SECUROLOGY

AN INITIATIVE BY **AVANCER CORPORATION**

VOLUME 1: EDITION 1

WHAT GOES INTO THE MAKING OF IAM TECHNOLOGY IN FINANCIAL SERVICE INDUSTRY?

SSH KEY MISMANAGEMENT: A GROWING THREAT PROFILE FOR YOUR BUSINESS

REGULATIONS THAT REQUIRE IAM SUPPORT

STOP BURDENING THE ACTIVE DIRECTORY

securology.us

ADDRESS ACCESS SYNCHRONIZATION, MULTIPLE INTEGRATIONS AND IDENTITY UNIFICATION ISSUES IN HYBRID IT SETUP WITH IDENTITY BRIDGE

Consult Experts
Email: info@identitybridge.us

IDENTITY BRIDGE

Intelligent Identity Integration

FROM THE TECH DESK

RAJESH MITTAL
Technology Specialist

With over 20 years of experience in Application Security, Identity Management and IT Infrastructure, Rajesh assists clients, spanning across industries, in every aspects of IT Security.

Businesses are readily embracing technology to achieve competitive advantage. With technological advancements, a parallel need for studying the security paradigm surrounding new technologies has been stated time and again. While information available in the market supports short-term needs of new technologies, a long-term perspective is often missing.

Given the threat-landscape, it is becoming important to study and visualize the security paradigm surrounding technological innovations. We envision technology as a strategic business facilitator. **Securology** is an initiative to enable businesses identify challenges around enterprise security.

Our first issue focuses on topics that are at the heart of IT security and business process automation discussions. These include identity integration in scenarios of multiple target sources, aligning SSH keys with right accesses and Internet of Everything (IoE) in financial services industry.

I look forward to your thoughts and valuable feedback on our flagship edition. Feel free to drop me an email at mittalr@securology.us.

OUR TEAM

SECUROLOGY, VOLUME 1: EDITION 1

SHINE KAPOOR
Editor-in-Chief

ASHA DEY
Senior Editor

RAJESH MITTAL
Technology Specialist

ARUN MEHTA
Enterprise Security Specialist

ABHA SHARMA
Market Specialist

SHOBHIT GUPTA
Market Specialist

JASNICA SINGH
Designer

OM PRAKASH
Designer

Email Id: info@securology.us | Phone: +1 (609) 632-1285 | Website: securology.us
Editorial Contact: editorial@securology.us | Advertising Contact: advertising@securology.us
Securology (**ISSN 2576-3369**) is published by Avancer Corporation, 101 Interchange Plaza, Suite 201 Cranbury, NJ 08512, USA.

CONTENTS

A secure system is required to kill complexity and act as a transient path for identities to interact with the system on a real-time bi-directional basis.

WHEN IT COMES TO UNIFYING IDENTITIES, STOP BURDENING THE ACTIVE DIRECTORY

Shine Kapoor

Hybrid IT is fueling the digitization agenda by aligning strategic requirements of IT function, while transforming IT architectures and supported roles. As some apps are linked on-premise and some to cloud, it is crucial to ensure that identity and access related dynamism falls in line with required considerations.

An important and perhaps the most ignored aspect of hybrid IAM is unification of identities from multiple identity sources (target systems). It is a challenge, because capturing multiple credentials of a user and setting them up to merge in the system can be complex.

This impacts identity flow into the IT system and achieving an ideal scenario of one user-one login becomes a far cry. To ensure scalability for any integration, IT folks have to work towards negating creation of duplicate entries in identity management system. In existing setup, this takes a lot of manual effort and does not assure that the system will be fool-proof.

Furthermore, target sources are burdened to supply identity related information while providing access to applications. Such an approach necessitates the target sources to link identities with diverse and unrelated information, impacting system efficiency and IT workflows.

In many cases target sources are not the true identity sources and pulling identity information from an untrue identity source results in additional maintenance challenges. There is a structural complexity in hybrid environment as flow of identities from multiple setup and their interaction with each indigenous IAM setup, including users and their access criteria, is not strategized for self-sufficiency. Any conflicting or overlapping identities have to be flagged to the system admin, ensuring that identity information is unified in true sense.

Amidst workflows and identity considerations, IT teams are deputed to ensure operational efficiency and reduced complexity. They are often busy consolidating workloads, juggling with concerns regarding user life cycle management, IT security, corporate governance, system performance, migration, upgrades and integrations.

VISUALIZING HOW IDENTITIES FROM MULTIPLE SETUP INTERACT WITH EACH INDIGENOUS IAM PLATFORM POINTS AT COMPLEXITY!

The struggle is further accentuated as users navigate between disparate systems, to bring identity consistency and manage admin dashboards of multiple applications. All this is to be done while ensuring that none of the systems or tools are going out of operations. The most complex task is to get identities to unify from multiple target sources such as Active Directory(ies), Office 365, PeopleSoft, etc. to enterprise apps, tools and IAM platform(s). It becomes a challenge and results in creation of duplicate identities in the enterprise identity management system. Identity unification could be achieved even without Active Directory bridges. System integrators use customizations to enable secured and real-time bi-directional transition of identities. A secure system kills the complexity and acts as a transient path for identities to interact with each other, in addition to flagging any conflicting or overlapping identities.

As businesses are increasingly seen to be moving towards cloud-based platforms, not much thought is given to ease of integration with existing on-premise applications and/or IAM setup. Hybrid integration solutions are also becoming an essential tool for organizations that are considering to combine on-premise apps and cloud-based apps.

Solving integration challenges and ensuring effective automation of IAM capabilities in hybrid environments is the way ahead. Going forward, it is crucial for businesses to optimize IT capabilities and put a mechanism to bring together hybrid IAM platforms. Identity management systems that are supported by tools, such as Identity Bridge by Avancer Corporation, facilitate operational requirements, supplement remote access and create mobile synchronized workflows.

Hybrid integration solutions are becoming an essential tool for organizations that are considering to combine on-premise applications with cloud-based applications.

LEADERS SPEAK

Cybersecurity is often an afterthought. The state of cybersecurity will only get worse until the risk dialog with the business gets underway. If IT security is going to be frictionless, then it's not about the business learning security, it's about security learning the business.

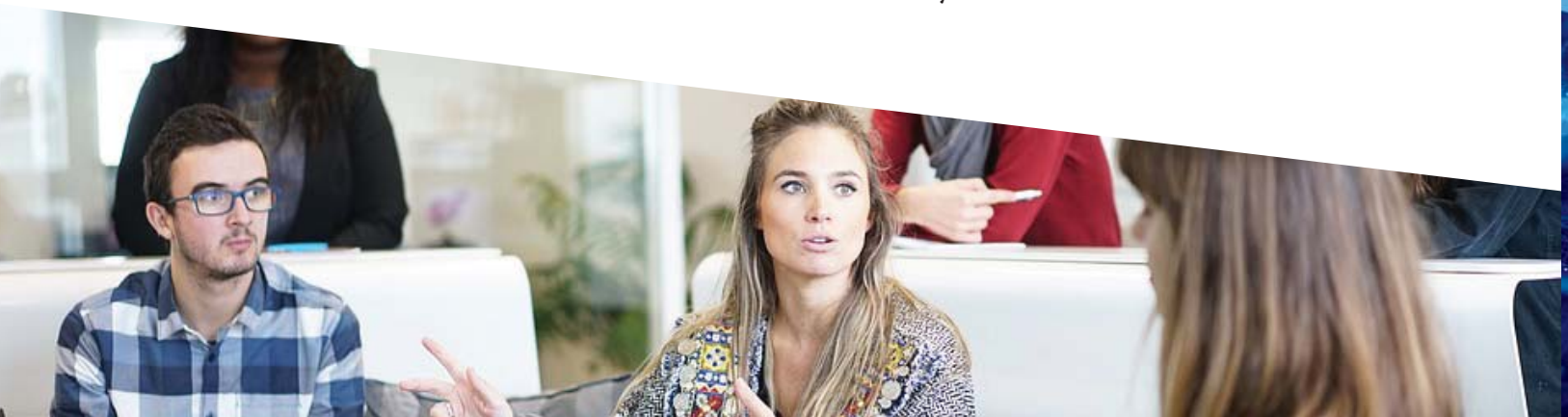
RED CURRY
Sr. Director of US Marketing & Security Evangelist
SSH Communications Security

Distributed identity, intelligent access decisions and automation of processes will dominate IAM space in the year 2018. Block chain technologies, artificial intelligence and Robotic Process Automation (RPA) would be the means to realize these three trends respectively and organizations should consider investing in them to stay ahead of the curve.

