically traveled to their places of work. Anything they needed done, any applications they needed to use or information they needed to gather or reference, etc. were all performed or handled at the place of business. And so, physical security both for the building and on the network was sufficient as well as fairly straightforward to manage. As hackers became increasingly more skilled at breaking through that perimeter, new technologies were invented and implemented to help secure the enterprise's critical information. Just as we have evolved our thinking about how our employees work and access data, so too have we evolved our protection against threats towards that data.

Technology vulnerabilities, while still important, are now less of a security concern than our own human weaknesses.

But if 2015 has shown us anything, it's that network security is no longer sufficient. The perimeter that once held our information safe has been eradicated. Instead of brute force attacks and SQL injections being the norm, intruders have slowly, but surely begun to favor to social engineering. Phishing emails and other means through which people inadvertently release information are one of the greatest threats to companies today.

A Billion Points of Exposure

Your users' – or identities' – access to the enterprise's systems is multi-tiered, encompassing the basic answer of "who can access" these applications to the more complex "what can be done with that access." Considering the number of identities an enterprise may have across employees, partners and contractors, the multidimensional systems they utilize and the varying levels of access required, it's easy to see how an enterprise would have millions, and in some cases, a billion points of access into their systems.

Every layer of access rights associated with an identity is, in reality, a point of exposure for your organization. Out of those billion points of exposure, it only takes one to be compromised and cost an organization millions in damages. Each point of exposure is tied to an identity. This should imply that the security vector companies need to focus on is the human vector, but it is something they seem to struggle with handling today.

Whether it's intentional or inadvertently, people are who cause a large portion of data breaches, and likewise are responsible for some of the largest breaches we have experienced. And as hackers continue to advance their strategies, more data breaches will occur from someone doing something they weren't supposed to do.

Identity is Everything

With the inevitable occurrence of a data breach, the network perimeter disappearing and the ever-present risk from the human vector, organizations must adapt and secure their best asset and simultaneously their greatest threat: their identities. User identities "hold the keys to the kingdom," and for your organization to be safe, securing those identities is everything.

To do this, putting identity at the core of the organization's security program is essential. Since identities are what are most likely to be targeted, securing them must be the top concern. By focusing on all the systems to which users connect, whether they are on-premises or in the cloud, security can be holistic. Only when IT departments have all the information can they make the right decisions.

The good news is that managing this complex network of users, systems and access is possible for IT departments with the right technologies. Those billion points of exposure are dynamic, constantly changing and extend beyond the physical walls of the enterprise to customers, partners, vendors and contractors. Therefore, organizations require a governance-based identity solution that can holistically and automatically manage identities at granular levels.

By employing a governance-based approach to identity knowing "who has access to what" is possible for all users and the applications to which they have access as they move in the company throughout their lifecycle. By utilizing a user-centric approach and integrating all the systems together (such as data governance, network security, user behavior analysis, etc.) into the identity governance platform, IT would now have visibility into the entire security ecosystem. Only then can the organization truly put identity at the core of its security and protect the information that they need to succeed.

SailPoint is Identity Governance

At SailPoint, we know your sensitive information requires safeguarding from outside – and inside – threats. We provide a solution that offers compliance, lifecycle management, data access governance and more, all with a proven approach to ensure compliance and mitigate risk within your organization.

By laying the foundation for effective governance across all identity activities and providing a complete framework for centralizing identity data, SailPoint can help organizations establish controls that ensure users have the right access to the right systems at the right time.

The SailPoint solution provides a single view of a user and his accounts, entitlements and associated risk across all applications, as well as structured and unstructured resources for "big picture" visibility and control. It also transforms technical identity data scattered across multiple enterprise systems into easily-understood and business-relevant information through intuitive reporting and dashboards. With the SailPoint platform, organizations can more quickly identify risks, spot compliance issues and make the right decisions to strengthen controls.

SailPoint, a Gartner Magic Quadrant Leader, built our business on the foundational principle that identity is everything.

Identity is Everything.
Secure it. Manage it.

Learn more at sailpoint.com/identity

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 in virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.

SB1013-1709