SailPoint

WHITE PAPER

Delivering Innovative **Security in the Cloud**

In today's modern enterprise, security and identity management are inextricably linked. For security teams, identity management provides a critical foundation for basic security practices. For identity teams, security is a critical element to ensuring the integrity of those valuable identities. Adoption of cloud-based enterprise solutions has changed the dynamics of both security and identity management, and enterprises must consider both when looking to move to the cloud.

SailPoint is an innovator in identity management, providing enterprise-class identity governance by delivering and managing user access to applications and systems that reside on-premises or in the cloud. IdentityNow is SailPoint's multitenant cloud-based identity governance solution that delivers a unified platform for access certification, provisioning and password management.

This paper provides a technical view into the security of IdentityNow and how SailPoint has taken an innovative approach to securing identity governance from the cloud.

Identity in the Cloud

In order to effectively understand how SailPoint ensures the integrity of identities in the cloud, it's important to understand why the problem exists.

Today's global workforce is a complex, distributed network of workers: employees, contractors, suppliers, partners and more. The different access requirements and the interconnectedness needed to keep this workforce productive has created a complex stew of security risks. More user information is exposed to the Internet – data that is extremely valuable to attackers – putting extreme pressure on IT organizations to maintain data security and privacy.

From an identity management perspective, usernames and passwords are often weak points where organizations are compromised. To protect data and ensure privacy, enterprise organizations require vendors – especially cloud vendors – to provide a multi-layered approach to security.

The risk of credential exposure begins when a user's accounts are initially provisioned, and continues through any further account actions such as password updates and access certifications. Sensitive personal data may also be a potential target, and securing this information both while in motion and at rest is critical. To address these risks, organizations must seek an identity management solution that protects against all avenues of attack, including the transmission of credentials and sensitive data as well as the security of the identity platform, development and operational processes and personnel training.

Enabling Enterprise-Grade Product Security

With so much data being accessed and shared outside the corporate walls, it's clear that the traditional methods for securing credentials and sensitive data are not sufficient. SailPoint designed IdentityNow from the ground up to address the core challenges presented by transmitting this valuable data in the cloud. Whenever sensitive data is in motion or at rest, IdentityNow employs at least two layers of encryption. These two layers of encryption will always be different types so that if either layer is compromised, the other cannot be compromised in the same way.

Secure Administrative Credentials

One key area where SailPoint has focused in its cloud identity offering is to secure administrative credentials that are needed for provisioning, password management and many other administrative tasks. Many vendors typically protect sensitive data in motion with only HTTPS or SSL. As vulnerabilities such as the Heartbleed bug of 2012 exposed, relying on a single layer of encryption is far too risky.

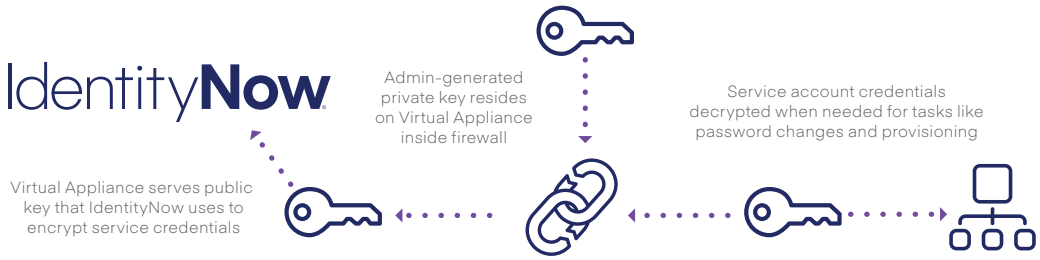

Figure 1: Securing Service Account Credentials with the SailPoint Virtual Appliance

Zero Knowledge Encryption – a first-of-its-kind SailPoint innovation – is used to protect administrative access and interaction with external systems for any actions where IdentityNow must use administrative credentials in order to accomplish an automated task.

Zero Knowledge Encryption secures credentials in a way that separates the key from encrypted data so that even SailPoint cannot decrypt customers' data. SailPoint, quite literally, maintains zero knowledge of the credentials, ensuring complete security.