VIBHUTI SINHA
Chief Cloud Officer
Saviynt

The way that we're going about security is actually failing. We're falling further behind, and the reason why is really two-fold. First, we're going through a massive shift to the cloud. But the vast majority of IT spending in security is still for on-premises...The other aspect is that the attack vectors have completely changed, as well. Hackers are increasingly focusing on users and their identities.

TOM KEMP
CEO
Centrify



CONTEMPLATING AN UPGRADE OF ORACLE IDENTITY GOVERNANCE?

AVANCER'S OFFERING FOR ORACLE IDENTITY GOVERNANCE 12c PS3 INCLUDES

- 2 connectors upgrade
- 3 to 4 months implementation timeframe
- Domain reconfiguration and configuration upgrade
- Schema upgrade and 12c installation
- 2 weeks post upgrade support

Consult experts, email us on info@avancercorp.com

Avancer
Simplified IT Security

COVER STORY

Experts encourage IT folks in financial industry to take a 360-degree view of identity, access and security challenges while integrating or streamlining IAM capabilities.

WHAT GOES INTO THE MAKING OF IAM TECHNOLOGY IN FINANCIAL SERVICES INDUSTRY?

Rajesh Mittal

Financial services industry—which includes banking, insurance, risk management, wealth management, asset management, and others that are monitored at the state and federal levels—is subjected to various regulations. It is crucial to explore technological aspects involved in the implementation of IAM solutions, for fulfilling governance requirements such as policy enforcement, assessing risks, auditing, compliance and reducing frauds.

Requirements for an IAM implementation by their very nature are complex. A broad range of stakeholders are integrated under the umbrella of IAM capabilities. This includes setting up of strong fundamentals in managing user identities. Understanding industry and compliance specific challenges in implementing IAM solutions and harnessing IAM technology in fast changing IT ecosystems is imperative.

In current digital environment, IAM in financial services has moved beyond provisioning and access controls. With continued adoption of various customer engagement models, innovative mobile and cloud technologies, financial services industry is at a constant struggle of creating robust capabilities to achieve IT security, workflow automation and system optimization. IAM in financial industry covers a wide range of users, devices and apps—leading to a massive upsurge in quantified identities, including employees, consumers and third-party vendors. Integration strategy of IAM (and IT security solutions) in the current environment must take into account vulnerabilities emanating from sensitive data, digital assets and intellectual property.

FINANCIAL SERVICES INDUSTRY FACES SIGNIFICANT CHALLENGES IN MANAGING DATA IN A SECURE MANNER, ALONG WITH COMPLYING WITH REGULATIONS SUCH AS:

- **Gramm-Leach-Bliley Act (GLBA)**
- **Sarbanes-Oxley Act (SOX)**
- **Payment Card Industry Data Security Standard (PCI DSS)**
- **Dodd-Frank Wall Street Reform and Consumer Protection Act**

In the financial services industry ensuring reliable and efficient access is complex. IAM technology in this scenario needs business intelligence in defining: **'Who' (employees, partners, contractors, customers), 'What' (sensitive customer information, database access) and 'When' (location, time, IP address)**. The deal is to achieve a strategic balance between providing information to right set of users and ensuring safeguarding of sensitive data.

Cyber regulations transcend borders. For instance, financial institutions with multinational imprints, especially in the European Union region, would be required to comply with General Data Protection Regulation (GDPR) starting May 25, 2018. GDPR gives citizens control of their personal data and all institutions that collect, process or share an individual's personal data will need to gain 'freely given, specific, informed and unambiguous' consent by the customer themselves. This is going to impact the way data privacy laws and mechanisms are standardized across industries.

In addition to self-driven checks, businesses in the financial sphere need to comply with strict norms, including OMB Circular A-123, Basel II, Consumer Privacy, Data Privacy, Check 21, Anti-Money Laundering, SAS 70, BSA, MiFID, PATRIOT Act, etc. While grappling with stringent compliance criteria, the industry is required to invest efforts to simplify compliance processes.

Organizations looking at cloud services for boosting efficiency and pruning costs of managing identities. It needs to be strengthened with greater controls and clear visibility of users' actions.

Managing identities in complex financial IT environment requires unifying and streamlining identity—from all the systems, apps and platforms under a repository guided through Active Directory or target source. This enables enterprise IT to gain control and achieve better visibility of users' actions, thereby reducing risk.

With strategically aligning IAM capabilities, financial organizations minimize risk of information or data loss. It also offers in-depth knowledge around ineffective and inefficient processes within an organization, thereby providing greater monitoring and checks. Alongwith understanding requirements of IAM technology, experts encourage IT folks in financial industry to take a 360-degree view of challenges and assess them from futuristic, best practices and strategic standpoint.

Addressing Unique Challenges While Implementing IAM in Financial Services

When it comes to implementing IAM in financial services, the industry faces certain challenges that are unique to it, leading to concern areas that are often overlooked.

Avoid exponential Identity creation by streamlining one user-multiple applications. Identity is no more just about a user, the algorithm of identity creation takes into account a user, associated devices and applications. This creates a conundrum of identities that grows exponentially. In the midst of IoT revolution, it boils down to the number of identities held by a single user, thereby creating multiple identities for monitoring, organizing and controling.

Creation of orphan user accounts should be discouraged. Orphan accounts are basically an identity in the system that does not have a defined owner. Often an account is created for an important task, but the usage of the account is not frequent. Such an account also lacks a clear ownership, resulting in undefined accountability and unmonitored access of sensitive data.

Putting in place a clear procedure for monitoring of users' accesses. Despite being an important checklist item, monitoring accesses is a difficult procedure to follow. This leads to hackers gaining access to unmonitored users and causing financial losses to organizations. Furthermore, without access monitoring, IT audit reports remain inconsistent and compliance to relevant regulations is not achieved.

STRATEGIC APPROACH FOR MANAGING COMPLEX FINANCIAL IT ENVIRONMENT STARTS WITH UNIFYING AND STREAMLINING IDENTITY(IES) FROM ALL CONNECTED SYSTEMS, APPS AND PLATFORMS, AND THEN ALIGNING THEM WITH THE TRUE TARGET SOURCE.

Patchy control of privileged accounts to be monitored for avoiding breaches. Another important issue is lack of control over privileged application access, including accounts of superusers. It is crucial to keep a tab on accesses made through privileged accounts as these could be easily located by cybercriminals. This is all the more important in a scenario, wherein temporary permissions are allocated to users and access is not revoked.

Providing just as relevant applications' accesses to users. It has been observed in many situations that individuals are given access to information or data they might not need, increasing the chances of misuse. A defined process should be followed and enforced to ensure that systematic flow for accesses is maintained in all situations.

