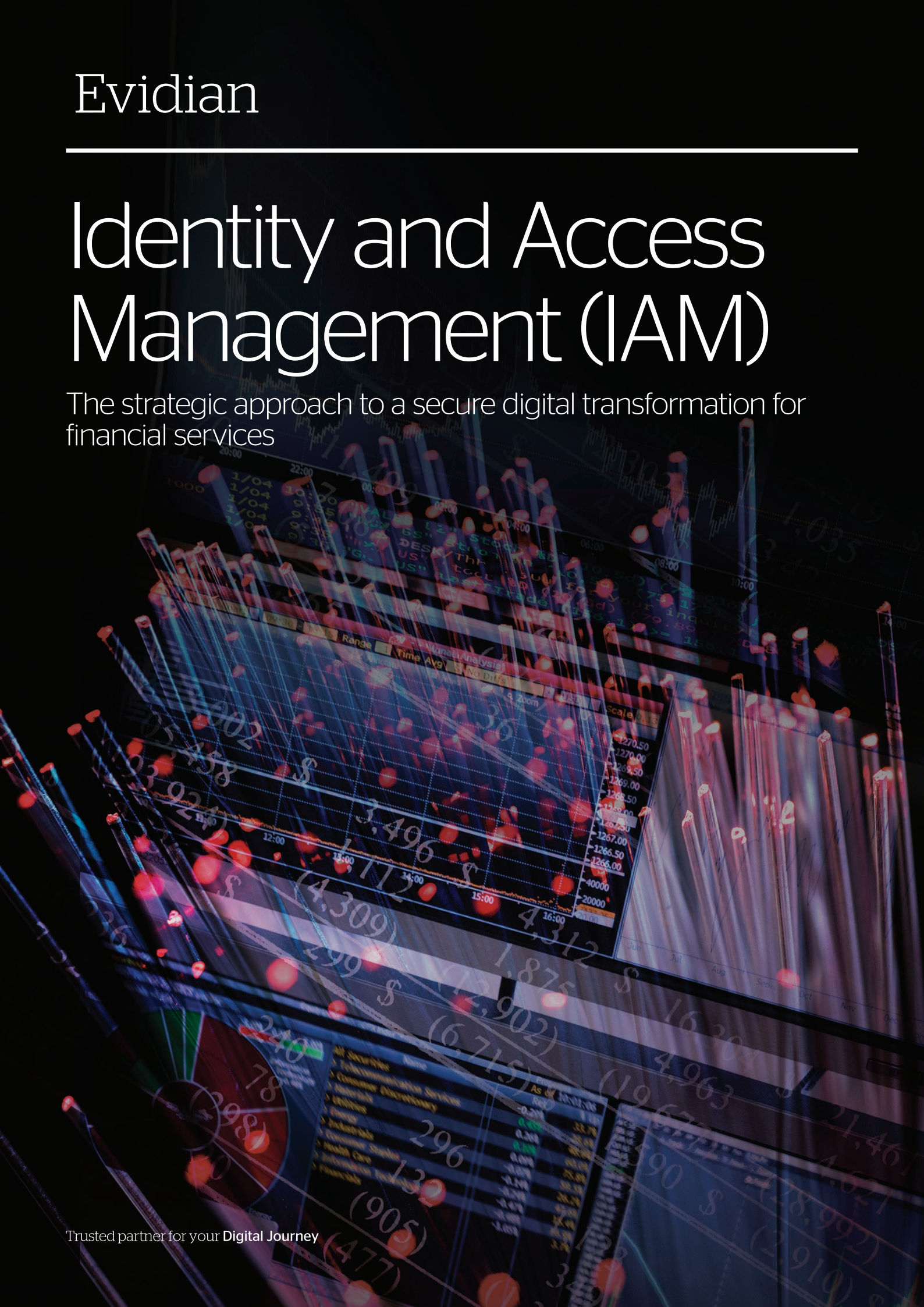
Evidian

Identity and Access Management (IAM)

