onelogin | cisco Cisco Cloudlock

WHITEPAPER

Intelligent Cloud Cybersecurity with IDaaS & CASB

What It Really Takes to Enable Fast and Secure Usage of Cloud Applications

Cloud App Usage Has Exploded, Delivering Both Unprecedented Gains and Risks

The adoption of cloud applications among businesses of all sizes has been dramatic in recent years. Trials of applications like Salesforce, WebEx, and Workday have transitioned to enterprise-wide deployments, and key business applications across all industries are moving to the public cloud, a market that Forrester predicts will reach $93 billion in 2016.

The main cloud computing benefits are well established, and can be easily measured in terms of IT cost and time savings. Beyond those, competitive advantages can be derived from the myriad choices of rapidly evolving cloud-based applications that can be rolled out quickly, without any upfront costs and minimal provisioning time. Essentially, cloud computing allows you to focus on advancing key business activities and objectives with unprecedented speed.

In fact, Gartner's 2016 Planning Guide for Identity and Access Management reports that global buyers of cloud applications continue to cite - besides cost - innovation and agility as the top reasons for adoption. The research company finds that CIOs are focused on using the cloud to establish a modern, innovative IT environment with operational agility and business advantage as key outcomes, confirming the strategic opportunity of using cloud services.

However, there is a flipside to this coin. The overwhelming majority of security breaches of recent years have involved some form of credential loss or theft, resulting in unauthorized access and data breaches. It does not help matters that employees, challenged with the growing number of passwords, resolve to write them down and keep them easily accessible, or use the same weak password version across all instances. Another common phenomena is for collaborators to share app credentials, further heightening the risk of password loss or theft and the resulting financial impact. A recent IBM Study revealed that the average total cost of a data breach in 2015 has increased nearly another 10% to $3.79 million.

Content

Despite Many Concerns, CIOs Continue to Heavily Invest in the Public Cloud

Key drivers besides operational and employee productivity gains also include the fact that "hands off" IT enables redirection of limited in-house staff to more strategic responsibilities, while deferring responsibility for ongoing availability and support to the SaaS provider.

Traditional on-premises identity and access management (IAM) solutions involved in protecting servers and devices as well as a finite number of applications behind corporate firewalls are no longer adequate for protecting SaaS services built for the cloud. They tend to take up large amounts of data-center space, are handicapped by increasingly outdated capabilities, and consume large amounts of energy, not to mention the poor performance and outage issues typical of aging systems.

31% of employees admit to re-using work passwords

– softwareadvice.com Report

Users will always pursue the fastest path to accomplish tasks and, collectively, there has never been a greater wealth of tools, apps and services at our disposal. However, the overhead of managing apps and their secure access has grown into a painful experience for end users in many organizations. Softwareadvice.com reports that "31% of employees admit to re-using work passwords" as a way to cope with access friction. Periodic password resets and minimum complexity policies, as well as incidental lockouts and multi-factor authentication for each app compound the challenges, and shift the user experience from painful to untenable.

The good news is that with growing cloud app adoption, a new form of security and identity solutions leveraging cloud benefits has emerged to address those risks and meet enterprise security requirements for SaaS deployments, playing a critical role to protect business data stored and shared in the cloud. Such IAM and CASB (Cloud Access Security Brokers) solutions protect and secure the hybrid enterprise, focusing on threat protection, cloud malware defense, and forensics across cloud environments by managing all identities that touch corporate data.

Cloud IAM has Emerged to Protect Business Data in the Hybrid Enterprise

There are many reasons why the advantages of SaaS have transcended to IAM. For example, processes such as installation and maintenance become easier, and implementation can be more standardized. This allows IT teams to move away from IAM on-premises deployments at their own pace, and away from IAM instances that are often heavily customized, brittle and difficult to maintain.

At the highest level, Cloud IAM securely enables the right people to have convenient access to the right resources at the right time for

the right reason based on a set of complex software functions that go beyond IT Administration, Security, Operations and Governance, extending to HR, line of business managers and, of course, end users. Cloud IAM offerings are accelerating the evolution of federation.