Robust IAM Capabilities to Create Futuristic IT Ecosystem

With evolution in digital technology, financial institutions are also seen to evolve its capabilities, especially in harnessing app-based mobile activities. This is leading the industry to integrate IAM capabilities to create a robust and scalable system as per newer developments in the FinTech space.

Integrate IT systems with customized capabilities. Various applications are integrated in the financial services IT architecture to serve the operational requirements, which might not be under the purview of IAM setup. Driving identities in enterprise applications setting through IAM platform is crucial for compliant, auditable and efficient system. Furthermore, attributes related to application access might need customization on the back-end, which should not be ignored.

Bring together Internet of Everything (IoE) devices in a single dashboard. Integration of IoE may help financial services organizations in providing better customer experience, reducing risks and redundancies, while increasing their market share. Key for successful implementation of IoE application is integration with a single IAM dashboard to monitor the status, location and security of devices, along with providing multiple alerts and notifications on a real-time basis.

Implementation of Consumer Identity and Access Management (CIAM) is leading the way. CIAM solutions are enabling financial services industry to put customers at the core, allowing users securely sign in into their

Financial services industry is at the forefront of implementing big data solutions, enabling it to take quicker decisions, optimize processes and generate insights.

systems through the social profiles. It helps in identifying and understanding user behavior across various digital platforms—including website, mobile applications and other marketing channels.

Setting a strong groundwork with Federated Access Management (FAM) mandate. It is important to constantly upgrade or patch new components into integrated system to circumvent the risk of being obsolete in the face of newer cyber threats. That's where FAM comes into the picture, providing instant upgrades, selecting the right set of components and patches, and enabling the system to seamlessly deploy IAM processes.

Becoming rich in Big Data insights. Financial services industry is at the forefront of implementing big data solutions, enabling it to take quicker decisions, optimize processes and generate insights. Balancing vast amounts of data on infinite scale requires continuous surveillance and on-going capacity optimization.

Financial organizations have to build digital capacities to secure IT ecosystems through digital identities check-points for all sets of users. The banking sector is seen to use custom apps for better functioning of their corporate offices and customer care centers, along with facilitating secure transfers of funds. The insurance companies also use a variety of applications for analyzing market data and helping customers manage their policies. Companies in the financial and insurance sectors are increasingly using apps to provide value-added services such as mobile banking, ATMs, risk calculators, fund transfers, etc. by utilizing big data insights.

To this effect, various FinTech capabilities are to be integrated in to the IT architecture. Such capabilities should support a mechanism that caters to high-volume business processes, allowing strategic treatment of access to various identities (including devices, users, applications and resources). The solution takes financial services enterprises closer to highly secured, personalized, quality, compliant and secured digital interface.

ELEMENTS OF STRATEGIC ACTIVE DIRECTORY MANAGEMENT

An agile Active Directory is the key to management of identities! Properly managed Active Directory(ies) strengthens the process of audit and compliance as it maps users with values. It also enables tightened security related to accesses, while bringing workflow success, business continuity and value addition.

Holistic
Directory Management

Streamlined
Security Permissions

Proactive
Identity Administration

Robust
Recovery Mechanism

Intuitive
Reporting and Alerting

Simple
Policy Management

Resolve Active Directory(ies) Management challenges in your organization, find out more by speaking to our advisors.
Email: info@avancercorp.com.

INDUSTRY REGULATIONS THAT REQUIRE IAM SOLUTIONS

Shobhit Gupta

Regulatory compliances and IAM technology go hand-in-hand, as they focus on the same two entities—user and data. At a high level, it includes users' actions around data, users' accountability, users' privacy and data protection.

While IAM implementation is often believed to be a high expense task for organizations, it is also pegged as an investment—that too a smart one! How? It is about subverting impending threats, strategically creating IT systems for business efficiency and improvements. The benefits from achieving compliance are two fold—meeting basic security requirements and bringing operational efficiency through automation of IT processes related to provisioning, authentication, SSO, attestations, etc.

As IAM solutions emphasize the importance of its role in helping organizations meet compliance requirements, it is imperative to take a closer look at each one of them and how they can be addressed at different levels. Many regulations require organizations to harness IAM technology. Violations of regulatory compliance often result in harsh penalization.

At the core of IAM concepts is an emphasis on just and right access provided to user roles, which plays a crucial role in meeting compliance requirements.

Bird's eye view of industry regulations that need IAM capabilities

Regulations	Applicable Industries	Access Capabilities						Identity Management				Privilege Accounts		Audits	
		Centralized Authentication	Secure Login	SSO	Federation	Mobile Access	Password Management	Role Management	Provisioning	De-provisioning	Approvals	Security Rules	Role-based policies	Users Actions	Response
Sarbanes-Oxley Act of 2002 (SOX)	Finance, Banking, Insurance	✓	✗	✓	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓
Payment Card Industry Data Security Standard (PCI DSS)	E-commerce	✓	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗
Gramm–Leach–Bliley Act (GLBA)	All Financial Institutions	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗
Health Insurance Portability and Accountability Act (HIPAA)	Healthcare, Life Science	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗
Family Educational Rights and Privacy Act of 1974 (FERPA)	Education	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
North-American Electric Reliability Corporation (NERC)	Energy, Utilities	✓	✗	✓	✗	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓
Health Information Technology for Economic and Clinical Health Act (HITECH)	Healthcare, Life Science	✗	✗	✗	✓	✗	✗	✓	✓	✗	✗	✓	✗	✓	✓
General Data Protection Regulation (GDPR)	E-commerce, Consumer Specific	✓	✓	✗	✗	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓

Regulations defend enterprise systems and protect users' accounts, taking intangible benefits to shareholders, public and most importantly, a business brand.

Some other compliances that require IAM technology include FDA 21 CFR Part 11; The Health Information Technology for Economic and Clinical Health (HITECH) Act; ISO 27001; Federal Information Security Management Act (FISMA); Freedom of Information Act (FOIA); Federal Information Processing Standards (FIPS 200); and National Institute of Standards Technology Special Publication (NIST SP 800-53).

Federal regulations and industry standards mandate businesses to enforce IT audit controls. Regulatory compliances defend enterprise systems for the protection of user accounts, shareholders, the public and most importantly a business brand. Therefore, regulations concerning privacy and separation-of-duty requirements are here to stay, and perhaps evolve for better!

While achieving compliance to regulations, security professionals need a strong hold on attaining tactical goals through managing, measuring and monitoring IT governance initiatives. It is recommended that the tactical goals are aligned to regulatory environment, applicable standards and controls. Integrated business systems for industry specific or cross-industry compliance requirements need to be achieved by keeping a close watch on core and non-core business applications. In addition, stepping-up the legacy architecture by bringing together IT systems with current business requirements will make them more responsive towards regulatory dynamics.

Avancer facilitates holistic management of corporate Governance, Risk and Compliance initiatives.

Find out more on GRC and security requirements for your business. Write to us at info@avancercorp.com.

Avancer's Testing Service for a 360 degree assessment of vulnerabilities within Enterprise IT System.

STEP BASED APPROACH

- Detailed discovery of system loopholes
- Enumeration of threats against loopholes
- Mapping of system vulnerability(ies)
- Vulnerability(ies) exploitation for assessment

Consult experts, email us on info@avancercorp.com

Avancer
Simplified IT Security

CREATING SECURED INTERNET OF EVERYTHING (IOE)

Abha Sharma

The world is accelerating towards embracing smart devices. We are in midst of a lifestyle revolution where each device has its own identity and interacts with a range of interconnected devices. Name a task and a smart device to conduct that task will surface.

There is a plethora of devices available in the market such as smart thermometers, wireless blood pressure monitors, smart Bluetooth bulbs, fitness tracker wrist bands, pet tracker collars and many more. These devices are controlled by remote sensors which include mobile phones, tablets, laptops, desktops, personal assistance devices, etc. Each of such devices collect information, has an identity assigned to them and conducts an allocated task. In geeks' language it is called Internet of Everything (IoE). This stresses on the fact that the world is getting connected with devices and each of them has an identity.