The strategic approach to a secure digital transformation for financial services



Trusted partner for your **Digital Journey**

Contents

Bolstering trust in challenging times

Financial institutions have been forced to accelerate digital transformation to adapt to the new operating models that require elevated customer experience and secured remote workforce. This transformation helps businesses evolve, but also leads to greater risks. Over the past 12 months, during the COVID-19 pandemic, financial services and insurance institutions globally have seen a surge in cyber-attacks and attempted attacks. The shift to home working and the increased flow of data from IoT or consumer devices has presented new security vulnerabilities. This has raised questions about how to protect sensitive data, reduce risks and prevent fraud.

According to the 2021 Data Breach Investigations Report from Verizon, 44% of the breaches in this vertical were caused by internal actors (having seen a slow but steady increase since 2017). Generally speaking, external parties target web applications for cyber-attacks or emails for ransomware. In contrast, internal breaches are often misuse actions, misconfiguration, or even malicious actions from internal employees. Giving a right to an employee which conflicts with another right (segregation of duties violation) or having a poor password hygiene (one person out of two admits reusing the same password for multiple accounts) are real examples of security failures. Human errors and password misuse are far too often Overlooked. However, they can be considered as one of the key challenges for companies that wish to make their IT system less likely to be breached.

Finance and insurance companies need also to put some strategies in place to mitigate internal threats starting with controlling employee's identities and access policies.

"From the beginning of February to the end of April 2020, attacks targeting the financial sector have grown by 238%"

Source: VMware Carbon Black threat data

"53% of people admit they reuse the same password for multiple accounts"

Source: securitymagazine.com/

Identities are essential to gain trust and protect reputation

Financial and insurance companies are moving business operations to the cloud as part of their digital transformation journey, to speed up response time and process more data. To take full advantage and mitigate the risks of managing multiple identities in a hybrid environment, it's necessary to control user access.

Identity and Access Management (IAM) is the set of business processes and tools for providing access to the right resources at the right time for the right reasons. It provides visibility into who has access to what and why, along with how the access is being used. Identity and access management secures identities, controls access and ensures policies compliance across the organization.

Stolen credentials are the most effective attack vector. Continued attention on strong IAM controls is a staple of any effective information security program. Strong authentication, monitoring user account behavior, privileged account management, and least privileged access controls continue to be vital.

CISO Executive Network, June 2020

Security focus points for the finance sector

The security challenges that a bank can encounter are the same for any investment or insurance company.

A highly secure digital work environment, available anytime, anywhere

Financial companies can now implement centralized, shared solutions, accessible by all their various branches, subsidiaries, and partners. They need to be reassured about the level of security. It is imperative for them to be able to delegate the administration of local users to middle managers or even directly to end users, by allowing them to submit their own requests. Protecting the confidentiality and integrity of user data is a crucial aspect of financial institutions.

Stronger security also means layered security, by restricting and monitoring access to customer data. With fine-grained access control, financial companies can ensure that limited people have access to user's data, and that they are the only ones who can view and manage them. This could further reduce the possibility of unintentional data leaks.

Certain actions within the company represent a larger threat and require users to take special measures to perform them. Strong multi-factor authentication can help reinforce the access to sensitive actions and assure the company that the associated users are both legitimate and safe to perform the actions in question.

The zero-trust model

Before becoming a set of technologies to be used in the company's information system, zero-trust security first is a state of mind: Do not trust anyone (internal or external) or any device (BYOD or COPE). The goal is to give users only the rights they need, according to what they must do and when they need to do it. Zero trust means constantly asking questions:

- Are the users from a high-risk group of identities?
- What resources do they try to access?
- Are these resources high or low risk?
- Is the user connecting from the company's offices?
- Does the user need to connect using a second authentication method?
- Do we authorize/deny the access?
- Do we launch a security alert?
- What is the global risk associated with user's connection?