When a new federation software capability has been developed, it takes significantly less effort on a per-customer basis to add the new feature to an existing hosted service and roll it out to all users in one single swoop. This means that the innovation wave that created Cloud IAM has a great side effect of reducing the cost of additional innovation and accelerating the integration with many different SaaS applications.

Leading Cloud IAM solutions also eliminate the risk of password loss and theft in a couple of powerful ways. They integrate with applications and use certificate-based authentication, removing the need for users to submit passwords for each individual app. Instead, once authenticated to their IAM system, they are automatically and securely authenticated to all their applications via Single Sign-On (SSO), designed to delivers secure authentication across applications with one set of credentials. Advanced Cloud IAM solutions support multi-factor authentication to protect apps and information with an added level of security where an unauthorized person who managed to obtained a correct username and password will still need to provide a second, separate authentication. Beyond that, Cloud IAM serves as a control point giving organizations the ability to revoke access for employees moving to different roles in an automated manner, as well as turning access off for departing users in real time.

Unfortunately, most approaches to identity management force enterprises to make a choice between integrity and business velocity. Enter OneLogin: a new class of identity management solution built for the high speed, well-governed business. OneLogin received highest scores in the latest Forrester's Cloud IAM Wave™ as a cloud-based solution that enables IT to execute identity policies across all users and devices, as well as cloud and on-premisess applications. OneLogin's cloud-based Single Sign-On (SSO) functionality gives users one central place to access all apps. Upon logging in via their organization's dedicated OneLogin subdomain, users are authenticated to all of their apps automatically, which they can then simply click through and start using. In addition, organizations can leverage OneLogin to set up Desktop SSO, whereby users are authenticated using their desktop credentials. In this case, users simply log in to their computer which in turn authenticates them against their Active Directory, LDAP, or OneLogin directory service.

OneLogin received highest scores in the latest Forrester's Cloud IAM Wave™ as a cloud-based solution that enables IT to execute identity policies across all users and devices, as well as cloud and on-premise applications.

Best-in-Class Cloud IAM and CASB Solutions Secure Cloud- and On-Prem Data in the Hybrid Enterprise

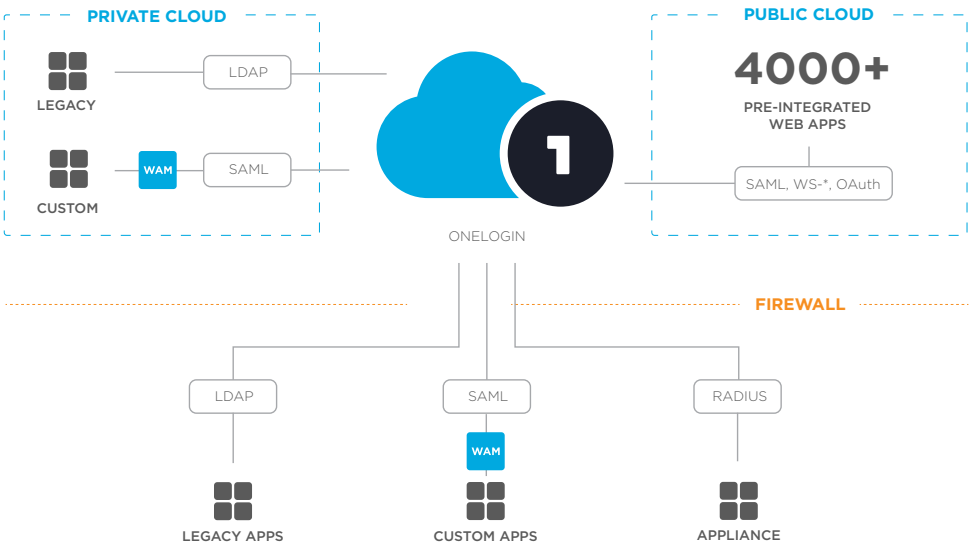
With the instant collaboration and powerful data management capabilities offered by the cloud, it's no surprise that a rapidly growing portion of data is moving off premises. An increasing number of enterprises are adopting a cloud-first strategy, and Cloud IAM is becoming increasingly popular to protect their business data. Other businesses are migrating to the cloud at their own pace, pursuing hybrid strategies with some data living on premises, and other data living in the cloud.