IoE as a medium connects devices in more relevant, empowering and smart ways. In the coming years billions of physical objects will be connected to the Internet, including industrial and household devices. So if we break this, it means:

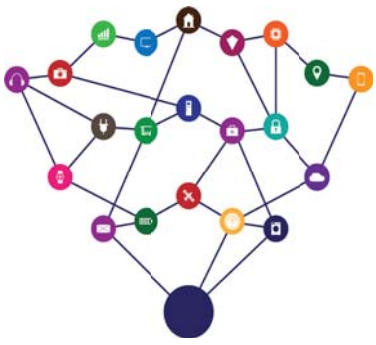
More Smart Devices
More Automation
More Access Points
More SSO Capabilities
More Securing Identity

…more for you to add

Inter-connected objects within a household is not a new concept, even enterprises in the oil, gas and utility industries have integrated connected equipment to support remote operations. IoE is an extension of this concept. It brings Internet into the picture, making inter-connected devices prone to cyber vulnerabilities. **In addition to conventional ways for cyber criminals to enter into a network, there could be numerous possibilities for hackers to breach vulnerable IoE connections**. The information captured by devices is synced by apps and is fragmented. A single dashboard that can compile information and enable interaction to bring out concrete information is missing.

IoE devices however are easy to secure. The importance of setting baselines for the type of data that network administrators use has been time and again reiterated by cyber security specialists. The number of devices per person keeps on adding up, leading to management of one's identity at the core of technological revolution. This also brings into perspective management of all devices through a one-time

Inter-connected objects within a household are not a new concept. Even enterprises in the oil, gas and utility industries have integrated connected equipment to support remote operations.



IOE ENABLED DEVICES ARE PRONE TO CYBER VULNERABILITIES AND LOOPHOLES. THERE COULD BE NUMEROUS POSSIBILITIES FOR HACKERS TO BREACH THE SYSTEM. HOWEVER, IT IS OFTEN OVERLOOKED THAT SECURING IOE DEVICES IS EASY.

login mechanism on the lines of SSO. The biggest worry definitely is adhering to the regulatory compliance, especially for data privacy, while adopting IoE.

For instance, the financial services market is monitored at federal and state levels, and is subjected to various regulations. Complexities in businesses, with increased regulatory as well as market scrutiny, have led to organizations adopting a structured approach in managing GRC. In this backdrop, IAM is seen as an enabler for fulfilling governance requirements such as policy enforcement, assessing risks, auditing compliance and reducing frauds. In order to close security related loops, it is crucial to govern access of IoE devices.

Come to think of managing zillions of identities, it needs customization and automation. Exploring potential impact and opportunities related to the deployment of IoE technologies is crucial, and developing strategies to combat threat is the way IT security market is headed.

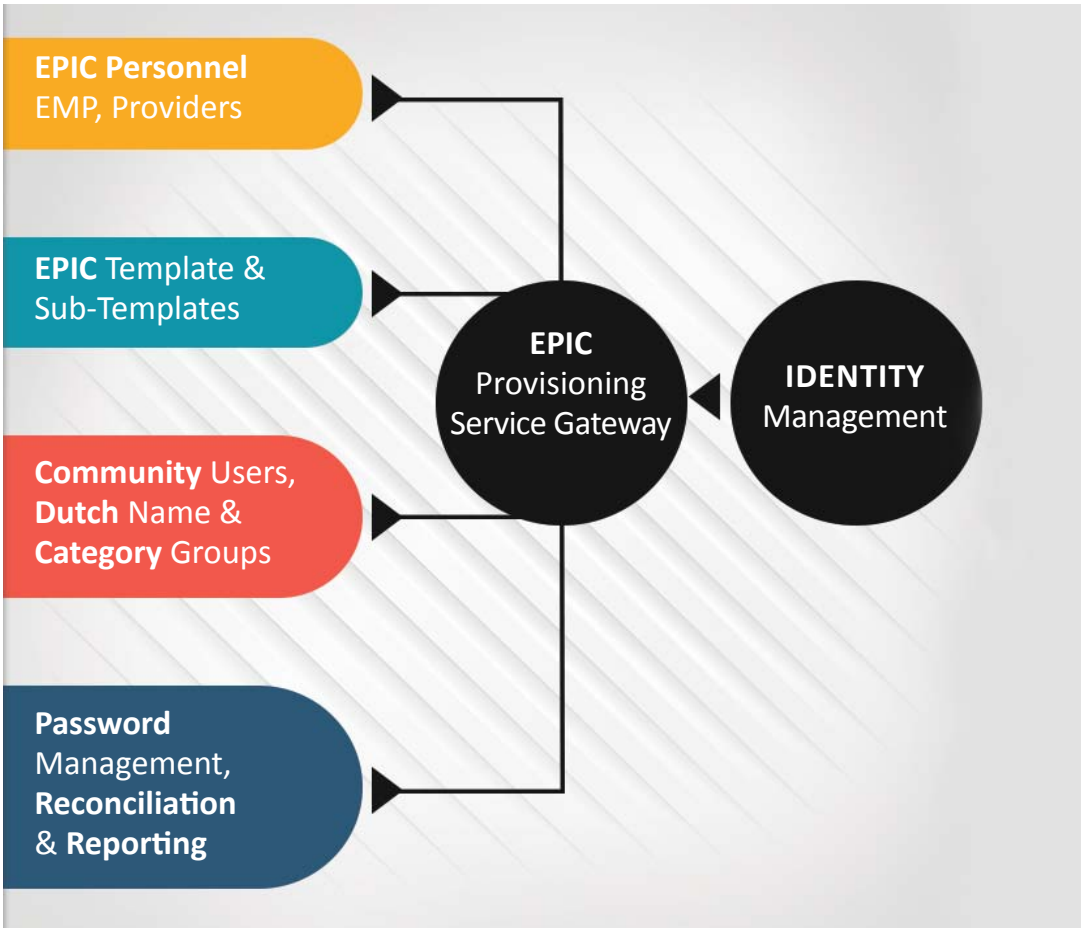
Although, IoE offers new opportunities, it might also disrupt the marketplace. It may facilitate the rise of new business models and a much more competitive market. For companies in the financial services to yield value from IoE, they would have to rethink, adapt, adopt and take a look at privacy and security requirements of the system.

