Creating an Identity-aware Organization

from Infrastructure to Users

SailPoint

Today's modern enterprise must compete in a world where agility and innovation are the name of the game. To standup to the challenge, these organizations are finding new ways to leverage technology and automation to not only stay relevant but also differentiate themselves from the rest. Amongst all this transformative and disruptive change are cybercriminals who silently prey on the opportunity and take advantage of a multitude of unmanaged and unsecured resources. In fact, cybercriminals are no longer just hacking through your firewall to gain entry to your infrastructure. They have found another, easier path in – your users.

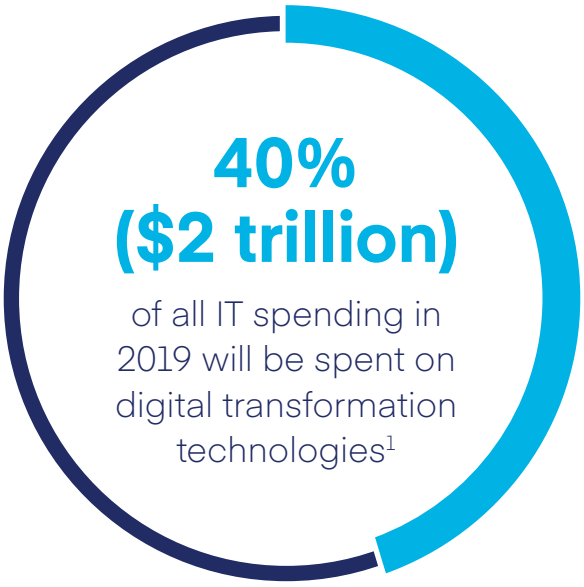
Users Hold the Keys to Your Data

According to McAfee, more than 40% of data loss is caused by insiders or users. However, before you start looking at every employee within your organization as a suspect, it's important to realize "users" also includes contractors, vendors, partners, and even bots – basically anyone or anything who accesses any part of your network. Cybercriminals have found your users are the weakest link and are exploiting that to gain access to your most valuable asset: your data.

Cybercriminals use several techniques to steal your user's credentials including phishing, malware and social engineering. Once obtained, they have all the same access your user has. This access includes data stored within databases, applications and systems as well as data stored in files which can be found strewn about cloud file shares (such as Box or SharePoint) and local file stores like NAS devices. Once accessed, they can encrypt the information for ransomware or exfiltrate it to be sold on the dark web to countless buyers.

In order to address the importance of security within organizations, compliance regulations have been put in place and continue to come online in the effort to hold organizations accountable when it comes to securing sensitive information.

As a result, organizations have had to rethink their approach to security and IT. With many enterprises continuing to use legacy and proprietary systems – while



[1]CIO, *4 Things Successful CIOs Know About Digital Transformation*

also adopting new cloud technologies – securing a complex and hybrid environment that includes a distributed workforce can be seen as a daunting task. However, organizations who are successful at addressing these challenges all have one thing in common: identity.

Identity is the Keystone to Secure Organizations

Identity management is key to ensuring a secure, compliant and efficient infrastructure. Any user or "thing" that has access to your network should be treated as an identity and tightly managed and governed with least privilege access, helping to mitigate the risk of a breach due to compromised credentials or even malicious intent.

When identity is woven within the fabric of your IT and security environment, you can then realize the benefits of an identity-aware infrastructure. This is made possible by an open identity platform that integrates and connects every identity, application, system and file share across your organization so access can be administered from a single pane of glass. This then allows organizations to know at any time:

- Who has access to what?
- Who should have access?
- How is that access being used?

By knowing and managing these key points, organizations can make huge leaps in their security and compliance programs. A successful identity program relies on organizations defining and enforcing access policies that are contextual to their security and compliance requirements. These policies then provide the rules of access for everyday IT activities including:

- Automated provisioning and de-provisioning of access for new/terminating employees and those moving roles
- Request for access to additional applications, systems or file folders
- Catching access violations such as separation-of-duty
- Remediating suspicious access behavior
- Enforcing password management best practices

In addition to enabling IT efficiencies, identity also serves the business by way of enabling a secure self-service environment for users. By automating repetitive tasks that typically require a phone call into the helpdesk, such as a password reset, users can be enabled with a secure and efficient way to reset their own passwords. Requesting access to new applications and file folders at any time can also be streamlined through pre-defined identity-centric workflows that ensure all requests are sent to appropriate business owners for review and approval. This is all done according to policy and fulfilled in a secure and efficient manner while also documenting all activities (requests, approvals/approvers, and action) for compliance and reporting purposes.

When identity is used in this manner, it infuses and extends security down into the DNA of every user and truly enables user-centric security. To the business, this not only means increased productivity and efficiencies, but also huge potential IT cost savings. In one year alone, a SailPoint customer with just under 1,500 users was able to recognize a total savings of $350,000 by simply implementing an identity-driven password management solution.

Finally, as organizations incorporate identity management into the heart of their environment, they will realize the overall benefit identity provides by sharing rich identity context with all the IT and security resources that are part of this identity-aware ecosystem. Identity context includes rich and meaningful information such as the relationships that identity has with other aspects of the organization including resources and people, policies and specific controls that apply to that identity, its current state (e.g. perhaps the user is on sick leave), and a historical log of all activities. By sharing this type of information with other resources such as SIEM and PAM investments, your IT and security teams can make smarter recommendations and decisions around risk assessments for governance controls. In addition, identity context can help highlight and differentiate benign versus risky behavior, allowing security analysts to know where to devote attention.

Wherever you may be on your digital transformation journey, it is never too late to start cultivating an identity-aware organization. Identity can help ensure your hybrid transforming environment is kept secure and compliant, while also incorporating automation and processes that lead to overall efficiency gains and cost savings.

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.

EB1244-1808