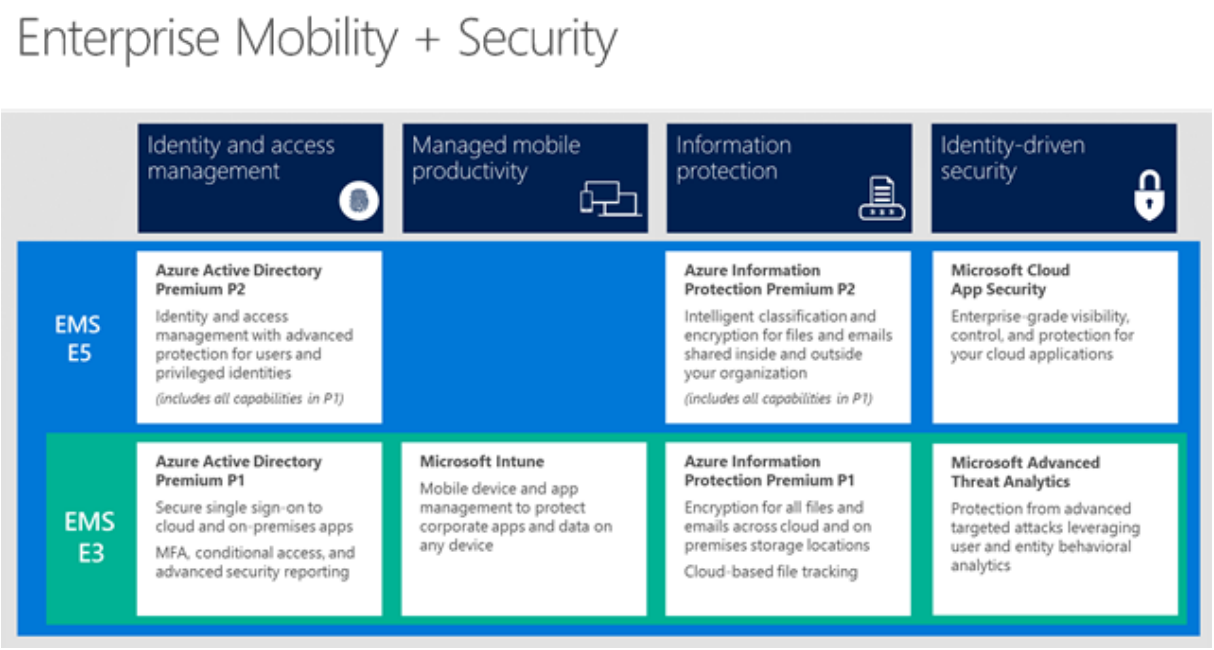
Microsoft Enterprise Mobility + Security (EMS)

Executive Summary

Microsoft Enterprise Mobility + Security (EMS), früher bekannt unter dem Namen Enterprise Mobility Suite, ist ein Paket aus verschiedenen aufeinander abgestimmten Produkten rund um die Verwaltung und Sicherheit Ihrer Infrastruktur und mobilen Geräte. Das Paket gibt es in den Ausführungen E3 und E5. Die Variante E3 bildet hier die Nachfolge der Enterprise Mobility Suite.

EMS E3 und E5 setzen sich aus den folgenden Produkten zusammen:



1. Hybrid Identity Management – Azure Active Directory Premium

Hybrid Identity erweitert Ihre vorhandene Active Directory-Infrastruktur in die Cloud mit Hilfe von Microsoft Azure Active Directory. Mit integriert sind die Optionen zur mehrstufigen Authentifizierung und für den bedingten Zugriff. Die Ausführung P2 beinhaltet zusätzliche Sicherheitsfeatures für die Benutzer- und Administratorkonten.

Azure Active Directory bietet Funktionen zur Benutzerverwaltung, Integration mit Ihrer bestehenden Windows Server Active Directory und Single-Sign-On für über 1200 Cloud-Anwendungen wie z.B. Office 365 und zahlreiche SaaS-Anwendungen.

Azure Active Directory-Premium ist ein benutzerorientiertes Identitäts- und Zugriffsverwaltungsmanagement in der Cloud. Durch die Bereitstellung eines maßgeschneiderten Portals mit dem Logo Ihres Unternehmens, können Anwender per Single Sign-on auf alle Ihre Cloud-Anwendungen gelangen.

intellecom GmbH

Standort Eberbach
Bahnhofsplatz 5
69412 Eberbach

Standort Böblingen
Otto-Lilienthal-Str. 5
71034 Böblingen

Kontakt
Tel. +49 6271 94 23 23
Fax +49 6271 94 25 50

www.intellecom.de
info@intellecom.de

Das People-Centric Konzept stellt hierbei den Anwender in den Vordergrund. Somit ist der Zugriff dabei nicht auf einzelne Browser, Geräte oder Plattformen beschränkt.