DATA SHEET

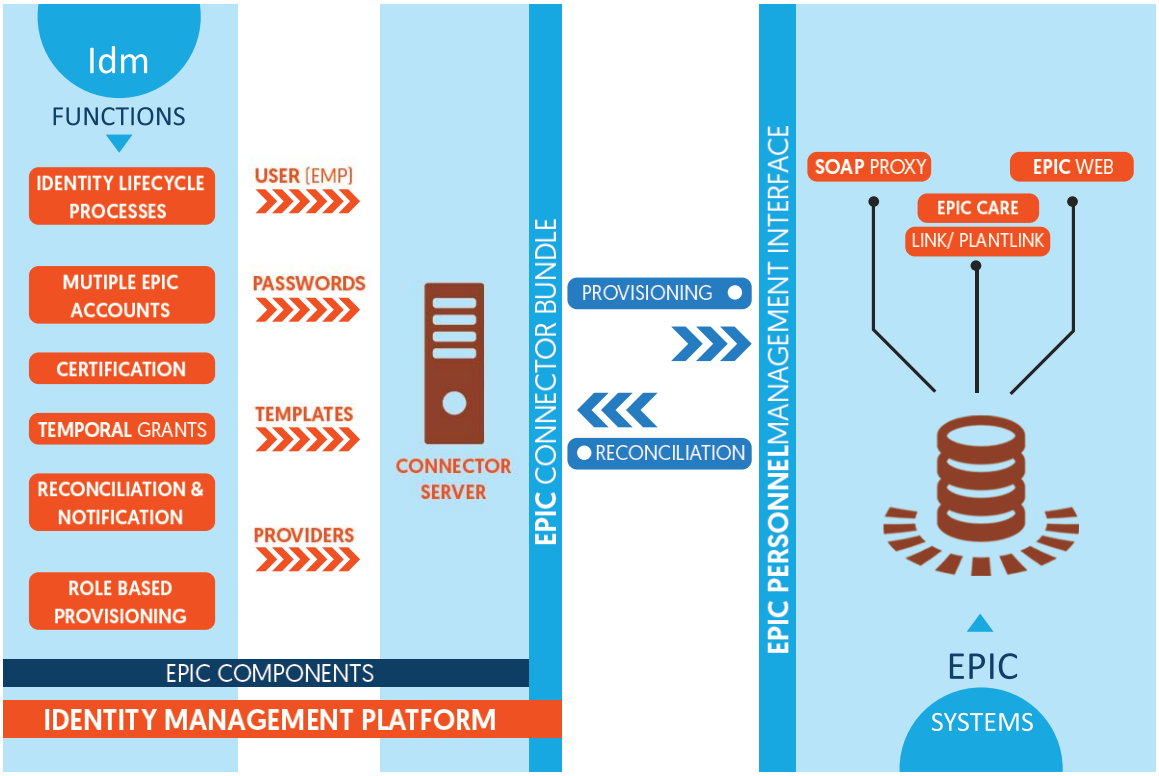
AVANCER'S EPIC – IDM PROVISIONING ENTERPRISE APPLICATION CONNECTOR FOR HEALTHCARE IT

Within the purview of healthcare industry, EPIC is an important application support system. It creates software for medical groups, hospitals and integrated healthcare organizations, spanning across clinical, administration and revenue divisions. It supports functions related to patient care, including registration and scheduling, clinical systems for doctors, nurses, emergency personnel and other care providers, along with systems for lab technologists, pharmacists and radiologists and billing systems for insurers.

According to EPIC, hospitals that use its software are in possession of 54% of patients' records in the US. Such a wide and extensive usage of EPIC applications makes it imperative to synchronize administrative IT capabilities that support identity management and access governance. This is important for achieving



In addition to ease in integration, connection between EPIC System and IAM Platform supports CRUD functions, reduces administration costs and provides better control of access.



High level diagram of processes that govern interaction between EPIC Systems and IdM Platform.

better interaction and security amongst application end points and IAM capabilities.

Establishing a connection between EPIC Systems and IAM platform takes down manual intervention, brings cost benefits and ensures system efficiency. However, the question is how is the healthcare IT system making efforts to shield against any access made via EPIC Systems? Also, how often do they audit for de-provisioned users or account for accesses made by users who were supposedly dormant?

IT administrators in healthcare organizations understand the work-loads that go in to management of EPIC Systems. Furthermore, getting EPIC Systems to interact with IAM solution is complicated. For a start, it needs to support simplified, real-time and robust interaction. Within EPIC's scope of usage, a user must be provisioned in each domain using tools that interact with IAM capabilities. IAM-EPIC Application Integrator helps to improve the usability and adoption of EPIC applications and integrating it with the exiting IAM platform. The connector focuses on strengthening IT system by easing workflow through SSO capabilities, simplifying administration through centralized automation of user identity and ensuring right access.

Ideally EPIC Systems connector must cater to all identity management functions to automate interaction between EPIC Systems and any identity management platform, including home-grown systems. Quantification of benefits to business when IAM drives workflows of any application are hard to put together, however some broad benefits can be identified as follows:

Drastically reduced error prone manual efforts. IT system workflows need to enable secure, timely and accurate automation of provisioning process and tie them to existing enterprise provisioning systems in an automated way. The connectivity established through EPIC-IAM application integration must take care of this, and can be quantified in recoding reduced help desk intervention for access or password management related requests.

Reduced man hours naturally brings down administrative costs. Channelizing information from an authorized source, IAM platform in this case, decreases maintenance costs, constant auditing requirements and data security risk. The checks placed in the process arms the IT teams to focus on strategic aspects.

As IAM and EPIC Systems interact with each other, duplication becomes a thing of past. Robust interaction with existing identity management systems does not need a constant watch. The integration facilitates provisioning/de-provisioning compatibility, tracks inactivate users' record on all associated domains from a single source, no additional certification required, etc.

Experts suggest that integration between EPIC Systems and IAM platforms ought to bring specific set capabilities, including:

- **Rapid Application Deployment:** Collate all identities by enabling Active Directory integration with EPIC System through a simple and quick process.

Interaction between EPIC Systems and existing identity management systems does not need constant monitoring.

- **User Synchronization Intelligence:** Bring together users' data, create, upgrade and delete identities (users and/or devices), and eliminate login-related duplicate tasks by integrating with corporate credentials.
- **Connected Application Integration:** Achieve users' access consistency based on entitlements–position, department and groups, access guidelines and healthcare industry regulations.

Functions performed by Enterprise Application Integrator as a trusted virtual administrator include lifecycle management, access assignment, authentication, management of passwords and attributes performed by EPIC. It adds value by eliminating complex and costly developments and extends the ROI of existing technology investments.

An example of functions performed by interaction between IAM and EPIC Systems is when a user has been created by the IdM system, it is automatically reflected in the EPIC Application system. **Activation of an account on EPIC Systems is conducted simultaneously. Once a user is created on an IdM system, the user details automatically gets reflected in the EPIC Application system**. Thus, activation of an account on EPIC Systems is conducted.

User's specifications based information updates get passed on to EPIC application system on real-time basis and identifies the items that are to be changed. Any changes in a user's detail, including department, position, role-based evolution, are to be consistently reflected on all connected platforms and/or applications. This must also allow limiting the access of inactive users from EPIC application web service to bring down chances of misuse of official information. When a user is out of the enterprise system, the application integrator deletes the account from the app. It also undertakes management of user passwords such as setting user or external passwords and forcing password change.

