DATENBLATT

Defender®

Schützen Sie Ihr Unternehmen mit einer Zwei-Faktor-Authentifizierung

Vorteile

- Höhere Sicherheit für nahezu alle Systeme und Anwendungen
- Nutzung der Skalierbarkeit, Sicherheit und Compliance von Active Directory
- Selbstregistrierung und Aktivierung von Token durch Benutzer
- Beschleunigte Problemlösung durch Helpdesk-Mitarbeiter bei Problemen mit der Benutzerauthentifizierung
- Unterstützung aller OATH-konformen Hardwaretoken
- Umfassende Audit-Trails für Compliance und Forensik

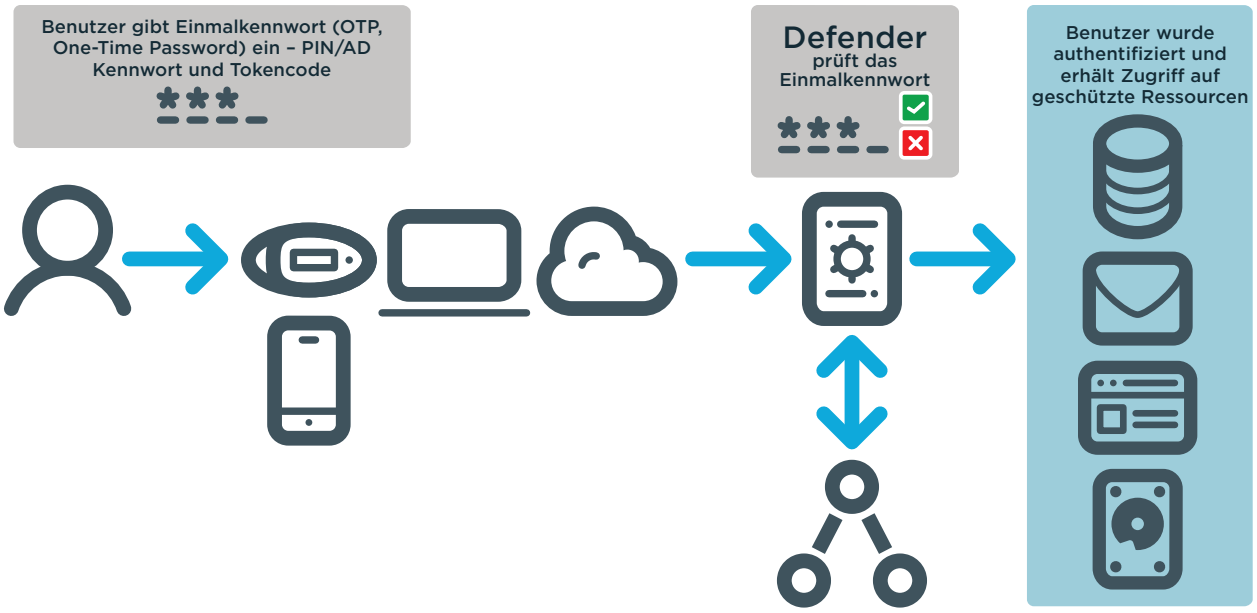
Systemanforderungen

Eine vollständige Liste der Systemanforderungen finden Sie unter oneidentity.com/Defender

Compliance- und Sicherheitsanforderungen von Organisationen gehen heutzutage weit über herkömmliche Sicherheitsniveaus in Form von Benutzername und Kennwort hinaus. Die Zwei-Faktor-Authentifizierung, die "etwas, was Sie haben" (beispielsweise ein Token) und "etwas, das Sie kennen" (Benutzername und Kennwort) kombiniert, ist im Bereich Sicherheits- und Complianceinitiativen der meisten Organisationen schnell in den Vordergrund gerückt. Herkömmliche Zwei-Faktor-Authentifizierungslösungen sind kostspielig in der Bereitstellung und basieren auf proprietären Schnittstellen und Verzeichnissen. Defender® basiert auf Standards (OATH, RADIUS, LDAP, PAM usw.) und nutzt Active Directory (AD) für die Administration und die Verwaltung der Identitäten. Die Verwendung von AD sorgt nicht nur für höhere Sicherheit und verbesserte Skalierbarkeit, sondern auch für geringere Kosten, da aktuelle Mitarbeiter Defender verwalten können.

Darüber hinaus können Benutzer mit Defender problemlos Hardware- und Softwaretoken anfordern und diese sicher selbst registrieren, was Kosten und Zeit spart, die normalerweise für die Einführung einer Zwei-Faktor-

ONE IDENTITY



Defender nutzt die vorhandene Infrastruktur eines Unternehmens und sorgt für eine optimierte Sicherheit – kostengünstig und flexibel.