Mit Azure Active Directory Premium können Anwender ihre eigenen Passwörter unter Berücksichtigung der Sicherheitsanforderungen Ihrer Organisationen selbst zurücksetzen.

- Erstellen und verwalten Sie nur eine Identität für jeden Benutzer in Ihrer hybriden Umgebung, und halten Sie Benutzer, Gruppen und Geräte synchron.
- Ermöglichen Sie den Zugriff auf Ihre Anwendungen per Single Sign-On, z. B. auf Tausende vorab integrierte SaaS-Anwendungen.
- Sorgen Sie für Sicherheit beim Anwendungszugriff mithilfe der regelbasierten mehrstufigen Authentifizierung für lokale Anwendungen und Cloud-Anwendungen.
- Verbessern Sie die Benutzerproduktivität, indem Sie die Self-Service-Kennwortrücksetzung und -Anwendungsanforderung für Verzeichnisse im Rechenzentrum und in der Cloud nutzen.
- Stellen Sie den sicheren Remotezugriff auf lokale Webanwendungen per Azure AD-Anwendungsproxy bereit.
- Nutzen Sie die hohe Verfügbarkeit und Zuverlässigkeit einer Lösung für die Identitäts- und Zugriffsverwaltung, die weltweit verfügbar, für Großunternehmen geeignet und cloudbasiert ist.
- Schützen Sie Ihre Benutzer-und Administratorkonten mit Azure Active Directory Premium P2 durch zusätzliche Sicherheitsfunktionen.

2. Mobile Device Management (MDM) – Microsoft Intune

Mit der MDM-Lösung aus dem Hause Microsoft setzen Sie auf eine plattformübergreifende Verwaltung Ihrer mobilen Geräte und Applikationen. Im Zusammenspiel mit dem System Center Configuration Manager (SCCM) steigern Sie das Potenzial, indem über eine einzige Konsole Ihre lokalen und mobilen Endgeräte und Applikationen verwaltet werden.

Mit Microsoft Intune steuern Sie den gesamten LifeCycle Ihrer mobilen Geräte und Applikationen vom Ausrollen und Verteilen der Richtlinien, Einstellungen und Applikationen bis zum Sperren, Entfernen einzelner Tools oder dem kompletten Löschen der Devices.

- Führen Sie die Bereitstellung und Verwaltung von Apps für alle aktuellen Plattformen, iOS, Android, Windows, Windows Phone und Windows 10 Mobile über eine zentrale Verwaltungskonsole durch.
- Vereinfachen Sie die administrativen Aufgaben, indem Sie erforderliche Apps automatisch während der Registrierung bereitstellen und Benutzern das einfache Installieren von Unternehmens-Apps über das Self-Service-Unternehmensportal ermöglichen.

- Steigern Sie die Produktivität mit den mobilen Office-Apps, mit denen Ihre Mitarbeiter vertraut sind, und schützen Sie Unternehmensdaten, indem Sie Aktionen wie Kopieren/Ausschneiden/Einfügen/Speichern in der verwalteten App-Umgebung einschränken. Erweitern Sie diese Funktionen auf vorhandene Branchen-Apps.
- Stellen Sie Zertifikate, WLAN, VPN und E-Mail-Profile automatisch bereit, sobald ein Gerät registriert ist. So ermöglichen Sie Benutzern den nahtlosen Zugriff auf Unternehmensressourcen mit den entsprechenden Sicherheitskonfigurationen.
- Stellen Sie eine umfangreiche Einstellungsverwaltung für mobile Geräte bereit, z. B. Remoteaktionen wie das Zurücksetzen des Kennworts, Gerätesperre und Datenverschlüsselung.
- Löschen Sie Unternehmensdaten und -anwendungen, wenn die Registrierung eines Geräts aufgehoben wird oder wenn es nicht kompatibel ist, verloren geht, gestohlen oder außer Betrieb genommen wird.
- Erweitern Sie Ihre vorhandene System Center Configuration Manager-Infrastruktur durch eine Microsoft Intune-Integration und ermöglichen Sie eine einheitliche benutzerfreundliche Verwaltung auf allen Geräten – lokal und in der Cloud.