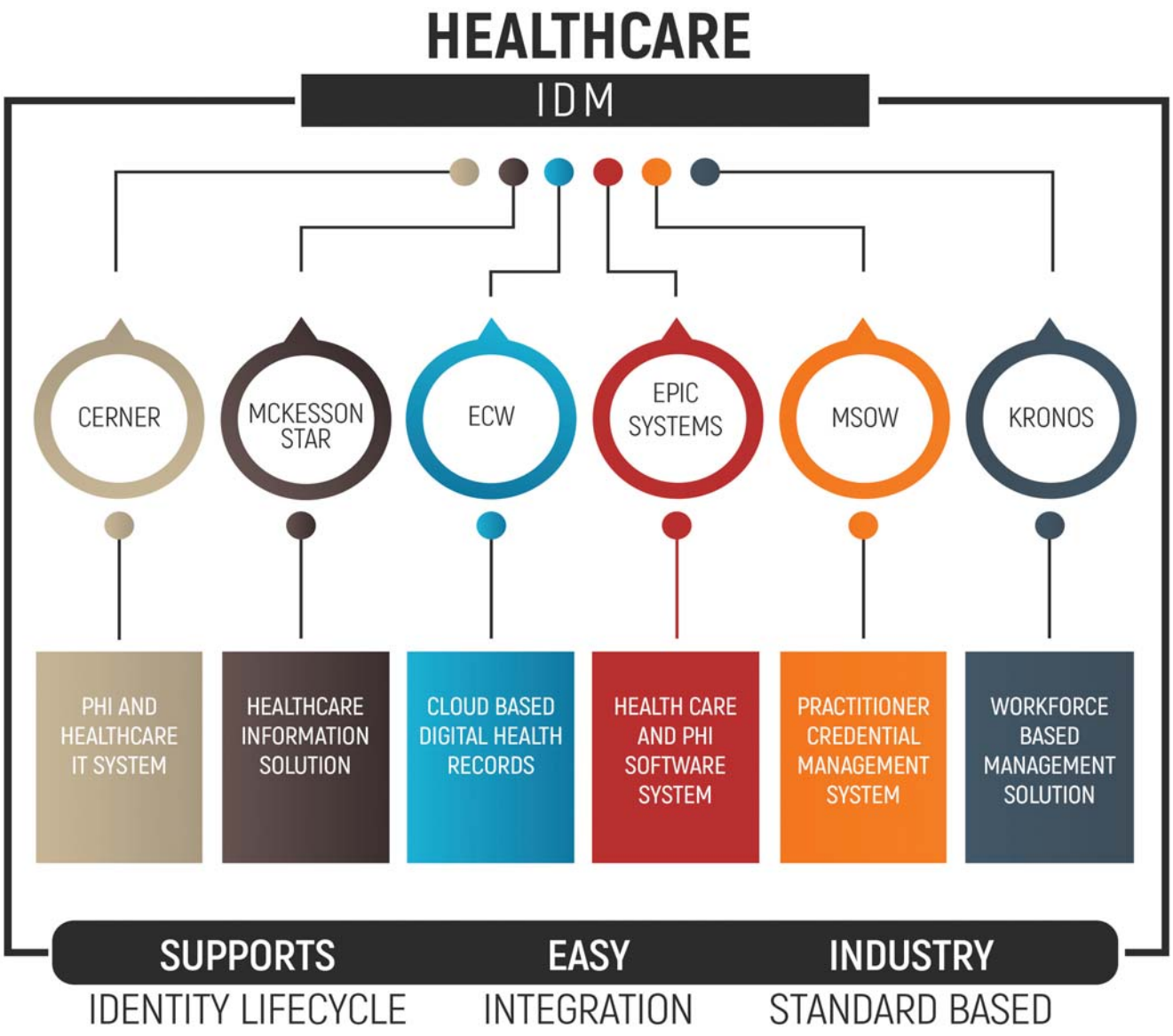
Supported Functions of EPIC – IdM Provisioning Enterprise Application Connector

Keeping the healthcare industry at the center of processes, during user creation EPIC connector performs CRUD operations on employee identity and setting items like multiple linkable templates, employee demographics and category report groupers. These functions can be performed singularly or depending on the operation in a batch mode. This is just a step to bring consistency with regulatory mandates and creating systems that are made to accommodate future needs.

EPIC-IdM connector by Avancer supports 2012, 2014 and 2017 Security Services Personnel Management and handles all identity life cycle events that includes joiners', transfers' and leavers' identity processes under the EMP records and Schedulable EPIC Resource (SER).

Details of functions performed by interconnected IdM platform and EPIC Systems

Functions	Details
Create User	Automated creation of a new user account on EPIC Application to provision the user and populate initial items. This function expands to set new items like multiple linkable templates, employee demographics and category report groupers during user creation. It also allows to create provider (SER) information.
Enable User	Activate a disabled user account on the EPIC Application and it also clears an end date set in the past, update the record based on the linked template and can add information to login history, if needed.
View User	Search user(s) from within the Active Directory.
Update User	Modify privileges or multiple linkable templates of users' accounts on the EPIC Application. The old value will be replaced with new value and new values can be assigned to the end of the list, if needed.
Update Community User	Update access to EpicCare Link/PlanLink/Healthy Planet Link ("community user") items
Disable User	Temporarily inactivate a user account on the EPIC Application. In EPIC system, inactivate a user record by setting the Status—Status (I EMP 50) item.
Delete User	Revoke the access of a user's account on EPIC Application. On EPIC System, this function soft deletes a user.
Password Management	Actively support tasks to manage, change (force change) and/or generate passwords. Password propagation to EPIC Systems for users who uses EPIC Native Authentication.
Reconciliation	Reconciliation of templates, sub templates and groups, access received from the target system. Reconciliation of users based on the data sent by EPIC on daily basis.
Reporting	Reports that allow the view of users' access such as the list of departments and their groups, list of locations and service areas.
Certifications	Undertake certification related actions for credentials and other information.



Dashboarding approach proposed by system integration experts at Avancer Corporation puts emphasis on centralized management of apps and IAM system(s)

Application dashboarding for healthcare application is a way of bringing together apps under one umbrella

The total number of data breaches reported till September 2017 to the Department of Health and Human Services' Office for Civil Rights (OCR) reached 272 incidents, with more than 4.6 million patient records being exposed or stolen. Management of EPIC systems in its current capacity is expensive; IT team of five resources for EPIC management spends about $500K annually only on human resources in making the system run smoothly.

Furthermore, the loss in terms of productivity and workflow inefficiency is not accounted for. Connection of IAM with healthcare apps facilitates managers and audit team members to take certification related actions such as certifying positions, credentials and other information or revoking positions. This helps to ensure closed loop remediation for any violations that maybe found in EPIC related system access.

IAM-EPIC integration helps to improve usability and adoption of apps and integrating them with existing IAM platform. It strengthens IT system by easing workflow through SSO for end-users, simplifies administration through centralization, automates user identity to ensure right access and betters control with an ability to govern access to the apps.

Customer Identity and Access Management (CIAM) for General Data Privacy Regulation (GDPR) Compliance

Catalyst for connecting marketing, business and security teams to form strong consumer engagement systems.

Learn More by Connecting with our Advisors
Email: info@avancercorp.com
Call: +1 (609) 632-1285

Avancer
Simplified IT Security

MFA VS. ADAPTIVE AUTHENTICATION: WHAT SHOULD YOU CHOOSE?

Arun Mehta

An absolute nightmare for an IT security professional is when protected data is accessed by unauthorized personnel. While passwords, firewalls and other basic protection methods are becoming easily 'hackable', organizations are seen shifting towards Multi-Factor Authentication (MFA), which includes voice callbacks, SMSes and OTPs, to combat the issue. MFA has been able to minimize associated risks to certain extent and has become a necessity. However, for strategic security management, the way ahead for enterprises is to protect their large data by implementing adaptive authentication.

MFA is the present, while adaptive authentication is the future. While MFA could help in tackling the security issue in the present scenario, enterprises looking at a long-term perspective need to focus on integrating

Adaptive authentication adds a layer of security, helping companies protect their data from unauthorized access, while allowing easy access to the system.

adaptive authentication. For instance, establishing the identity of a user through a step-up OTP might not be the most ideal solution, as it is device-possession dependent. In such a scenario, adaptive authentication takes user and behavior context to the next level. It is based on a matrix of variables that provides a risk profile of a user, and based on this risk profile the system generates additional authentication process before the user is allowed access. While MFA could be a part of adaptive authentication process, the latter is much more intuitive and real-time, with factors such as knowledge-based questions, geo-location and identity assurance making the authentication process robust.

SIMPLE MFA IS NOW MOVING AWAY, PAVING WAY FOR ADAPTIVE AUTHENTICATION.

MFA is process driven, while adaptive authentication is dynamic and real-time. MFA follows a set-pattern and has certain processes to be followed, with regards to adaptive authentication, the end-user is an integral part of the security process. Elements such as out-of-band (OOB) authentication through SMS or email, and knowledge-based authentication help in creating a dynamic security system, which is difficult to hack. For instance to control access of the employees to their floors or designated areas, the staff is provided with badges or biometrics that has only conditional access. In this scenario, accesses might be intuitive in nature and may deny entry to anyone based on attributes, such as frequency of their visit to a particular place or area.

