Persistent

Top 10 Legacy IGA Challenges

Resolved by Next Generation IGA Solutions

Risk

Difficult to Manage IT Compliance

Discrepancies between processes developed over the years, fail compliance standards. E.g. rubber stamping of access, poor SOD management etc.

Vulnerable to Cyber Attacks

Research shows, more than **74%** data breaches start with privileged credential abuse[1].

Not Cloud-Enabled

83% of enterprise workloads will be in cloud by the end of 2020[2]. Limited deployment and infrastructure architecture options.

Poor Visibility in User Access

No usage-driven analytics or risk insights. Identity federation is just not enough.

Operational Efficiency

Lack of Reporting Function

Restricted only to connected systems. Limited audit capabilities.

Longer Upgrades

Heavy customizations. Thus, require **12 – 18 month long deployments** for initial phases with limited applications.

Lack of Automation

Takes **5x** more time to execute processes than automated IAM.

Slowdown Digital Business Initiatives

Require custom coding with out-of-the-box integrations with modern resources and applications.

TCO — Hardware, Support & Maintenance

Higher hardware $$ investment. Lack of support for EoL legacy `platforms. Requires timely maintenance. 1 hour of outage can cost **$50,000** or more.

UX

Poor User Experience

Doesn’t support chatbot integration, inline consultation, management of vendors, and non-human identities with ownership.

REFERENCE:

1. Privileged Access Management in the Modern Threatscape.
   www.centrify.com/resources/centrify-privileged-access-management-in-the-modern-threatscape-2019/

2. Cloud Vision 2020: The Future of the Cloud Study.
   www.logicmonitor.com/resource/the-future-of-the-cloud-a-cloud-influencers-survey/