There are many reasons an organization may keep certain data on-premises. Some face data security and compliance regulations that require strict data residency compliance. Others depend on legacy applications and on-premises security solutions for which they want to protect their legacy investment. For example, many organizations keep their employee user directory on-premises. For larger organizations, a hybrid strategy is often, at least initially, the best approach.

There is a clear trend that leading IT and security and risk (S&R) professionals are embracing Cloud IAM as a crucial components for improving their organizational security posture. In its 2016 Planning Guide for Identity and Access Management, Gartner recommends to embrace Cloud IAM, and suggests to prepare the move of core IAM functions to the cloud to support critical use cases for workforce access to both SaaS and on-premises applications.

An increasing number of enterprises are adopting a cloud-first strategy, and Cloud IAM is becoming increasingly popular to protect their business data.

SECURE HYBRID ENTERPRISE



Garrett Bekker, senior security analyst at 451 Research, stated in a recent OneLogin press release that "Cloud-focused IAM providers are under increasing pressure to deliver a unified and secure way to ensure compliance across all of an enterprise's technology investments, both cloud and on-premises. OneLogin's melding of cloud with legacy and on-premises solutions can help provide greater security and compliance for the many firms that are pursuing a hybrid cloud strategy."

Pre-integrated with thousands of enterprise SaaS applications and commonly used web applications, OneLogin is simple to deploy and easy to administer, dramatically reducing the time to on-/off-board employees while reducing the risk associated with bad password hygiene. As a comprehensive identity solution for hybrid environments, OneLogin easily integrates into heterogenous web environments to manage all identities that touch corporate data, across all users, apps and devices. In addition to OneLogin's existing support for federation through SAML & WS-Trust, OneLogin's new LDAP service allows enterprises to connect to OneLogin's cloud directory via LDAP.

"OneLogin's melding of cloud with legacy and on-premises solutions can help provide greater security and compliance for the many firms that are pursuing a hybrid cloud strategy."

– Garrett Bekker, senior security analyst at 451 Research

CASB Expands Control over Account Compromises, Cloud-Native Malware, and Data Breaches

The growing number of data breaches directly related to applications and users moving to cloud-based services has made it painfully obvious that enterprise controls for managing policies and access to cloud services need to extend beyond identity and access management. As such, they have spawned an additional class of security products analyst firm Gartner refers to as the Cloud Access Security Broker (CASB) market, and Forrester describes as Cloud Access Security Intelligence (CASI) solutions.

The effectiveness of CASBs depends on their ability to deliver security visibility, threat prevention, data protection and regulatory compliance for cloud adopters, all while maintaining the core functionality and effectiveness of the cloud service platforms in use across organizations.

In many cases, CASB solutions are used to help expose so-called "Shadow IT" operations. As enterprises pursue innovation and growth, they prioritize capabilities that enhance operations in support of customer value, enable accelerated innovation, and increase overall business agility. In practical terms, this means more and more enterprises source solutions from cloud providers — with or without the knowledge of security teams, making their job even more complex. Not only are they often in the dark about what sensitive data may have been stored in the cloud, they don't even know in which cloud applications the sensitive data resides and what users, organizations, or other applications such data may be connected to.

With breaches and other security incidents taking place in increasing numbers across businesses of all sizes, S&R professionals need, as part of their investigative work, access to forensic information on how users and programs accessed the web interface or APIs of SaaS applications, and what exactly they looked at or downloaded. But cloud providers are hesitant to make their application logs available due to data privacy and workload separation concerns.