Whether it is the cloud or software as-a-service, a modern company's digital environment is continually changing. With zero trust, companies regain control and visibility beyond the traditional perimeter.

Seamless experience

Finance companies need to be able to work in a daily basis with a secured, user friendly and always traceable system. All of this must be accomplished without creating a huge increase in their administrative overhead. It is important to be able to reuse current infrastructures without having to modify existing assets such as applications and websites. However, in our fast-moving society and changing working environment, it is also increasingly important to be able to benefit from seamless infrastructures like the cloud (SaaS) to stay on top of new technologies and digital transformation.

Moreover, password management can be a serious challenge for any company — especially for users. Having to remember a password for each application can not only be dangerous security wise (if users have the same password for every application) but it is also time consuming. The challenge is to prevent users from authenticating every time they need to connect to an application, to increase security and satisfy regulatory constraints. Companies need to save time for users and enable more secure passwords which are less sensitive to theft.

Finally, users need to have self-service features within the company's system to reduce helpdesk overload.

On-premises and multi-cloud

Cloud is a key enabler of transformation. Whether it is for faster time to deploy as compared to on-premises solutions, the cost to ratio or elasticity that enable rapid growth, cloud (or SaaS) solutions tend to take a more prominent role in a company's digital transformation. A combination of both cloud and on-premises solutions seems to be the right evolution for financial companies that wish to follow the tide while keeping control of their IT systems.

Regulatory compliance

To meet regulatory requirements, the key players in financial markets and insurance companies must implement measures to manage their risks. These requirements translate into implementing mechanisms to strengthen the access control to the information system to protect the integrity and confidentiality of data.

Finance and insurance companies regularly increase their compliance (Basel 3, Sarbanes-Oxley, GDPR, PCI DSS) and certification (Certified Financial Technician CFTe, chartered market technician CMT) requirements. A suitable IAM solution should therefore include these requirements as their top priority. The compliance answer could be found in an IAM analytics and reporting tool, which can help companies meet these requirements.

Risk mitigation

Financial companies regularly increase their certification (CFTe, CMT) requirements. A governance feature within your IAM system should therefore check the validity of users' accreditations before granting rights/roles/access to the company's assets.

Furthermore, an analytics solution within the company's IAM system can mitigate risk by editing views, dashboards and reports that can detect discrepancies and threats within the system. For example, highlighting segregation of duties violation to prevent fraud or errors.

Finally, an IAM solution that meets the expectations of the finance and insurance sector should enable the company to:

Reinforce security coverage

Facilitate compliance

Deliver a seamless user experience

The goal is to strike the right balance between these key components.

IAM to reinforce security

"Managing identities and controlling access to resources help to create a safer working environment and empower digital trust".

Modeling the requirements for access rights

In order to assign access rights for users, IAM Suite uses an approach based on role-based access control (RBAC) and organization-based access control (OrBAC) models. These models allow you to link rights to a particular role: normally a job within the company. To avoid the proliferation of roles, Evidian also uses the concept of "organization" to define the rights of people who fulfill a particular job in a given organization.

It is also possible to assign rights directly (without going through role assignment) in order to deal with exceptions.

The model also encompasses the concepts of organizational and hierarchical inclusion and exclusion to facilitate the task of assigning and managing the rights associated with a role. The rules governing segregation of duties ensure consistency by avoiding assigning a toxic combination of rights to the same person.

This modeling of rights will also be used internally to dynamically identify the actors of the user and rights lifecycle processes, as well as the behavior of those process — to easily tailor it to the company's needs.

