

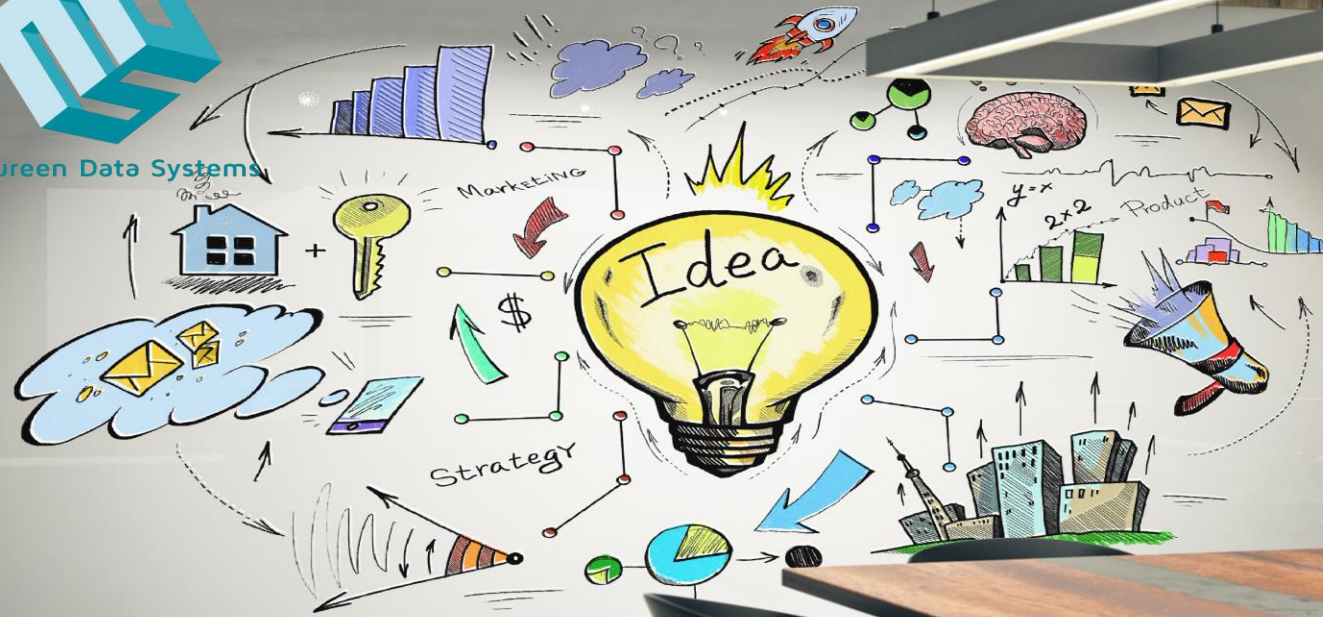
Build Zero Trust foundations

Zero Trust foundation Implementation Strategy

Let's start security with an intelligent idea



Maureen Data Systems



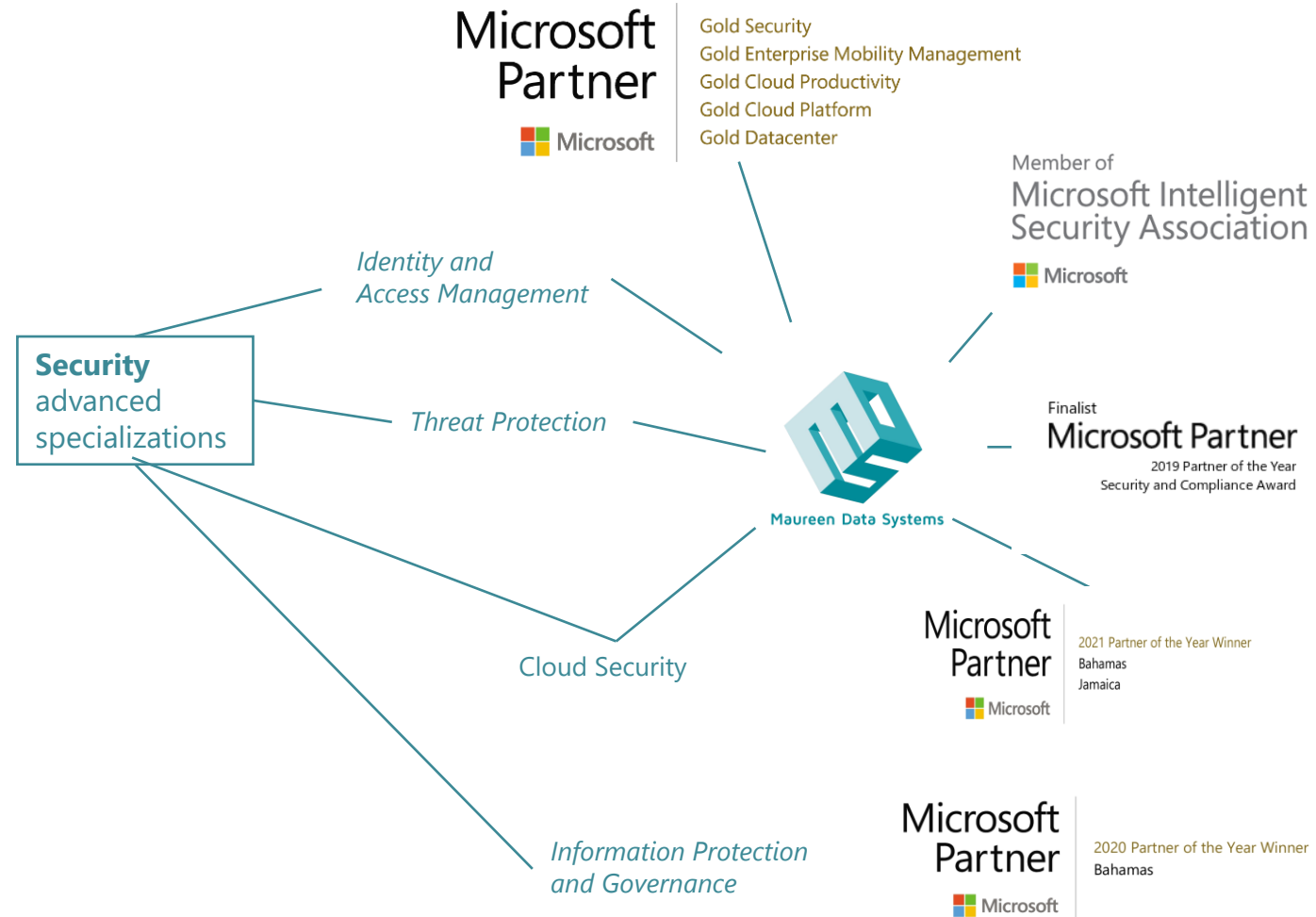
MDS Security Insight

MDS Security delivers security, risk, privacy and compliance services to Global companies.

Gold Certified Microsoft Security with Advance Security Specialization.

Highly seasoned professionals who can engage from the security engineering team to the C-suite, Compliance, Privacy and boardroom.

| | | |
|--|---|---|
| <p>Highly Capable Security, Compliance, Privacy Team</p> <ul style="list-style-type: none"> Senior team of professionals with deep technical skills Privacy, Legal and Compliance | <p>Highly Specialized in Cloud Security</p> <ul style="list-style-type: none"> Information Identity Governance, risk, and compliance Privacy, IT Legal | <p>Broad Set of Security Services</p> <ul style="list-style-type: none"> Strategy Implementation Managed Security Service SOC Service IR and Digital Forensic Service |
|--|---|---|



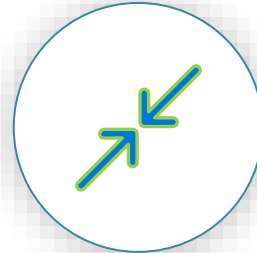
Zero Trust Implementation Strategy



Verify explicitly

Always validate all available data points including

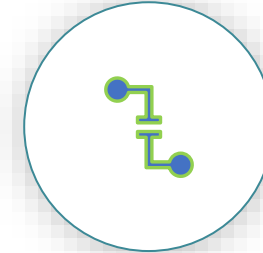
- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies



