THE SIRIUS SECURITY APPROACH

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.

IDENTITY & ACCESS MANAGEMENT

TAKE CONTROL OF CORPORATE ACCESS

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.

With the disappearance of the traditional security perimeter and widespread adoption of cloud computing, sensitive data is being distributed farther than ever across locations, devices and repositories. Organizations need to provide secure access to resources across a globally connected web of 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.

SIRIUS | SECURITY

www.siriuscom.com
800-460-1237

From current state discovery to program management, Sirius helps you mature your organization's identity and access management capabilities.

Key focus areas include:

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.

Sirius provides technology bake-offs and customized proof-of-concept testing in our TEC. We help you consider your organization's current and future requirements, and choose a solution that has the right level of flexibility and capabilities to meet them.

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.

Sirius helps you evaluate leading PAM controls and identify, design, deploy and tune the solution that best fits your needs. We work with you to manage the identities and privileges of an increasingly diverse group of users that use a multitude of devices to log into systems both inside and outside the enterprise.

Single sign-on (SSO)

Streamline access to accounts. SSO helps organization 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.

Sirius partners with the leading providers of on-premises and cloud-based SSO solutions. We help you evaluate, design and deploy SSO controls that align with your business goals, and incorporate multi-factor authentication to reduce risk.

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 is often deployed in a way that leaves users feeling harassed. Risk-based, adaptive solutions help verify 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 frustrating users, and also makes it easier by providing them with a variety of authentication choices such as push notifications, biometrics, SMS and more.

We partner with the leading providers of risk-based authentication solutions, and work with you to test and deploy the right solution for your environment so you can strike the right balance between user experience and security.

Please contact your Sirius client executive for more information, visit **siriuscom.com/security**, or call 800-460-1237.

SOL_IDACCESSMGMT January 2020