Flexibilität

- Migration Ihrer IT in eine cloudbasierte Infrastruktur oder Anbinden an ein bestehendes System Center 2012 R2
- Nutzung auf diversen Formfaktoren unter Verwendung Ihrer Sicherheitsrichtlinien
- Self-Service-Portal senkt den Verwaltungsaufwand

Kontrolle

- Zentral verwaltete Updates und Anwendungen
- Proaktives Monitoring der Endgeräte
- Verschlüsselung, Multifaktor-Authentifizierung (MFA) und Fernlöschung

Produktivität

- Vereinfachte Administration durch einheitliches Gerätemanagement
- Einheitliche Infrastruktur
- Kostenoptimiertes IT-Management inklusive Tracking-Funktion für Hardware und Software
- Zentral verwaltete Endpoint-Protection

Durch den Einsatz von Microsoft Intune können Sie die Anwendungs- und Geräteverwaltung komplett über die Cloud oder per Integration in System Center 2012 Configuration Manager bereitstellen – alles über eine zentrale Verwaltungskonsole.

Außerdem hat Microsoft Funktionen für Verwaltung und Datenschutz direkt in die mit Intune verwalteten mobilen Office-Apps integriert, um die Produktivität zu steigern. Gleichzeitig ist es möglich, diese Verwaltungsfunktionen mit dem Intune App Wrapping Tool auf Ihre Branchen-Apps auszuweiten.

intellecom GmbH

Standort Eberbach
Bahnhofsplatz 5
69412 Eberbach

Standort Böblingen
Otto-Lilienthal-Str. 5
71034 Böblingen

Kontakt
Tel. +49 6271 94 23 23
Fax +49 6271 94 25 50

www.intellecom.de
info@intellecom.de

Geschäftliche und private Daten trennen

Um immer und überall produktiv sein zu können, wünschen sich Benutzer, dass sie mit allen Geräten auf die Unternehmensressourcen zugreifen können. Die geschäftlichen Anforderungen ändern sich ständig, da Unternehmen sich im Wettbewerb behaupten müssen. IT-Experten müssen nicht nur die Unterstützung unterschiedlicher Geräte sicherstellen, sondern auch die Unternehmensdaten schützen und für Compliance sorgen. Microsoft Intune bietet Ihnen die Möglichkeit die Kommunikation zwischen Ihren geschäftlichen Applikationen und Ihren privaten Applikationen zu trennen. So bleiben Ihre Unternehmensdaten in Ihrem geschützten und verwalteten Bereich.

3. Data Protection – Azure Information Protection Premium P1/P2

Mit dem Azure Information Protection Premium Service teilen Sie ihre Dokumente mit anderen und haben die Sicherheit, dass die Empfänger diese auf allen gängigen Endgeräten nutzen können. Dabei werden sämtliche Datei-Formate von den gebräuchlichen Office-Formaten über Bilddateien, PDF und XML auf den aktuellen Plattformen (Windows, Windows Phone, Windows 10 Mobile, Mac OS/X, iOS und Android) unterstützt.

Azure Information Protection Premium steht als SaaS-Lösung über die Microsoft Azure-Cloud zur Verfügung. Dabei hat Microsoft selbst keinen Zugriff auf die Inhalte Ihrer Daten. Die dokumentenspezifischen Schlüssel können dabei auch über Ihre lokale IT verwaltet werden („Bring Your Own Key").

Mit **Data Loss Prevention (DLP)** können Sicherheitsrichtlinien erstellt werden, sogenannte Templates, welche granuliert festlegen, was für Daten über welchen Weg und von wem weitergegeben werden dürfen.

Mit **Azure Information Protection Premium** werden Ihre Dateien in der Cloud verschlüsselt, können verschlüsselt abgelegt werden und garantieren eine sichere Zusammenarbeit im Team beim Versenden von Dateien über das Internet oder per E-Mail. Die Verschlüsselung ist dabei an die Benutzeridentität gebunden und kann auch verwendet werden ohne das Azure Information Protection Premium für das Unternehmen aktiviert worden ist.

- Verschlüsselungsrichtlinie auf Dateiebene, mit der das Dokument innerhalb und außerhalb Ihrer Organisation verfolgt wird, z.B. E-Mails unabhängig vom E-Mail Dienst des Empfängers.
- Erhöhte Sicherheit bei der Zusammenarbeit durch Schutz für nahezu alle Dateitypen auf jeder Geräteplattform, z.B. aus Anwendungen wie SharePoint, Office oder Exchange durch leicht konfigurierbare Berechtigungsregeln.
- Sicherer Austausch von Dateien per E-Mail oder über Ihren bevorzugten Cloud-Speicherdienst, z. B. Microsoft OneDrive oder Dropbox.
- Wahlmöglichkeit zwischen flexiblen, lokalen und cloudbasierten Bereitstellungsoptionen je nach Anforderungen Ihres Unternehmens.

- Der dokumentenspezifische Schlüssel kann von der eigenen IT verwaltet werden.
- Kontrolle über die eigenen Daten (on-premise, hybrid oder cloud).