Use least privilege access

To help secure both data and productivity, limit user access using

- Just-in-**time** (JIT)
- Just-**enough**-access (JEA)
- Risk-based **adaptive** polices
- Data protection against **out of band** vectors



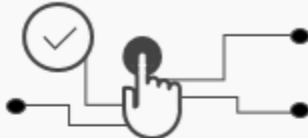



Assume breach

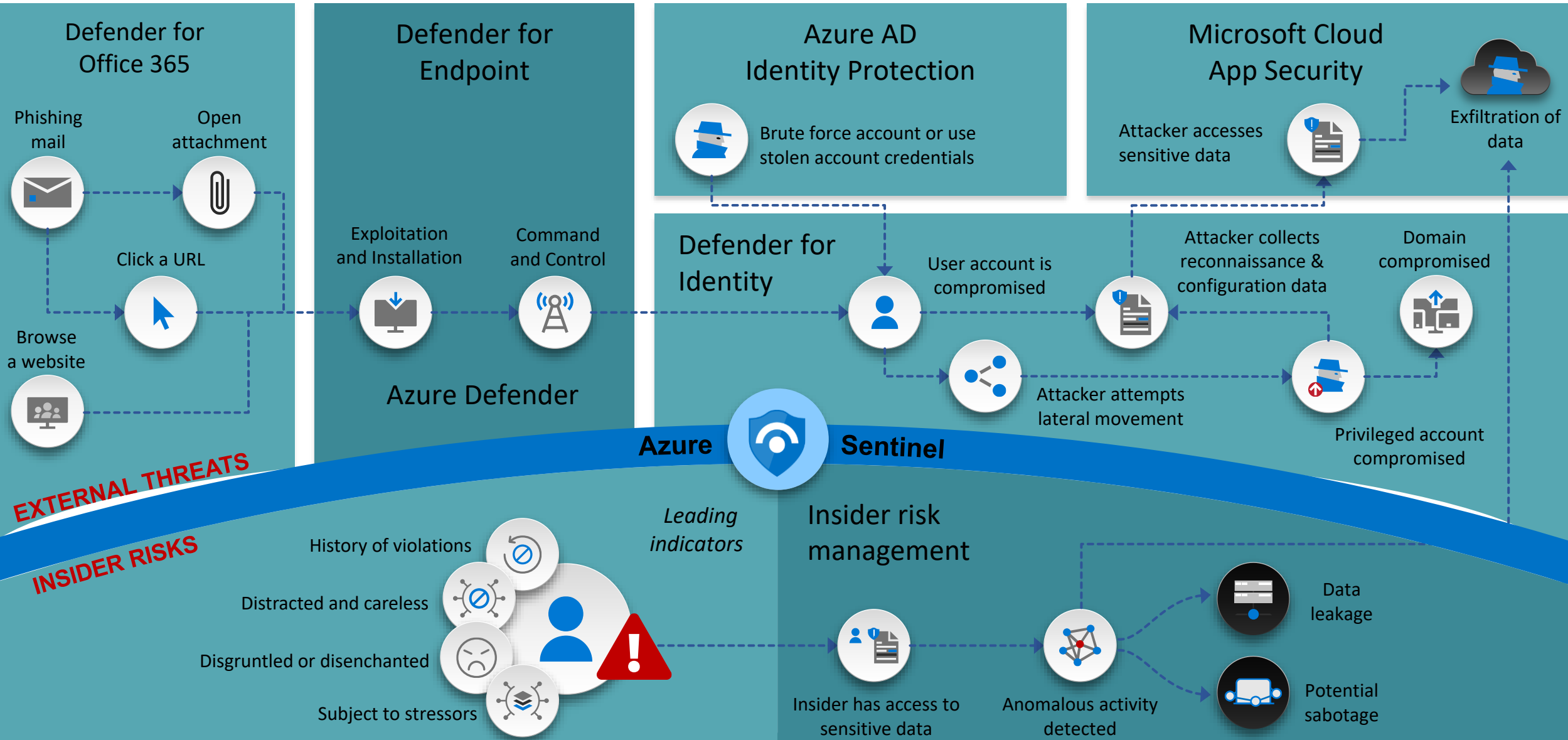
Minimize blast radius for breaches and prevent lateral movement by

