Microsoft Security Services

AGENDA

- Sirius & Microsoft Partnership
- Data & Advanced Analytics
- AI, Machine Learning & Chatbots
- Security, Identity & Access Management
- Digital Transformation
- DevOps
- Workplace Modernization
- Cloud Storage
- Infrastructure as a Service

Sirius & Microsoft Partnership

Gold
**Microsoft
Partner**
Microsoft

Sirius has an established methodology for moving clients to the cloud.

Business solutions that span:

› Artificial Intelligence
› Cloud
› Customer Engagement
› Data & Analytics
› DevOps
› Digital Transformation
› Enterprise Content Management
› Machine Learning
› Security

4,500+
earned cloud certifications

65+
security experts

15+
Office 365 skills

Success in Artificial Intelligence (AI) on Office 365 and Azure

75
data & analytics engineers

Microsoft expertise in:

- Azure
- Azure DevOps
- Microsoft 365
- Artificial Intelligence
- Data Platforms

- Power Platform
- Security & Compliance
- Identity & Access Mgmt.
- Endpoint Management

100+
DevOps engineers

FIVEOUT
A SIRIUS AGENCY

Sirius' very own FiveOut agency is focused on Digital Strategy, Design, Experience, Branding and Marketing for our clients

WHY SIRIUS FOR MICROSOFT SECURITY SOLUTIONS?

SIRIUS

Broad skills

Sirius delivers technical expertise in storage and data management in legacy, public and hybrid cloud.

Technical caliber

We know how to use the technology. Sirius has four industry-certified and designated masters.

Earned certifications

Our experts have 4,500+ earned certifications.

Always involved

We serve on an advisory council for every backup we do.

All That Data is a Major Security Risk

In the first half of 2017, over 10 million data records were stolen every day.

DATA RECORDS LOST OR STOLEN
FIRST HALF OF 2017
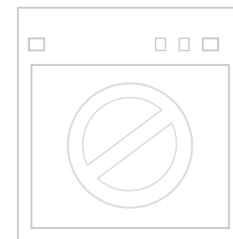
10,507,550
EVERY DAY

437,815
EVERY HOUR

7,297
EVERY MINUTE

122
EVERY SECOND

- Gemalto Breach Level Index, First Half of 2017

MICROSOFT IDENTITY MANAGER

- Synchronize identities between directories, databases, and applications
- Self-service password, group, and certificate management
- Increase admin security with policies, privileged access, and roles
- Thwart identity theft
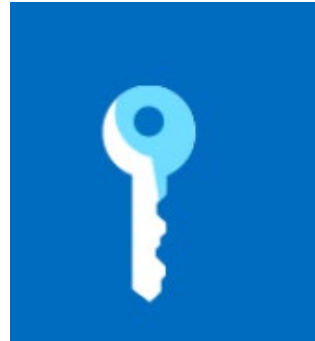
Microsoft Identity Manager Benefits

Common Identity

Protect Data

Enable Users

Unify Access

Enterprise-level Identity Protection

SIRIUS

81%
of all hacking-related breaches use compromised credentials[1]

15%
of phishing attack victims fall victim a second time[1]

95%
of phishing attacks that led to a breach were followed by some form of software installation[1]

75%
of individuals use **only** 3 or 4 passwords across all of their accounts[2]

Safeguard and manage identity: Protect identities and proactively prevent compromised identities from being abused.

Detect and respond to identity-based threats: Manage cloud activities more securely.

Protect against password attacks: Replace passwords with strong two-factor authentication, and better protect credentials against persistent threats.

[1] Verizon 2017 Data Breach Investigations Report (ref. P11 of Security Playbook)
Security Week Survey (ref. P11 of Security Playbook)

Identity and Access Management
with a **Azure Active Directory (Azure AD)**

- An integral component of **Office 365, Azure and Enterprise Mobility + Security**

- Manage user identities and create intelligence-driven access policies to secure your resources

- Centralizes identity and access management to enable deep security, productivity, and management across devices, data, apps, and infrastructure

- Built to work for apps in the cloud, on mobile, or on-premises

Most businesses struggle with:

- Lacking the security talent to get ahead of security and compliance risks
- Unable to identify, assess, and mitigate security risks
- Unfamiliar with security best practices and the overall threat landscape
- Confused with many offerings and features
- Unable to correctly respond to compliance obligations in a timely fashion

Sirius Security Specialties

- Infrastructure
- Data & Application
- Intelligence & Analytics
- Threat & Vulnerability Management
- Identity & Access Management
- Program Strategy & Operations

