DATASHEET

Identity Manager

Take the risk out of enterprise identity and access management

Benefits

- Govern access to on-premises, cloud and hybrid resources from request through fulfillment for users and data
- Reduce risk by ensuring users have only the access they need
- Satisfy audit and compliance initiatives with attestation/ recertification policies
- Put access decisions where it belongs — in the hands of the business
- Build on existing investments and infrastructure and grow from there

Overview

Traditional identity and access management (IAM) frameworks are expensive to build and time-consuming to implement and maintain. They are burdens on most IT departments as IT typically handles all user identity lifecycle management. To meet the varied IAM needs of different business units, IT often works with a siloed set of narrowly focused tools and security policies and relies on manual processes for enforcement. This leaves the environment vulnerable and increases risk, and makes it difficult to meet SLAs.

You can increase productivity by giving users access to the data and applications they need to do their jobs—and nothing more.

Mitigate risk, secure data, meet uptime requirements and satisfy compliance by giving users access to data and applications they need. Now, identity and access management (IAM) can be driven by business needs, not by IT capabilities. With Identity Manager, you can unify security policies and satisfy governance needs — today and long into the future.

You can do this while improving business agility today and in the future with a modular and scalable IAM solution.

MITIGATE RISK. CONTROL ACCESS. GOVERN IDENTITIES. SECURE DATA.

Now, identity and access management (IAM) can finally be driven by business needs.

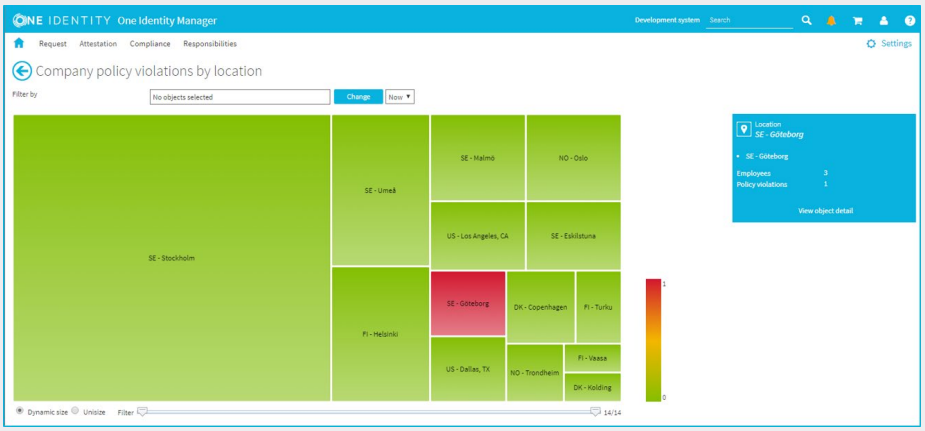

Figure 1. *Governance Heatmap enables quick drilldown on policy violations*

Features

Risk reducer

Make better security decisions by combining security information and policies from multiple sources to reduce exposure and eliminate information silos

Cloud Connect

Extend investment in identity governance beyond on-premises applications to hybrid and SaaS applications with an add-on cloud-based, managed-service offering that builds upon One Identity Manager (7.1 or later)

Governance 360

Provide auditors with detailed, real-time governance reports that includes information about what resources are in your environment, who has access to them, when and why that access was granted and terminated.

Provisioning done right

Eliminate manual mistakes by automating provisioning to any system, platform or application on premises or in the cloud. Extend provisioning to enterprise applications such as Exchange Online, SharePoint and Oracle E-Business Suite.

Access done right

Enhance security by providing employees, contractors, partners, customers, students, alumni, constituents and patients with only the access they absolutely need - nothing more and nothing less.

Compliance Now

External regulations? No problem. Internal policies? No problem. Get the complete visibility you need while meeting the demands of all the other groups.

Data Governance

Get control and visibility of your data.

Self-service access portal

Enabled the business to save time and help themselves. Reduces IT effort via a customizable online intuitive "shopping cart" portal. This enables users to requests access to security assets such as physical assets, groups and distribution lists and control access rights and permissions for their entire identity lifecycle with predefined approval processes and workflows.

Privileged Access Governance

Unified governance approach for all employees, regardless of their role and level of access. Users can request, provision and attest to privileged and general user access within the same console.

Access Review dashboard

Schedule on-demand or routine attestation and display the status of group or distribution list in a clear, concise dashboard view; and enables you to produce detailed reports for discovery, as well as to satisfy compliance.

Password reset

Reset user account passwords and set user-policy preferences that mirror organization's password rules and requirements. Enables multiple password policies depending user roles.

Multi-factor now

Enable two-factor authentication through Identity Manager with integrated deployment across enterprise applications and integrated with One Identity Starling Two-Factor Authentication (2FA).

Scale up and out

Build on your existing investments and infrastructure you already have and grow from there. Migrate your current legacy platform by integrating a modular and integrated solution into your "traditional" IAM frameworks as you progress to a single, consistent IAM strategy.

System Requirements

For a complete list of system requirements, visit https://support.oneidentity.com/identity-manager/8.0.1

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com