Zero Knowledge Encryption is deployed via SailPoint Virtual Appliance: a secure, scalable and redundant interface to both on-premises and cloud resources. Virtual appliances are deployed in clusters, and each may contain multiple, redundant virtual appliances. The first virtual appliance in a cluster generates an RSA 2048-bit encryption key which is unique to that cluster. Additional virtual appliances in each cluster add redundancy and load-balancing capacity. Each cluster may have its own unique user-assigned passphrase, and multiple clusters may be deployed to meet the distributed needs of an organization's particular security model, such as deploying a cluster within each datacenter or geography in order to keep security zones compartmentalized.

The virtual appliance cluster runs inside the firewall and requires no ports to be opened. The company administrator specifies a passphrase (known only to them) which is used to generate a 2048-bit RSA public/private key pair that is used by the virtual appliance to secure administrative communications. All encryption uses a key that is created and maintained within the security perimeter, keeping the organization's intrusion prevention and firewall enforcement policies intact. The key is then managed and rotated according to the user's security policy.

Secure Password Management

Passwords are a time-honored cornerstone of computing security, but can often be a key vulnerability. While good password policies, education and enforcement can help make passwords themselves more effective, the tools used to facilitate password management may introduce additional attack surfaces. This issue becomes even more complex as today's workforce is increasingly more mobile and password management solutions are becoming an integral part of these diverse enterprises. SailPoint designed IdentityNow's password management service to have a security infrastructure strong enough to ensure that credentials are never exposed to attackers.

When the user updates their password on a given target system, IdentityNow secures this transaction in order to prevent an attacker from intercepting the new password when it is in motion. Once again, IdentityNow implements Zero Knowledge Encryption to complete the password update without putting the credentials at risk.

IdentityNow also uses Zero Knowledge Encryption to secure the sensitive administrative credentials that may be required to update the password, just as it does for any administrative action such as provisioning.

Authentication

Authentication is a critical element for protecting access to applications and systems. IdentityNow uses highly-secure mechanisms for authentication. As with other critical services, SailPoint uses Zero Knowledge Encryption along with multiple layers of encryption for direct authentication into IdentityNow. Additionally, an extensive range of read-write direct connectors allow integration with trusted authentication technologies that may already be in place.

IdentityNow administrators use Identity Profiles to define populations of users, such as employees or contractors. Each Identity Profile can be configured to utilize either direct IdentityNow authentication, or to use pass-through authentication with one of the sources of data that is connected to IdentityNow.

Additionally, IdentityNow can be integrated with single sign-on tools, which adds the ability to authenticate into IdentityNow using Federation via the SAML protocol. This authentication method has proven extremely difficult to hack.

Direct IdentityNow Authentication

SHA-256 is a 256-bit (32-byte) implementation of the Secure Hash Algorithm (SHA). This is a cryptographic hash function, which is like a signature for text or other data. The SHA-256 algorithm is a one-way function that generates fixed-size 256-bit hash that cannot be decrypted back to the original data, which makes it ideal for password encryption. SHA-256 is one of the strongest cryptographic hash functions available.

When a new user in an Identity Profile that has been configured for direct IdentityNow authentication creates their password, a SHA-256 hash is created. This creates an ultra-secure cryptographic representation of the password that is sent to IdentityNow over a secure TLS connection, giving two layers of encryption. Since the SHA-256 algorithm is a one-way cryptographic hash, the plain text password cannot be recovered from the hash value, even by SailPoint. At no time does SailPoint know or store the user's password.

Whenever the user signs in to IdentityNow on subsequent logins, the actual password is never used. Instead, this cryptographic hash is generated each time the user signs in and the user is authenticated into IdentityNow based on the hash value. Additionally, if they require strong authentication in order to access a protected resource or for administrative access, the answers to the security questions are provided in a one-way hash. All of this is sent over TLS, giving at least two layers of encryption at all times.

Pass-Through Authentication

Pass-through authentication enables administrators to retain control over users' sign-in to IdentityNow in the same way they have traditionally done so: by controlling the directory.