- **Segmenting access** by network, user, devices, and app awareness.
- **Encrypting** all sessions end to end.
- **Use analytics** for threat detection, posture visibility and improving defenses

Zero Trust Implementation Strategy

| Pre-Zero Trust | Verify identity | Verify device | Verify access | Verify services |
|---|--|---|--|---|
| <ul style="list-style-type: none">✗ Device management isn't required✗ Single factor authentication to resources✓ Capability to enforce strong identity exists✓ Data classification and information protection exists |  <ul style="list-style-type: none">✓ Strong identity is verified and enforced✓ Passwords are eliminated in favor of biometrics✓ Access to applications and data is limited to minimum required to perform job function |  <ul style="list-style-type: none">✓ Client device health is enforced✓ Unmanaged devices have secure alternative access methods✓ Users don't have administrative permissions on client devices |  <ul style="list-style-type: none">✓ Internet is the default network in all Microsoft office locations✓ Network segmentations are built based on role and function |  <ul style="list-style-type: none">✓ Applications and conditions are enforced using conditional access✓ Applications and services are accessible directly from the internet |
| Pervasive telemetry | | | | |

Zero Trust with MITRE ATT&CK Architecture



Zero Trust Implementation Strategy

Zero Trust security models have emerged as a better alternative to traditional perimeter-based defenses, especially given the shift to remote work and expansion of the attack surface.

The purpose and objectives of this engagement are to develop a Zero Trust Implementation Strategy focusing on:

- The best starting point for deploying a “never trust, always verify” security model
- How to prioritize the path to Zero Trust security – and measure results along the way
 - People
 - *Zero Trust user experience balancing productivity and security*
 - *Adoption and change management for modernizing security*
 - *Security awareness training*
 - Process
 - *Zero Trust Adoption and change management strategy for modernizing security*
 - *Security and Compliance risk remediation alignment process*
 - *End-to-end security risk mitigation for cloud and business management*
 - *Work from anywhere on any device security process*
 - *Identity onboarding/offboarding and governance management*
 - Technology
 - *Advance conditional access using AAD, MEM, MCAS, Defender for Identity*
 - *Privileged account management using Azure PIM / PAM*
 - *Device security and management using MEM Intune, Defender for endpoint*
 - *Data protection and security using MIP, MCAS, and Azure Purview*

Zero Trust Implementation Strategy

- The key pillar of Zero Trust strategies implementation will focus on
 - Enforcing strong identity
 - *Ensure that a strong identity is verified and enforced.*
 - *Eliminate password-focused authentication in favor of biometrics.*
 - *Limit access to resources based on job function by using least-privilege access principles.*
 - Enforcing client devices health
 - *Intune for policy-based configuration management, application control, and conditional-access management.*
 - *Microsoft Defender for Endpoint (MDE) is configured to protect our devices, send compliance data to Azure AD Conditional Access, and supply event data to our security teams.*
 - Limiting access to data with least-privilege access
 - *Reduce the impact of a compromised identity by progressively eliminating unnecessary access.*
 - *Reduce the impact of a compromised identity by progressively eliminating unnecessary access.*
 - *Reduce the impact of a compromised identity by progressively eliminating unnecessary access.*

During this engagement, MDS will develop a Zero Trust security strategy program aligned to your business strategy and risk to enable your organization for rapid adoption of digital transformation.

MDS will then use the developed Zero Trust security strategy program to implement a foundation Zero Trust Microsoft security technologies.

MDS will also provide a Zero Trust maturity model and roadmap to be implemented later as your organization matures the adoption of Microsoft security solutions.