4. Microsoft Advanced Threat Analytics

Microsoft Advanced Threat Analytics (ATA) ist ein on-premise Produkt, mit dem Sie Sicherheitsattacken, unter Verwendung von User and Entity Behavioral Analytics (UEBA) Technologien, erkennen.

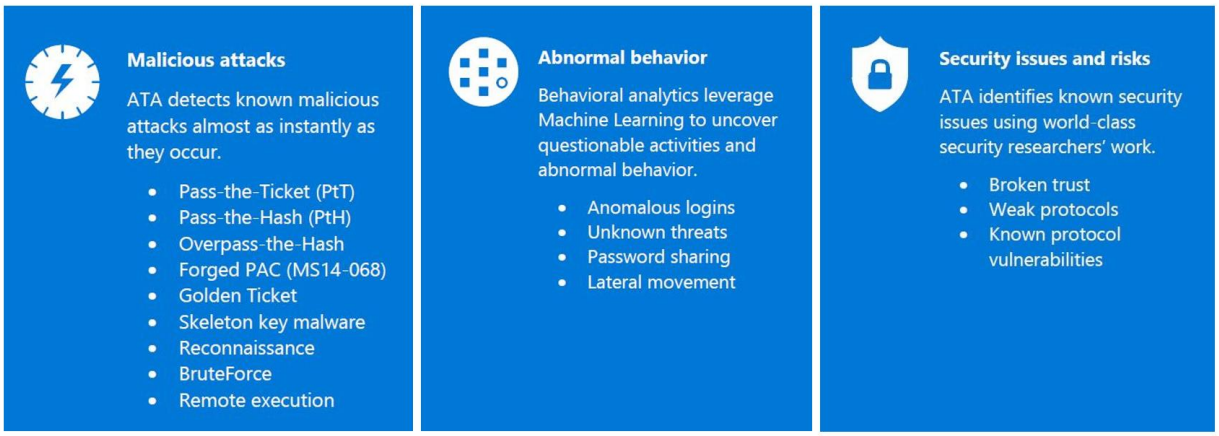
Durch die Identifizierung von verdächtigen Benutzer- und Geräteaktivitäten, bietet ATA eine einfache und schnelle Art und Weise zu verstehen, was in Ihrem Netzwerk passiert. Sobald diese Aktivitäten identifiziert sind, bietet ATA klare und relevante Informationen über die Bedrohung in einer einfachen, klaren Timeline.

ATA ist eine On-Premise-Plattform, die Ihr Unternehmen vor gezielte Angriffe schützt, indem es automatisch normale und abnormale Verhaltensweisen von Benutzern, Geräten und Ressourcen analysiert, lernt und identifiziert.

Bösartige Angriffe: Die Diagnose Engine erkennt bekannte Angriffsmethoden beinahe in Echtzeit.

Abnormales Verhalten: Die verhaltensbasierende Analyse nutzt maschinelles Lernen um fragwürdige Aktivitäten und abnormales Verhalten aufzudecken.

Sicherheitsprobleme und Risiken: ATA identifiziert bekannte Sicherheitsprobleme und Risiken anhand der Arbeit der weltweit führenden Sicherheitsexperten.



- Erkennung verdächtiger Aktivitäten und böswilligen Angriffe mit Verhaltensanalysen
- Anpassung an die sich verändernde Art der Cyber-Sicherheitsbedrohungen
- Fokus auf das, was ist wichtig, mit einer einfachen Angriffs-Timeline
- Reduzieren Sie Anzahl von Falschmeldungen

intellecom Mobile Services

Die intellecom GmbH wurde von Microsoft zum Vertrieb von Microsoft Online Services profiliert.

Nutzen Sie unsere Erfahrungen und Kompetenz und vereinbaren einen unverbindlichen Gesprächstermin zu diesem aktuellen Themenkomplex.

Im Einzelnen bieten wir Ihnen:

- Vorab WEB Cast oder vor Ort Präsentation der Produktmöglichkeiten mit unserem mobilen Test- und Demo-Lab
- Lösungsberatung, Strategieberatung, Konzeption für den Einsatz von Microsoft Enterprise Mobility + Security
- Evaluierung sowie Pilotierung
- Erstellung Ihres Proof of Concepts
- Migration und Implementierung
- Mobility to go as a Managed Service

Nehmen Sie Kontakt auf!

Für Fragen zum Thema oder weiterführende Informationen stehen wir Ihnen gerne zur Verfügung unter Tel: +49 6271 942323 oder per E-Mail info@intellecom.de

intellecom GmbH

Standort Eberbach
Bahnhofsplatz 5
69412 Eberbach

Standort Böblingen
Otto-Lilienthal-Str. 5
71034 Böblingen

Kontakt
Tel. +49 6271 94 23 23
Fax +49 6271 94 25 50

www.intellecom.de
info@intellecom.de