Other solutions may introduce security risk by requiring installation of agents on LDAP or Microsoft Active Directory servers in order to allow this kind of integrated authentication. Agents impose limits on scalability, and do not provide redundancy or high fault tolerance. Some other solutions even require ports to be opened in the firewall to allow communication. IdentityNow keeps the internal systems secure by using the virtual appliance.

When a new user whose Identity Profile is configured to use pass-through authentication creates their password, IdentityNow uses Zero Knowledge Encryption to encrypt the new password. The new password is encrypted in the browser using the 2048-bit RSA public key that is hosted by the virtual appliance. Once within the company's firewall, the virtual appliance then derives the password using the customer-managed private key, and sets the password on the target system. SailPoint never knows this password, and cannot access or decrypt it.

When the user signs in to IdentityNow in the future, this 2048-bit encrypted representation of the password is sent to the SailPoint Virtual Appliance within the customer's firewall, where the target system password is derived. The target authentication system must then validate the user's credentials. IdentityNow will allow the user to log in only if they are authenticated successfully by the target authentication system.

All of this communication between the browser and IdentityNow is conducted over TLS connections – a second layer of encryption in addition to the 2048-bit RSA encrypting the password.

Strong Authentication

Strong authentication enables administrators to offer additional security for more sensitive resources, reducing the risk of unauthorized access based on trusted geographies or networks. IdentityNow can require strong authentication for extra assurance over self-service password management, administrative access to IdentityNow, access to higher risk applications and access to IdentityNow from untrusted geographies or networks.

Strong authentication can also be used to provide different populations of users with appropriate levels of additional scrutiny in order to allow basic access to IdentityNow. Multiple strong authentication mechanisms are used in IdentityNow to ensure users are who they say they are, all of which may be fine-tuned for each organization's authentication policies.

A popular method of strong authentication that is included in IdentityNow is knowledge-based authentication, where the user is prompted to answer security questions to verify their identity.

Since the answers to these security questions can be used to take actions such as changing passwords or access to higher-risk applications, these answers themselves constitute sensitive data that needs to be secured. SailPoint has addressed the need to secure the knowledge-based authentication information with the same rigor as is applied to passwords and other credentials.

When an IdentityNow user sets their answers to the administrator-defined security questions, the answers are then encrypted into a one-way hash, using a salt that includes a random string constant and the user's UUID.

This makes the user's answers extremely difficult to hack. IdentityNow also includes options for multi-factor authentication. The IdentityNow administrator can configure which methods of multi-factor authentication are to be supported, including a growing list of trusted third-party integrations, such as Duo Security and RSA SecurID.

Federation Using SAML

Often when addressing a broad identity management project, organizations will choose an identity provider to assist with access management; specifically, single sign-on. When IdentityNow is integrated with such a tool, users who have authenticated into the identity provider will be able to sign into IdentityNow using federation.

Federation provides authentication without requiring the user to ever enter a password into IdentityNow. Authentication methods using Federation for authentication have proven to be extremely difficult to hack. Security Assertion Markup Language (SAML) is an open standard data format that allows exchanging authentication and authorization data between trusted parties. SAML allows federated authentication, where IdentityNow trusts the identity provider to perform authentication. When IdentityNow uses Federation for authentication, a trust relationship is established between the IdentityNow and the identity provider. Users who are securely logged in to the identity provider can access IdentityNow directly without the need for passwords.