It is also observed that progressive organizations are now discouraging use of MFA processes and not letting members or employees enter OTPs or passwords for executing even simple tasks. Sample this, a prominent retail shop introduced membership renewal process which is based on adaptive authentication—the system validates a customer through certain checks and balances—which is based on users' shopping behavior in the past, along with other details.

MFA is usually password-dependent, while adaptive authentication follows more stringent identity verification. Adaptive authentication helps in setting up additional identity verification through various channels,

THE MOVE IS TOWARDS BEHAVIORAL ASPECTS OF USERS RATHER THAN DEVICE-BASED SIMPLE PASSWORDS AND OTPS.

including integrating hardware solutions such as biometrics. Although, biometrics would mean additional cost, it is worth the investment. Passwords are seen as the weakest link in any security system and backing it up with additional authentication, especially biometrics, ensures authorized access to the system. Furthermore, biometrics protects or minimizes risks against data breaches, cyber-attacks and fraud.

Although companies are often seen to shy away from integrating adaptive authentication due to the perception of budget hike, there are companies that are providing these products at an economical cost, with even the implementation pricing at a lower spectrum. Given the number of breaches that are occurring these days, safeguarding assets from theft should be the prime prerogative of organizations rather than saving cost.

IT IS BETTER TO INVEST IN STRINGENT VERIFICATION METHODS THAN FACE POSSIBLE DATA BREACH ISSUES.

Adaptive authentication approaches access in a more intelligent way and aims at creating a fool-proof mechanism by layering risks checks through various attributes such as behavioral biometrics, geo-fencing, directory lookups, etc. The process of adaptive authentication discourages misuse of valid credentials, with access anomalies and failed authentication attempts being recorded and escalated on a real-time basis.

BRINGING APP INTELLIGENCE THROUGH ENTERPRISE APP WAREHOUSE

Asha Dey

As the need and acceptance for 24×7 connectivity grows in both personal and professional lives of burgeoning corporate professionals all over the globe, a large number of organizations are moving towards enterprise-wide mobility. Such a business model requires intelligent application stores with a strong suite of functionalities.

Mobile platforms to support corporate app warehouse structure can be looked at.

This can be achieved by provisioning of applications for a particular user through an identity management platform. However, for multiple reasons that relate to security, control and performance, it's absolutely necessary that enterprise architects should first think about creating an enterprise app warehouse, which is available to users based on their roles and responsibilities.

An enterprise app warehouse can manage corporate sanctioned apps on all connected devices–PCs, cell-phones, tablets or any other

procurement strategies. The idea therefore is to distribute an enterprise oriented application through app stores like Google, Apple or an enterprise app store within mobile platforms. This will create a new enterprise marketplace inside an existing marketplace.

Setting up functionalities and app related capabilities is possible with correct approach.

Enterprise app store application needs to be built and deployed through public app stores. What this means is that platforms like Apple, Google or Microsoft need to set certain policies where organizations can discretely and securely distribute apps to their employees while taking advantage of the services the store provides.

Dedicated profiles need to be created for the app store, which will share login credentials and SSO capabilities between the apps within the enterprise app store. The apps or services distributed through these channels should then get synced to ensure they are encrypted or SSO compliant, thereby making it easier for IT admin to monitor usages and accesses. Furthermore, from an IdM system, the provisioned apps will be able to take advantage of features like geo-fencing and time-based usage and the admin should be able to lock these apps based on the time, frequency or the location of an employee. For e.g. employees won't be able to access these apps over a weekend or in a country of conflict to protect sensitive data.

When a user is off-boarded, enterprise app store will no longer exist for that specific user, applicable for cases where mobiles are being stolen or lost, and helpdesk can revoke access. Also possibilities like remote wipe and account removals should be fairly easy without physically wiping or confiscating the devices. The good news is companies such as Blackberry, Google and Apple are already partnering with established defense companies, banks and IT giants to make this a reality.

The app culture created fear in the minds of security professionals, but it was not long before a fix was found. The lunch table discussion is now no more about the problems, but the possibilities surrounding enterprises using app warehouse. So, don't be afraid about app-synchronized IT environments, there is already an app (store) for businesses to capitalize on!

CASE STUDY

TAKING MANAGED IAM SERVICE TO A HEALTHCARE SETTING

A leading medical center engaged Avancer to provide production support for Oracle Identity Management platform. The association was sought for continuity of Healthcare IT System and creation of continued, error-free IdM process.

About the client

- Ranked first in Chicago metro region and Illinois
- Ranked eighth in the nation, according to the U.S. News & World Report (2016–17)
- Honor Roll of America's Best Hospitals ranks the client 13 out of 16 clinical specialties offered

Challenges faced

The client struggled with incident, problem management and resolution of automated systems. **The IT department at the client's end sought support in production app service maintenance and service level guarantees achievement.**

The client reached out to Avancer for IAM managed services support as system and app administration services and enhancements were required to be conducted through trusted source, proper integration and delivery support.

Solutions proposed by Avancer

To this effect, Avancer got into the picture to provide support services for the following technologies, tools and capabilities:

- Oracle Identity Manager
- Oracle BI Publisher (reporting engine for OIM)
- Oracle Web Logic Environments & Connector Server
- Multiple People Soft Modules
- Multiple Active Directory Domains Management
- Active Directory Password Synchronization

Solution implementation and managed IAM support offered by Avancer

Avancer extended an end-to-end implementation of solutions and management of the services delivery. The project was undertaken through a team of highly focused technical resources, providing support against 24×7 workflow-related processes.

The support steered through basic parameters of engagement, including:

- Management of communication between stakeholders and participants

THE TECHNICAL EDGE OFFERED BY AVANCER'S RESOURCES GUIDED THE CLIENT TOWARDS BEST PRACTICES. THE CLIENT HAS BEEN ABLE TO GET CLEAR AND DEMONSTRABLE VALUE IN THE SERVICES THROUGH MULTIPLE ENGAGEMENTS WITH AVANCER.

- Preparation and review of monthly reports related to logs, accesses and identities
- Attend to Service-Level Agreements (SLAs) based governance of identities and their access

Avancer offered resource support to the client, including service level manager and technical resources. The service manager became the escalation point for all IAM related glitches, monthly reporting and reporting issues with Avancer's team.

The engagement was aimed at creating IT systems to accelerate engagement of business, technology and operations (work-flows). The focus was not just on service delivery but also on training client's resources and knowledge sharing for creating a self-sustaining module.

For a scalable IT system in a healthcare setting, application support processes, upgrades and management play a crucial role in creating agile systems.

APPROACH OF MANAGED IAM SUPPORT OFFERED BY AVANCER

Focus on on-boarding client's team through engagement and planning. Establish a clear communication and reporting plan to bring in transparency in work processes and responsibilities.

Parallel transition of systems and networks required for Avancer's access. This enables Avancer's team to collaborate with subject matter experts and provide desired services to the client.

Outline the scope to achieve a steady state of managed IAM operations. Services outlined under Avancer's responsibilities were broadly related to knowledge transfer to client's resources.

Review of service delivery based on a comprehensive assessment. A set of activities and review of current versus estimated volumes occurs at a set time interval during the term of engagement.

Avancer's IAM Healthcare Solution takes medical facilities closer to deliver highly personalized, good quality, compliant and secured medical care.

Connect with our experts at info@avancercorp.com for more information.

Organizations often find themselves in dead-end when it comes to integrating identity and access technology because of lack of extensive know-how. IAM program adds business value by reducing the cost of IT systems' management, and thus highly specialized know-how and support has to be provided to enable efficient IAM infrastructure.