A highly extensible CASB solution can offer unparalleled levels of insight due to its ability to correlate security events across formerly disparate data streams, allowing organizations to detect risky incidents that would otherwise slip through the cracks. For instance, imagine a CASB that detects an unusual volume of file downloads from a SaaS application, instantly turns off user access and triggers your Cloud IAM solution to require multi-factor authentication for the associated identity to log in again. Ultimately, this type of heightened integration can enable a substantially more secure enterprise no matter where your data resides.

Cisco Cloudlock, a leading CASB platform, defends against compromised accounts with cross-platform User and Entity Behavior Analytics (UEBA) for SaaS, IaaS, PaaS, and IDaaS environments, and uses advanced machine learning to detect anomalies in account usage based on factors such as activities outside of whitelisted countries and actions across distances in an impossible amount of time.

Cloud-native malware - malicious cloud applications connected to corporate systems - has emerged as a new cyber threat in recent years. Differentiating between benign and malicious connected cloud applications can be a challenge for security teams, as organizations have, on average, over 540 unique cloud applications connected to corporate systems, as reported in Cisco Cloudlock's Cybersecurity Report, The 1% Who Can Take Down Your Organization. To combat cloud-native malware, Cisco Cloudlock discovers and controls cloud apps connected to the corporate environment, and provides the largest crowd-sourced security solution to identify individual app risk, using its Community Trust Rating. Cisco Cloudlock is the only company to have discovered over 100,000 unique connected cloud applications.

The Integration of OneLogin & Cisco Cloudlock Delivers a Powerful Solution Set

Hybrid cloud organizations inevitably have hybrid security needs that are best addressed with a full, unified view of all their security instances across both cloud and on-premises environments. The integration of OneLogin's Cloud IAM solution with Cisco Cloudlock's CASB offering solves the top security use cases to protect the secure hybrid enterprise. The innovative integration provides threat protection, cloud malware defense, and forensics across cloud

The integration of OneLogin's Cloud IAM solution with Cisco CloudLock's CASB offering solves the top security use cases to protect the secure hybrid enterprise.

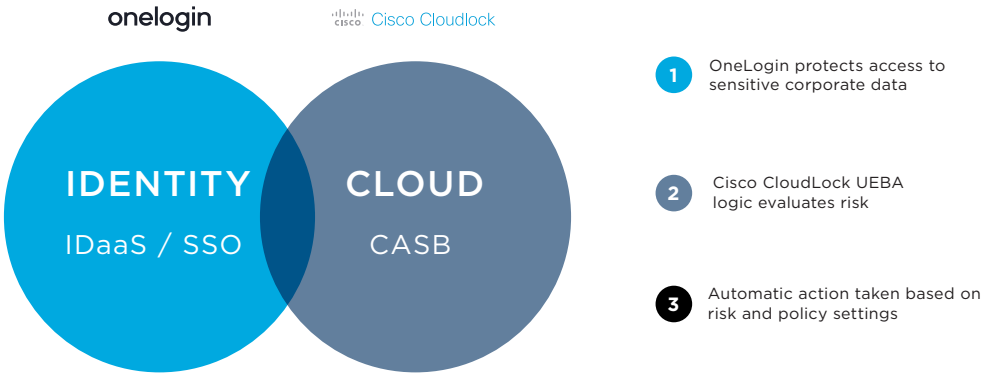
environments by managing all identities that touch corporate data, and protects organizations from threats and cloud malware across users, accounts and applications.

Information and access management data combined with unparalleled levels of insight due to the ability to correlate security events across formerly disparate data streams now allows organizations to detect events that seem innocuous in isolation, but with context are risky. Cisco Cloudlock's UEBA, acting in an orchestration role between event feeds from OneLogin and SaaS applications, utilizes advanced machine learning techniques to dynamically classify the riskiness level of user behavior. This classification level is shared with OneLogin for purposes of automatically stepping up or stepping down the security policy of the user in real time. For instance, when Cisco Cloudlock detects suspicious activities by a user (say login from a previously unknown location or access to sensitive records within a SaaS application), it will tell OneLogin "this user is now classified as risky". In turn, OneLogin can apply a new security policy to 'step up' the security policy of the user in real time perhaps requiring more frequent MFA challenges. Later, once the account exhibits more normal activity, the user's risk rating can be reduced again and the OneLogin security policy stepped down.