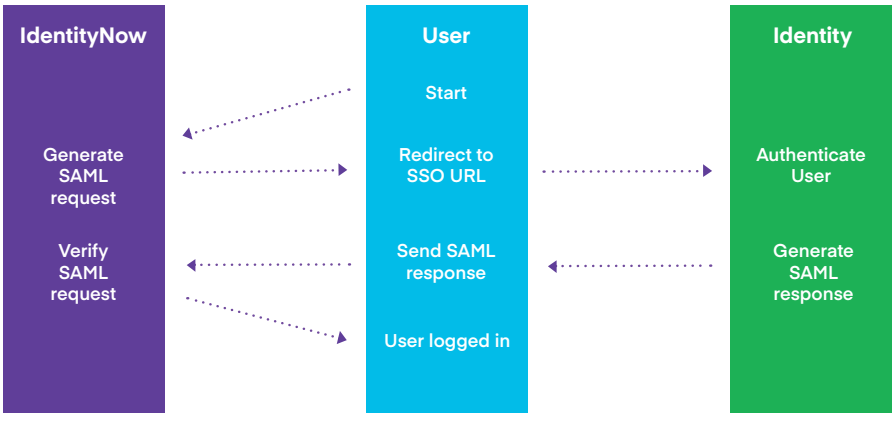

Figure 2: SAML

IdentityNow Platform Security

SailPoint not only developed IdentityNow to mitigate certain risks inherent to other solutions, it also deploys it with a highly-secure cloud infrastructure. Each element of the platform is carefully crafted to deliver the most secure service possible.

Cloud Architecture

The IdentityNow service is hosted on Amazon Web Services (AWS) cloud platform, which provides substantial protection for the base infrastructure[1], and this includes the virtual servers, data storage, databases, network, and other resources. SailPoint DevOps adds additional layers of security to this infrastructure security baseline, including monitoring and alerting, privileged user controls, and other tightly audited processes. These processes are audited annually in a SOC 2 Type 2 audit.

IdentityNow Information Security Assessments

SailPoint completed two information security assessments for its IdentityNow product line. These standards evaluate development practices and the treatment of confidential information within the product. The two assessments include:

ISO/IEC 27001:2013
An internationally recognized security standard, specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

The SOC 2 Type 2 attestation
As established by the American Institute of Certified Public Accountants (AICPA), provides detailed information and assurance about the controls at a service organization relevant to the Trust Services Principles of security, availability, and confidentiality of the information processed by its systems.

With the completion of these assessments, SailPoint customers can be confident in the integrity, security and reliability of the IdentityNow service.

[1]Amazon's security can be reviewed in their white paper: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

IdentityNow's web application uses HTTPS, which employs Hypertext Transfer Protocol on top of a security layer of TLS. All communication between the browser and the IdentityNow server is conducted over HTTPS. Use of HTTPS provides both a layer of encryption, as well as ensuring the authenticity of the server throughout the session. This means that all sensitive data are protected in transit against forged content, rogue servers, tampering or eavesdropping.

Web Application Attack Prevention

IdentityNow employs various industry-standard and specialized techniques to prevent the range of web application attacks that it may encounter. Every HTTPS request that can potentially modify data on the server, such as a POST, has to include a cross-site request forgery (CSRF) protection header. In addition, a one-time use random number, known as a cryptographic nonce, is created for each request that must be validated by the server in order to further prevent against CSRF attacks.

IdentityNow takes extensive measures that prevent cross-site scripting (XSS) attacks. For example, IdentityNow will not allow JavaScript to be loaded from any domain except the preconfigured domains that SailPoint controls and in-application notification tools employed by SailPoint. Additionally, IdentityNow will reject any XMLHttpRequest (XHR) that was produced as a result of an XSS injection.

And, IdentityNow requires the browser to inform the server if any attempt to violate these security policies has been made, even though such an attack will have failed.

Transport Layer Security (TLS) is a protocol that provides privacy and ensures data integrity between a web browser and the server to which it is connecting. Data sent over TLS is encrypted using secure certificates and a combination of public and private keys, providing a base layer of internetworking security that is completely transparent to the user.

The Hypertext Transfer Protocol (HTTP) used in conjunction with TLS is known as HTTPS. This protocol is widely used on the internet to ensure authentication of a website and to protect the privacy and integrity of the data exchanged with it.

In the TLS exchange of initial data handshake, the web server sends its signed certificate, and the browser uses this certificate to verify that the browser is interacting with an authentic server rather than a rogue or unauthorized server. Encryption keys are exchanged and used for the duration of the session to encrypt all communications between the browser and the web server.

Customer Data Privacy & Security

With a cloud service that stores data and interacts on behalf of a number of customers, it is critical to ensure that each customer's data is secure and that it can only be accessed by the authorized customer. IdentityNow authenticates each user only within the scope of their instance of IdentityNow, and only users authenticated to that scope can access any data for their instance. This user-scope authentication is validated on each and every API call that is made, whether from the IdentityNow web application or the SailPoint mobile application. As an added measure, all inputs to the server are validated on the server to ensure they are well-formed.