In a healthcare organization, compliance to regulation for securing identity of users, information of patient health records and managing applications has to be in parallel with IT functions. IT security departments can bring managed support resource(s) to get equipped for future needs, become agile and scalable and overcome short-term hiring deficiencies.

The technical edge offered by Avancer's resources continually assists client in guiding towards best practices. The client has been able to clear and demonstrable value in the services through multiple engagements with Avancer.

PARTNER STORY

SSH KEY MISMANAGEMENT: A GROWING THREAT PROFILE FOR YOUR BUSINESS

Team SSH Communications Security

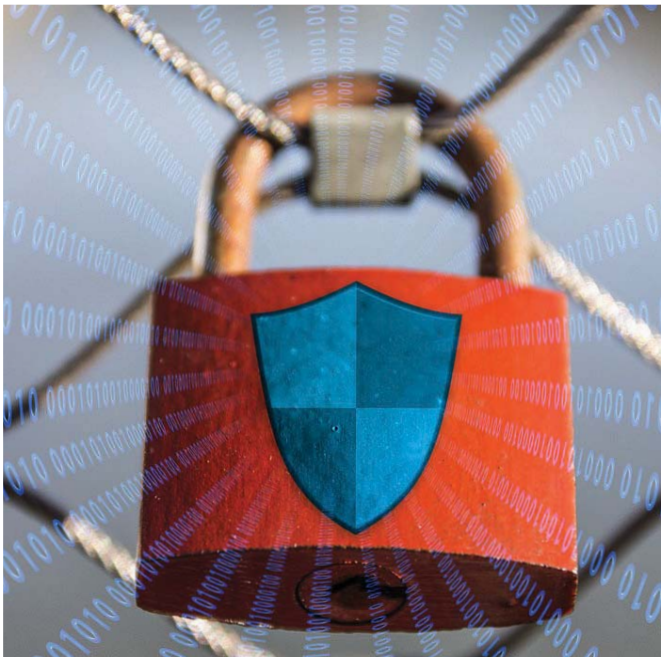
Information security starts with **'Who'** has **'What'** access to systems and data and **'How'** that information is being accessed. Keeping in perspective the important data routed via SSH, there are a few important questions for IT department heads to ponder over:

- Can the IT team detect the use of anunauthorized SSH key on the enterprise network?
- How does the organization mitigate risks wherein SSH keys do not expire?
- What kind of security systems are implemented by IT security folks for SSH key integration within cloud environments?

Enterprises have been using SSH keys to access IT systems and to securely transmit data. However, they often neglect management of SSH keys that require robust access management and identity linked protection. SSH keys have often been overlooked in identity and access management planning, implementation and audits. In a scenario where SSH key and IAM technology are not integrated, when a user gets created, management of SSH keys related to granting access is done manually without any oversight or controls.

The SSH keys grant access to enterprise resources such as production servers, databases, routers, firewalls, disaster recovery IT systems, databases including financial information, payment channels, intellectual property and sensitive information. Furthermore, SSH keys

SSH KEYS SYNCHRONIZED WITH IAM RESOURCES BRING CUSTOMERS PRECISEPRIVILEGED ACCESS TO KEEP SSH KEY MANAGEMENT FROM BECOMING AN UNCONTROLLABLE CYBERSECURITY RISK.



When it comes to auditing SSH keys, most organizations do not even have basic information such as the number of keys running wild across the enterprise, the rotation of keys, or provisioning issues such as employee termination.

often grant access to privileged accounts at an operating system level. In many cases, the SSH key is utilized at the command line level within an IT system.

Many organizations report varied issues related to SSH keys, including no record of keys, no provisioning or termination processes for users. Most often, system administrators self-provision permanent key-based access without governance policies, processes or oversight. The mismanagement is believed to be systematic in nature.

Most large organizations have accumulated a great number of SSH keys within their environments. Now they are finding enterprise-wide deployment issues in Secure Shell management. These issues have been overlooked due to lack of governance for years, encouraging misuse of SSH keys, violating corporate access policies and opening backdoors for cyber criminals.

SSH keys synchronized with IAM capabilities bring customers better access processes to keep SSH key management from becoming a cybersecurity risk that may get out of control. It also widens the security umbrella and strategically aligns cyber security considerations.

This calls for auditing of SSH security related vulnerabilities. As there has been a greater understanding of dealing with SSH security issues, specific SSH key related challenges can be curtailed. This will help in creating a reliable access management mechanism and preventing keys from being used to circumvent controls that exist for SSH keys.

What's making hackers surpass SSH keys?

Lack of control over SSH keys allows hackers to infiltrate through existing perimeter layers of security.The hacker's use of SSH to infiltrate your enterprise is like giving away the keys to the kingdom.

Hackers can purchase SSH keys on the dark web. However, the question is how the keys got beyondenterprise walls and to dark web. Attribute it to system inadequacies that were not thought of by companies at the time of setting NIST compliant IT system. Further, despite being used to provide the highest privileged access to administrators, SSH keys are poorly managed by most organizations.

SSH keys often are overlooked in IAM planning, implementation and audits. Given the vulnerabilities associated with SSH keys, it is crucial for businesses to keep a close watch on unauthorized privileged access, lateral movement across the enterprise and unmonitored exfiltration. A robust program of SSH key management can prevent major and costly cybersecurity breaches.For more information on SSH key management,experts at Avancer can discuss specific solutions. Write to us at info@avancercorp.com.

ssh communications security

SSH
USER KEY
MANAGEMENT

ACCESS
COMPLIANCE
MANAGEMENT

PRIVILEGED
ACCESS
MANAGEMENT

STOP. THINK. GOVERN.
TRUSTED ACCESS

VISIT US
www.ssh.com

IMPORTANT ASPECTS OF IT SECURITY ONE SHOULD NEVER IGNORE

Information technology is not just about computing and networks, there is more to it—including security, risk management, access & identity dynamics, cloud, hybrid systems, threat intelligence, etc. Here are important aspects of IT security that CISOs and Enterprise S&R Professionals should not ignore in order to achieve complete IT security.

SAVIYNT

"Saviynt enables enterprises to protect data, applications and infrastructure for the Cloud and Enterprise in a unified platform. With built-in support for advanced risk analytics, real-time event based protection and continuous compliance management, Saviynt helps customers address complex security and compliance needs."

SACHIN NAYYAR
CEO OF SAVIYNT

IDENTITY GOVERNANCE & ADMINISTRATION
SECURITY MANAGEMENT

FOR CLOUD | ENTERPRISE

- Risk-based Identity Management
- Usage & Risk Analytics
- Continuous Controls & SOD Management
- Privilege Access Management
- Data Security

- devSecOps and Secure CI/CD
- Real-time Cloud Protection
- Customer Identity Management
- Controls Exchange

AVAILABLE FOR:

Office · ORACLE · Microsoft · salesforce · workday · amazon web services

Microsoft Great Plains Business Solutions · Cerner · Epic · SAP · PeopleSoft · box

ONE STOP SOLUTION FOR ALL ENTERPRISE IT NEEDS

Empower your IT System with streamlined and smooth operations, powered with 360-degree IAM capabilities, IT Security and Big Data Management.

OUR APPROACH

1. **PROBLEM IDENTIFICATION**
2. **ROADMAP CHARTING**
3. **KNOWLEDGE TRANSFER**

SYSTEM INTEGRATION | GREENFIELD PROJECTS | SOLUTIONS UPGRADES
SOLUTIONS MIGRATIONS | TCO OPTIMIZATION | BUSINESS PROCESS (RE)DESIGNING

Learn More by Connecting with our Advisors
Email: info@avancercorp.com
Call: +1 (609) 632-1285

Avancer
Simplified IT Security