SECURING IDENTITY AND ACCESS MANAGEMENT IN THE DIGITAL ERA

In October 2018, 30 million Facebook users lost their personal data to hackers. In the same month, it was reported that over 500,000 Google+ users had their data exposed to hackers. The list of such hacks which happened in the preceding12 months or so is long and exhaustive. This speaks volumes about the danger of **consumer information and identity theft** for carrying out financial fraud or other frauds on employment, taxes, loan/lease, etc.

Infosys®
Navigate your next

Greyhound Research, a leading analyst firm, estimates that over one-third of the US population was impacted by identity breach in 2017 and this number is expected to increase by 25% in 2018. A separate study by Greyhound further confirms this trend - while 78% of the respondents, chiefly large enterprises with a global presence, said they deployed an **Identity and Access Management (IAM) tool**, over 80% of them confirmed lack of confidence in their ability to manage identities and personal information in a constantly evolving threat scenario. Interestingly, over 62% of these organizations still rely on manual controls to audit and manage user access to systems and other sensitive corporate resources.

CHECKING UNAUTHORIZED ACCESS

Infosys has consistently observed these trends across most of our client base. One of our key findings is that organizations face the most **IAM threats from unauthorized access** by internal and external agents. This happens due to:

- **Proliferation of point solutions,** designed to solve one specific problem, over a period of time
- **Low incentive to revamp systems** due to high upfront investments and total cost of ownership
- **Lack of seamless access** to applications on cloud and on premise, across devices and locations

A large banking client was facing many of the above problems due to their complex global IT environment. With over 1,000 log files collected on a daily basis from multiple sources, the organization had massive **log monitoring requirements** of privileged account activities in SOX (a compliance requirement for publicly-traded companies to have internal controls and procedures for financial reporting) and non-SOX applications across different platforms, applications, and databases. To make matters worse, the client performed log correlations and detection of violations in user activity manually, through a **sampling-based process**. This led to increased costs, a lower rate of **fraud detection**, and breaches in SLA.

Organizations battling similar IAM issues must take an all-encompassing view covering the entire security ecosystem and stakeholders, including customers, employees, partners, security administrators, cloud-hosted applications, enterprise applications, and data center administrators, and consider **solutions with scalable architecture** to allow for growth in user base and applications.

AUTOMATION TO THE RESCUE

We set up an **Enterprise Log Monitor Automation solution** for our banking client to efficiently handle log aggregation and event correlation of privileged user logs, and reporting of violations. We used server and client architecture module to **define policy and procedures** for the tool to run log monitoring and correlation across a host of platforms, database, and applications. This also enabled **proactive and reactive analysis** to identify (past or potential) breaches or fraud.

The solution worked within the client's landscape of heterogeneous IAM applications, database, and platforms. It **automated follow-up and investigation** of access breaches/violations where unauthorized access or inappropriate activity was identified. It also had a p**ortal for displaying the automation statistics** and handling end users' responses.

Our solution not only helped the client **save 50-60% of manual effort**, it also helped them save on license cost, **improved security governance**, and ensured better adherence to SLAs and reduction in manual errors. A dedicated 24x7 team which manually processed log correlations through sampling was replaced with the Infosys Enterprise Log Monitoring solution powered by **Robotic Process Automation** (RPA), leading to almost 100% of the logs being processed, **improving accuracy.** This not only allowed **timely detection of violations**, but also enabled **better enforcement of standard policy** at all levels.

SECURING IDENTITY AND ACCESS MANAGEMENT IN THE DIGITAL ERA: THE FIVE TAKEAWAYS

1 **Use** integrated security solutions instead of monolithic point solutions

2 **Enforce** policy-driven access control for all organizational resources

3 **Audit** using analytics to identify user behavior and profile and access violations

4 **Automate** monitoring processes to ensure proactive and reactive analysis of identity breaches or fraud

5 **Define** policy and procedures to run log monitoring

BIG LEARNING:

As organizations increasingly use new applications, databases, and APIs, the risk and complexity of securing and managing identities is multi-fold, pressing organizations to take a fresh approach to IAM in a highly regulated SOX regulatory environment. Organizations need to stop viewing IAM as an IT problem and look at it with a strategic lens. A sound IAM strategy in today's environment is imperative not only to help organizations reduce overall business risk but also deliver enhanced user experience.

WE DID THIS FOR THEM.
WE CAN DO IT FOR YOU.

To learn more about identity and access management, reach out to us at askus@infosys.com

For more information, contact askus@infosys.com

Infosys®
Navigate your next