Additionally, it is important to be able to define and limit what data might be stored in the cloud in the first place. IdentityNow allows administrators to fine-tune the account and identity attributes, as well as other user data that is stored in the cloud independently for each source that is connected to IdentityNow. This ensures that only the data the customer identifies as necessary is ever stored in the cloud by IdentityNow.

Process Security

Security is achieved through more than just product architecture and good platform standards. In order to build a truly secure solution, vendors should also practice stringent controls when putting the product together – especially in the cloud, where products are updated at a much more rapid pace.

Secure Development Standards

SailPoint developers must participate in ongoing security training, including instruction on how to develop secure code, and all code requires a sign-off before it is committed. IdentityNow code is kept secure by using an industry-standard cloud code repository that requires all users to be authenticated into SailPoint's organization. It also utilizes access-level restriction based on each user's department or role. For example, developers with commit privileges cannot access production resources, and developers with production access cannot modify or commit source code.

The IdentityNow build infrastructure is hosted locally within SailPoint's datacenter and is securely firewalled against any intrusion. Access to this build infrastructure also requires secure authentication into the SailPoint organization. To further ensure that the build and deployment process cannot be compromised, any deployment into a production environment requires director-level approval.

Additionally, IdentityNow source code does not contain any information that can be used to reverse-engineer or decrypt encrypted sensitive user data. SailPoint's Zero Knowledge Encryption assures that the key to decrypt customer data is never known to SailPoint, and that no other security keys used within the platform for non-user data are ever committed into the source code repository.

Penetration & Security Testing

SailPoint conducts regular third-party penetration testing on IdentityNow to ensure the continued security of the platform. This suite of testing evaluates all parts of the platform for an exhaustive range of vulnerabilities. These tests effectively gauge resiliency of IdentityNow in response to various attacks that may be launched against both authenticated and unauthenticated surfaces.

IdentityNow is routinely tested to a level that includes an exhaustive evaluation of all vulnerability classes. The third-party security firm who conducts the testing is given unlimited access to IdentityNow so they may fully analyze the application and resources, as well as create the range of exploits that can fully test its resiliency.

The results of these tests are used to further enhance and refine SailPoint's development practices and improve the security of IdentityNow.

Platform Security Practices

The IdentityNow platform deployment team employs a variety of tools that make it possible to fully audit and track all security-impacting actions on the IdentityNow service. A full audit log of all AWS infrastructure actions is automatically created any time these actions are taken. Additionally, all commands that run on a command line interface are recorded and stored in this audit log. The audit log is stored in a secure offsite location and cannot be deleted, edited or changed by any SailPoint personnel.

In addition to logging, alerts are generated for security-related events, and development operations personnel are notified of these events in real time.

Only critical personnel have access to IdentityNow production environments, and access is even blocked at the network layer to ensure only the authorized personnel can gain access to any sensitive data.

Personnel

In order to ensure IdentityNow remains secure, both now and in the future, SailPoint employees complete online computer-based security awareness training annually. Additional training is provided at the departmental level as appropriate for each role. All members of the engineering team are provided education about developing and testing secure applications including the Open Web Application Security Project (OWASP) Guide to Building Secure Web Applications and Web Services, the most current documents from the OWASP Top Ten Project, Essential Skills for Secure Programmers Using Java/JavaEE from the Secure Programming Council and SANS' Top 25 Programming Errors.

Conclusion

To optimize the benefits of moving to the cloud, the modern enterprise requires an in-depth approach to enterprise security. Visibility and controls over users, applications and data along with the relationships between them make identity management pivotal for enterprise security. Organizations should seek an identity management solution that provides robust functionality and advanced protection against all avenues of attack. SailPoint IdentityNow provides innovative, enterprise-grade security through a comprehensive set of processes and technologies that span hiring and training, software architecture and development, operations, and the underlying cloud infrastructure. SailPoint's commitment to innovation and security is evident in IdentityNow today and will be tomorrow as we invest in identity governance to secure the enterprise.

WP1185-1807