Cisco Cloudlock's UEBA, acting in an orchestration role between event feeds from OneLogin and SaaS applications, utilizes advanced machine learning techniques to dynamically classify the riskiness level of user behavior.

This integration allows OneLogin administrations to configure risk-appropriate security policies for their organization based on settings such as frequency of MFA challenges, password strength, password expiration, etc. without being concerned that the assignment of users to these policies is static and thus will eventually become stale. For instance, consider an organization that wishes to enforce MFA only when a user is off site. Thanks to Cisco Cloudlock's UEBA capability, the users will automatically be classified, simplifying the administrator's work and providing users with a better experience.

THE CISCO CLOUDLOCK CYBERSECURITY ORCHESTRATOR™



The integrated solution delivers the best of both worlds, with the ability to deploy new apps and on-/off-board employees within seconds to optimize productivity, while access changes propagated in real-time to all end-points instantly update all systems across the entire app portfolio to keep enterprise data secure. This reduces risk through automated response actions, such as password reset when Cisco Cloudlock detects potential account compromises, and OneLogin mitigates the risk by providing instant lock-down and notifications of identity changes and breaches.

In addition to the full integration of Cisco Cloudlock and OneLogin, Cisco Cloudlock can be accessed through OneLogin's IDaaS solution via SAML integration, enabling security professionals to easily manage user access through the OneLogin Admin Console.

Businesses must find a reliable way to mitigate the challenges, while taking advantage of the agility and power cloud apps offer.

Conclusion

Businesses are engaged in an exciting era of technological advancement. As cloud technology continues to evolve, more and more apps are becoming available that dramatically alter the way corporations create value. Yet, with all the advancements the cloud has introduced, tremendous security risks, complex IT structures, and frustrations with user experiences abound. Businesses must find a reliable way to mitigate the challenges, while taking advantage of the agility and power cloud apps offer.

It used to be a formidable challenge to protect and manage access as well as detect intruders across SaaS applications as they attempt to get to sensitive data. Traditional security information management (SIM) and IAM tools with static policies and rules can only meet these requirements when armies of practitioners are managing a myriad of rules, which is not only expensive but also prone for error and lacking the agility to respond to new and emerging threats.

By leveraging the tight integration of OneLogin's Cloud IAM solution with Cisco Cloudlock's CASB offering, businesses can gain a new level of control and insight over their cloud app activities and protect their intellectual property while delighting their IT organizations and end-users alike.

To learn more about how OneLogin's IAM solution can help your business manage challenges within the cloud, visit onelogin.com.

To learn more about how Cisco Cloudlock can enable your enterprise to protect data in the cloud, reduce risk, achieve compliance, manage threats and increase productivity, visit cloudlock.com.

About OneLogin, Inc.

OneLogin brings speed and integrity to the modern enterprise with an award-winning SSO and identity-management platform. Our portfolio of solutions secure connections across all users, all devices, and every application, helping enterprises drive new levels of business integrity and operational velocity across their entire app portfolios. The choice for innovators of all sizes such as Condé Nast, Pinterest and Steelcase, OneLogin manages and secures millions of identities across more than 200 countries around the globe. We are headquartered in San Francisco, California. For more information, log on to www.onelogin.com, Facebook, Twitter, or LinkedIn.

About Cisco CloudLock

Cisco Cloudlock is the leading CASB and Cybersecurity-as-a-Service solution, enabling enterprises to protect their data in the cloud, reduce risk, achieve compliance, manage threats and increase productivity by continuously monitoring and protecting more than one billion files for more than 10 million end users daily. Cisco Cloudlock delivers the only complete, risk-appropriate and people centric approach to cloud cybersecurity. Learn more at cloudlock.com.