Sirius Zone Defense

NEXT STEPS: SECURITY, IDENTITY & ACCESS MANAGEMENT
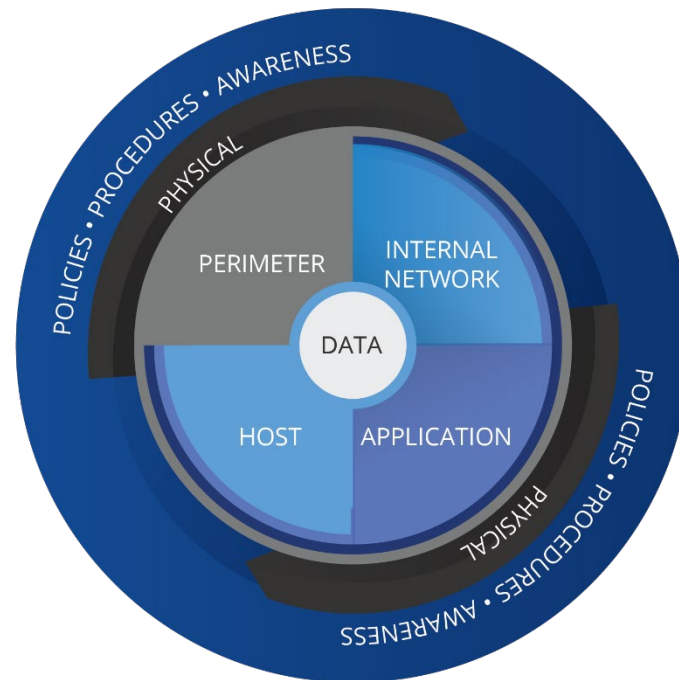
Sirius Security Architecture Review

Azure Active Directory Solution Alignment Workshop

Security & Management

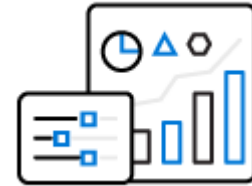Meet your data protection needs while delivering the best user experience

- Supports your diverse mobile ecosystem
- Achieve IT efficiencies in the cloud
- Protect data with or without device enrollment
- Deploy and success with our help

Microsoft Intune Features

Help your people
stay productive
and secure

Get unparalleled
Office mobile app
management

Select from a variety of
management scenarios

Workshop to understand your project objectives, challenges and success criteria for an Intune deployment

Proof of value to help end-users familiarize themselves or compare to your current MDM solution

Run technical workshops to address specific concerns

Workplace Modernization

- Windows 10
- System Center Configuration Manager
- Enterprise Mobility + Security

Windows 10

- Enhanced security platform
- Built-in SDDC capabilities/Azure compatible infrastructure
- Cloud-ready application platforms
- Mainstream support (e.g., patching, incident management)
- Ensures flexibility and agility for new applications

System Center Configuration Manager

- Empower user productivity by enabling employees to access corporate applications from anywhere
- Simplify administration with improved visibility and enforcement options
- Unify your IT management infrastructure and streamline operations
- Built to work with Windows 10

Microsoft 365 Security and Compliance Scenarios

Enterprise-Level Identity Protection

Implement and manage cloud identity and access. Audit and mitigate use of cloud apps.

Control and Protect Information

Assess and classify data. Implement and manage information policies and procedures.

Proactive Attack Detection and Prevention

Perform security assessment analysis, migrate and deploy security solutions and provide managed security services.

Regulatory compliance

Help with increased demands of regulators and legal authorities in every country in which they operate.

SECURITY SOLUTION ALIGNMENT WORKSHOP

- *Security Planning:* Assist you in evaluating how the Microsoft security capabilities in the Microsoft 365 product sku will meet *your* security requirements, and achieve your desired business outcomes.

- *Goal:* Via a review of your current environment and tools, understand any gaps and create a deployment plan for the Microsoft capabilities in consideration.

- *Deliverable*: Planning document including technical preparedness requirements, as well as an implementation plan which is critical for a successful implementation.

Identity and Authentication

- Multifactor Authentication (MFA) with Azure AD
- SSO with Azure AD
- Conditional Access with Azure AD
- End-point Filtering
- Admin Protections
- Privileged Identity Management
- Risky Login
- Self-Service Password Reset
- External Access

Threat Protection

- Mail Hygiene
- Mail Encryption
- Mail Transport Rules
- SIEM/SOAR
- SPF/DKIM/DMARC
- Endpoint device anti-malware
- Anti-phishing, anti-malware and anti-spam

Information Protection

- Tenant Security Hardening
- Tenant and Data Encryption
- Microsoft Cloud App Security (MCAS)
- External Content Sharing
- Data Loss Prevention (DLP)
- Discovery, Classification, Protection and Monitoring of email and documents with Azure Information Protection (AIP)
- Potential integration points with third-party solutions with AIP

Endpoint Device Management

- Review current MDM policies to minimize risk
- Discuss Conditional Access Policies with Intune
- Review MAM Capabilities

Features Demonstration

- Conditional Access
- Data Loss Prevention (DLP)
- Microsoft Secure Score
- Microsoft Compliance Score
- Microsoft Cloud App Security
- Microsoft Compliance Manager