Strong multi-factor authentication

IAM Suite allows an employee to authenticate using several methods, such as:

- User ID and password
- TOTP (time-based one-time password)
- X.509 certificate smart card
- SAML (service provider/identity provider) token
- Authentication method based on the Radius protocol
- Virtual keyboard and grid card password: each user has their own card for solving a one-time only challenge
- QR code via smartphone
- Push authentication via smartphone
- SMS OTP or email OTP: each user can obtain an OTP via mobile phone and/or email
- Biometrics, fingerprint and face ID
- Contactless with password, PIN, tap and sign/lock with NFC/Mifare card
- Kerberos and other Windows domain authentication methods
- External authentication mechanisms such as CAS, OpenID, OAuth, or linking to any external mechanism using SDK.FIDO 2.0

Those authentication methods can be combined to offer multi-factor authentication. The level of authentication required can be different for each application.

Seamless IAM

Making it easier to assign rights and monitor changes

Once rights have been modeled, it's important to be able to not only easily assign these rights to employees, but also to have mechanisms to monitor functional changes that affect employees, along with the associated rights changes.

IAM Suite employs a user's attribute values to assign roles to them that will involve rights. It is also possible to define exceptions. For example, everyone working in a banking agency must have the role of accessing the annual leave declaration application, in contrast to external users.

This feature makes it very easy to assign one or more roles to a newly hired employee, as well as to dynamically adapt to any new roles that an employee may take on as a result of transferring within the company. For instance, a banking office employee that moves to the headquarters automatically obtains the right access permissions.

By this means, companies can ensure that users have the optimal rights at any point in time as their job roles evolve.

It is also possible to assign roles to individuals using the role assignment process.

Password management

IAM Suite offers single sign-on (SSO) functionality. With this feature, the employee is authenticated only once, and any new request for authentication to access an application is taken into account by IAM Suite. This ends the problem of people forgetting their passwords after a long weekend or vacation.

Furthermore, a self-service password reset enables users to save time from helpdesk requests and reduce IT cost.

Reusing existing infrastructure

IAM Suite can be integrated into existing environments with no need for modifications.

Customer websites can be secured using IAM Suite without having to modify them. This allows authenticated users to benefit from advanced services or provide self-registration capacity.

Compliant IAM

Delegating responsibility to the business

IAM Suite offers a standard set of processes for managing identities, roles, accounts and services.

Currently, more than 50 processes are included as standard.

By using these processes, decisions about rights and user lifecycles are completely delegated to business users. Security officers and operational managers become accountable for those decisions.

You can move from centralized administration to a delegated administration where decisions are taken closer to the field.

Ensuring that rights are appropriated at any time

The principle of least privilege (PoLP) refers to an information security concept in which a user is given the minimum levels of access — or permissions — needed to perform his or her job functions.

Evidian IAM Suite provides a set of processes to perform access certification campaigns. Those access certification campaigns enable managers to validate/correct the existing rights of one or several employees. Undue access rights can be removed, to respect the principle of least privilege and reduce the risk of users having too many rights.

Controlling the required user accreditations

In many organizations — particularly in the finance market — access to applications doesn't depend solely on the user's business profile, but also on their level of accreditation. A certain level of accreditation (training, certification, signing a charter) may be required to comply with current legislations, insurance, company charters, etc. During audits, compliance reports may also be requested.

To meet these requirements, Evidian IAM Suite integrates a feature to verify that a user has the required level of accreditation when assigning rights. This feature also makes it possible to consider changes in accreditation level over time: granting rights upon obtaining accreditation or revoking them upon expiration of accreditation.

Proving compliance and enabling audit

IAM Suite can provide auditors and security compliance officers with advanced analytics capabilities.

This feature enables you to follow and analyze the use of your identity and access management system. IAM's analytics directly collect data from the other solutions of the IAM Suite and highlights evolution trends for accesses and entitlements. This overall view allows security professionals to detect suspicious events and take a risk-driven approach to IAM.

Finally, functions such as reconciliation allow you to detect discrepancies between what have been defined as the rights an employee must have and the actual rights they have. Corrective actions are then proposed, to allow the company to respond and close the gap.

