SENSORY

IDENTITY & ACCESS MANAGEMENT

Users and their identities are among the most vulnerable links in a network, and controlling access to corporate assets has become a critical challenge. Identity and access management (IAM) technology has emerged from the back office to become a key enabler for the digital world, and it involves more than just governing employee access.

TAKE CONTROL OF CORPORATE ASSETS

Sensitive data is now being distributed across locations, devices and repositories. It’s essential to provide secure access to resources across users—including employees, partners and customers—who are accessing IT environments wherever, whenever and however they choose.

IAM strategies need to be able to accept external identities via federated connections, apply risk-based authentication methods to ensure strong authorization across dynamic ecosystems, and provide insight and control over how customers, employees and partners interact with applications, data and services.

OUR APPROACH TO IDENTITY & ACCESS MANAGEMENT

Sirius recommendations are rooted in decades of experience gained in the field, as well as customized testing in our state-of-the-art Technology Enablement Center. Our Identity & Access Management solutions and services generate the intelligence about identity and access activities you need to increase your knowledge of broader security events, and advance your overall security posture.

We partner with the leading IAM solution providers and work with you to select the right solution for your environment so you can strike the right balance between user experience and security. We offer expert professional services to help you manage, optimize, secure and transform your business.

• Identity Governance & Administration (IGA)
• Privileged Access Management (PAM)
• Single Sign-On (SSO)
• Risk-Based Multi-Factor Authentication (MFA)
IDENTITY GOVERNANCE & ADMINISTRATION (IGA)

Ensure that only the right people get access to the right resources, at the right times, for the right reasons. IGA solutions manage identity and access for users across multiple systems by aggregating and correlating disparate identity and access rights data to enhance access control. The aggregated data serves as the basis for core IGA functions, including identity life cycle and entitlements management, access requests with approval workflows, access certification, and role-based or policy-driven administration, fulfillment, auditing, reporting, and analytics.

PRIVILEGED ACCESS MANAGEMENT (PAM)

Actively manage access to information. PAM controls help organizations restrict privileged access within an existing Active Directory (AD) environment. PAM accomplishes two goals: re-establishing control over a compromised AD environment by maintaining a separate bastion environment that is unaffected by malicious attacks, and isolating the use of privileged accounts to reduce the risk of those credentials being stolen.

SINGLE SIGN-ON (SSO)

Streamline access to accounts. SSO helps organizations manage account access and mitigate the problems caused by the growing number of applications and logins. One set of login credentials is used to access multiple accounts—users no longer have to struggle with remembering multiple passwords, and administrators can set rules for that password, control access, and remediate vulnerabilities more easily.

RISK-BASED MULTI-FACTOR AUTHENTICATION (MFA)

Make access hard for hackers, but easy for users. Compromised credentials are a common means of unauthorized access. MFA helps prevent attacks that leverage stolen passwords, but organizations often deploy it in a way that can leave users feeling harassed. Risk-based, adaptive solutions help verify that users are who they say they are by automatically evaluating the access risk, and requesting additional authentication only if the risk warrants it. This helps to avoid user frustration, and makes verification easier by providing them with a variety of authentication choices such as push notifications, biometrics, SMS and more.

SIRIUS IDENTITY & ACCESS MANAGEMENT SERVICES

<table>
<thead>
<tr>
<th>Discover</th>
<th>Assess</th>
<th>Consult/Design</th>
<th>Architect/Implement</th>
<th>Optimize/Manage</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM Workshop</td>
<td>IAM Assessment</td>
<td>IAM Strategy &amp; Roadmap Development</td>
<td>Solution Design &amp; Deployment</td>
<td>Solution Optimization &amp; Tuning</td>
</tr>
<tr>
<td>Cloud Workshop</td>
<td>User Rights Review</td>
<td>Remediation Plan Creation</td>
<td>Privileged Access Management</td>
<td>Managed Authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TEC: Evaluation, PoC, Bake-Off</td>
<td>Access Governance</td>
<td>IAM &amp; PAM On-Demand Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Single Sign-On</td>
<td>Managed Application Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Managed Process Services</td>
</tr>
</tbody>
</table>

For more information, please contact your Sirius client executive, visit siriuscom.com, or call 800-460-1237.