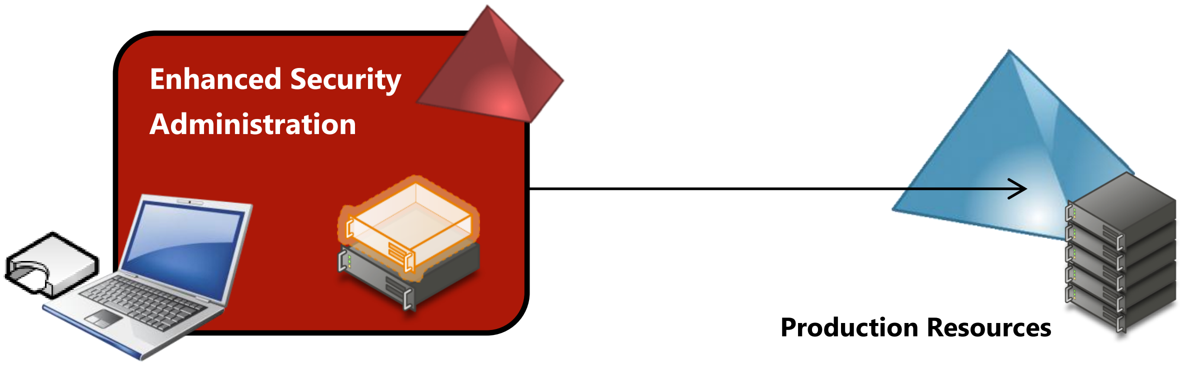
Enhanced Security Administrative Environment

Helps prevent compromise of administrative credentials from cyber-attacks



Protections for your most valuable accounts

- Provide an enhanced security environment for administrative accounts
- Implement advanced security tools including exploit technique mitigations, attack surface analysis, and application whitelisting
- Separate admin and user accounts
- Enforce two-factor authentication for admins
- Restrict admin accounts to high trust computers
- Restrict internet browsing and other high-risk activities for administrative accounts
- Monitoring of enhanced security environment and production Domain Controllers (DCs) for security events and operational health
- Easy to use for administrators

Overview

Cyber-attackers have been very successful at rapidly gaining administrative access to corporate and government computing environments. These devastating attacks result in malicious actors with full remote access to most or all of an organization’s electronic documents, presentations, applications, databases, and other intellectual property. Recovery from these attacks is extremely difficult, slow, and expensive.

The Enhanced Security Administrative Environment (ESAE) offering is designed to help thwart a critical element of these credential theft attacks by limiting exposure of administrative credentials.

How the Offering Works

The ESAE offering leverages advanced technologies and recommended practices to provide an administrative environment and workstations with enhanced security protection.

As attackers inevitably adapt, this solution is designed to evolve to include protections for future attack vectors.

Combines cutting-edge technologies and enforcement of recommended practices

Technologies used in this solution:

- Windows Server 2008 R2 Active Directory Domain Services (AD DS)
- Smartcards and Windows Server 2008 R2 Active Directory Certificate Services (AD CS)
- Microsoft System Center Operations Manager 2007 R2
- Microsoft SQL Server and Reporting Services 2008 R2
- ForeFront Identity Manager (FIM) 2010
- Windows 7 x64
- Bitlocker
- AppLocker
- Attack Surface Analyzer (ASA)
- Security Compliance Manager (SCM)
- Enhanced Mitigation Experience Toolkit (EMET)

*For more information about Consulting and Support solutions from Microsoft, contact your Microsoft Services representative or visit **www.microsoft.com/services***

Credential Hygiene and Smartcards

Credential hygiene is the recommended practice of ensuring privileged accounts only logon to the workstations and servers that are sufficiently trusted and do not perform high risk activities like Internet browsing. This is critical because an administrator accessing a low trust workstation may enable attacker-controlled malware on that workstation to steal the administrator's credentials.

This solution enforces credential hygiene by separating administrative accounts from normal user accounts (for email and web browsing) and compartmentalizing logon access for each type of administrative account. The solution also enforces two-factor authentication for administrative accounts with smartcards.

Auditing and Monitoring

For attack detection and accountability purposes, the solution implements auditing and monitoring of high-impact administrator activity. This ensures administrators are alerted to events that could indicate a compromise as well as providing a tamper-resistant record of events.

Advanced Protection Technologies

Administrators logon to dedicated physical workstations that are hardened to improve their ability to resist remote attacks, local privilege escalation attacks, and physical compromise. The solution employs Security Compliance Manager (SCM) for secure baseline configuration, Attack Surface Analyzer (ASA) for identifying and closing configuration vulnerabilities, AppLocker for application launch control, BitLocker$^{\text{TM}}$ for system integrity, and the Enhanced Mitigation Experience Toolkit (EMET) for exploit technique protections.

Solution Delivery

This solution may be deployed to protect all administrative accounts or only higher privilege domain administrator accounts. For deployments managing large numbers of administrators, we recommend smartcard lifecycle management with ForeFront Identity Manager (FIM) 2010, an optional solution component.

Contact your Microsoft Services representative for more information.

This data sheet is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.