Identity and Access Management in action

What are the strategic identity and access management requirements for finance companies today, how can Evidian respond to their needs and what are the benefits of such solutions?

Major challenges faced by banks and insurance companies

- Implement user lifecycle process automation and access governance.
- Need to delegate user rights decisions to operational staff
- Comply with market regulations and be able to prove it through audit enablement and detailed reports.
- High security requirements, with strict segregation of duties (SOD) management.
- Need for a web single sign-on (SSO) across several applications, with adaptive authentication depending on the security level required and based on the user rights policy.
- Avoid password fatigue by replacing passwords as main authentication.
- Emergency access with a self-service password reset feature.
- Save time and decrease helpdesk costs with password reset.
- Access from smart devices without changing applications configuration (non-intrusive).
- The solution must be multi-site capable with 24x7 access.

Solution

- Evidian IAM suite provides comprehensive, modular, and flexible identity solutions that are proven to answer the requirements of the financial sector.

Benefits

- Automated user lifecycle management based on reliable identity sources.
- Accurate management of user rights performed by operational staff.
- Monitor compliance with the security policy regarding the target applications.
- Toxic combinations eradicated, reducing risks.
- Enhanced security with reinforced password policies and identity governance.
- Web access and single sign-on to enforce the access security and increase user productivity.
- Reduced helpdesk costs with self-service password reset.
- Improved user experience with non-intrusive technology.
- Reporting capabilities for administrators, internal audit, and regulatory compliance.

Conclusion

By implementing Evidian IAM Suite, a finance company will benefit from an identity and access management solution that enables it, among other things, to:

- Manage the identities of people accessing the information system
- Implement the principle of least privilege.
- Verify that users have the required accreditations to access certain applications and follow the evolution over time.
- Delegate rights management to those closest to these people, who really know their business needs.
- Ensure that the access governance policy currently in force is always respected.
- Immediately consider any changes in people's rights, for example to reflect changes in their job role, a long absence, changes in their contract of employment.
- Evolve to reflect any organizational changes in the company.
- Give employees the autonomy to manage their own access without compromising company security, for example with a self-service password reset feature.
- Access a set of reports showing the information system governance.
- Provide simple and secure access (no password to remember).
- Adapt to the existing infrastructure.
- Ensure fine-grained access control to be sure that only limited people have access to user's data, and that they are the only ones who can view and manage them.
- Meet regulatory requirements.

Without exhaustively describing the capabilities of Evidian IAM Suite, this white paper demonstrates that Evidian is the ideal partner to help financial firms meet their needs.

Evidian IAM Suite

Our IAM solution is recognized by customers and analysts for its completeness. The Evidian IAM Suite offers the following components that can be deployed independently or combined. The implementation can be done on-premises or deployed as an as-a-service solution.

Evidian Identity Governance and Administration allows authorization governance and full lifecycle management of identities and access to applications, driven by a security policy combined with approval workflows.

Evidian Web Access Manager provides secure, policy-based authorization, identity federation, web SSO and multi-factor authentication.

Evidian Enterprise SSO enables access to enterprise and personal applications from workstations and mobile devices, freeing users from the password constraints.

Evidian Authentication Manager provides strong authentication on workstations and mobile devices: smartcard or token, X509 certificate, contactless RFID cards, biometrics and one-time password.

Evidian Analytics and Intelligence enables raw data from Evidian's IAM solutions to be collected and transformed into value added information for the company in the form of dashboards, views, and reports.

Evidian SafeKit brings high availability and load balancing to applications.

White Paper

About Evidian

Evidian is the Identity and Access Management (IAM) software suite of Eviden.

Evidian IAM is the European leader in identity and access management with a presence which is growing rapidly beyond Europe, particularly in Japan and the US.

More than 5,000,000 users in more than 900 organizations throughout the world connect to their companies every day and manage their access rights with Evidian identity and access management solutions.

For more information: **evidian.com**

CT-210531-JS-WP-IAM