Authentifizierung aufgewendet wurden. Defender unterstützt alle OATH-konformen Hardwaretoken, bietet zahlreiche Software-Token und unterstützt die Nutzung von Webdiensten wie Google Authenticator oder Authy. Dank der Verwendung vorhandener Infrastruktur, Selbstregistrierung durch Benutzer und Unterstützung für mehrere Tokentypen können Organisationen mit Defender ihre Sicherheits- und Compliancemaßnahmen auf eine flexible und kostengünstige Art und Weise optimieren.

Funktionen und Merkmale

Active Directory-basiert: Nutzen Sie die Skalierbarkeit, Sicherheit und Compliance von Active Directory, um eine Zwei-Faktor-Authentifizierungslösung für jedes System sowie jede Anwendung oder Ressource bereitzustellen und die Vorteile des bereits vorhandenen Unternehmensverzeichnisses zu nutzen, statt ein zusätzliches proprietäres Verzeichnis zu erstellen. Die Zuordnung von Benutzertoken ist ist einfach ein zusätzliches Attribut in den Benutzereigenschaften in Active Directory.

Webbasierte Verwaltung: Im webbasierten Defender Verwaltungsportal stehen Defender Administratoren, dem Helpdesk, und auch Endbenutzern entsprechende Optionen zur Token-Verwaltung, Token-Bereitstellung, zum Anzeigen von Echtzeitprotokollen, zur Fehlerbehebung und Berichterstellung zur Verfügung.

Token-Selbstregistrierung: Ermöglichen Sie den Benutzern die Anforderung von Hard- oder Soft-Token auf der Grundlage von Richtlinien, die von den Administratoren festgelegt wurden, und weisen Sie diese Token mithilfe eines sicheren Mechanismus dann schnell und einfach dem jeweiligen Benutzerkonto zu.

Problembehandlung durch Helpdesk-Mitarbeiter: Mit nur wenigen Mausklicks und über jeden Webbrowser können Defender Administratoren und Helpdesk-Mitarbeiter Probleme bei der Benutzerauthentifizierung analysieren und lösen. Zeigen Sie eine Liste von Authentifizierungsversuchen und -routen, mit den entsprechenden Ergebnissen, möglichen Fehlerursachen und Lösungsschritten mit nur einem Mausklick an. Darüber hinaus können Sie Benutzerkontodetails und zugewiesene Token anzeigen und haben die Möglichkeit zum Testen oder Zurücksetzen der PIN-Nummer, zum Bereitstellen einer temporären Tokenantwort oder zum Zurücksetzen oder Entsperren des Kontos.

Tokenflexibilität: Stellen Sie beliebige OATH-konforme Hardwaretoken vom Tokenanbieter Ihrer Wahl bereit. Defender bietet auch eine große Auswahl an Softwaretoken für die beliebtesten und weit verbreiteten mobilen Plattformen. Mit einer universellen Softwaretokenlizenz kann der Administrator ganz einfach die erforderliche Gerätelizenz neu ausstellen, wenn ein Benutzer die mobile Plattform wechseln möchte.

"Nach Jahren der Nutzung hat sich Defender als solide, robuste Lösung bewährt. Mir fällt keine Situation ein, in der Defender jemals versagt hätte. Die Lösung ist benutzer-freundlich und hat sich vollständig in unsere Umgebung integriert, sodass wir sie nicht mehr als separate Lösung betrachten."

Gregory Pronovost
Assistant Director für IT
City of Bakersfield

Sicherer Web-E-Mail-Zugriff: Ermöglichen Sie sicheren webbasierten Zugriff auf das E-Mail-System Ihres Unternehmens von jedem Webbrowser aus, jederzeit und überall. Defender beinhaltet eine spezielle Lizenz für Cloud Access Manager, der über die Reverse-Proxy-Funktion den sicheren Zugriff auf Webmails gestattet. Sie können Defender-Token nutzen, um den Zugriff auf die entsprechende Authentifizierung ungeachtet des Zugriffspunkts sicherzustellen.

ZeroIMPACT-Migration: Führen Sie mit ZeroIMPACT eine schrittweise Migration von einer etablierten Legacy-Authentifizierungslösung nach Defender durch. Da Defender und das Legacy-System parallel aktiviert sind, werden alle Benutzerauthentifizierungsanforderungen an Defender geleitet. Wenn der Benutzer noch nicht in Defender definiert ist, wird die Authentifizierungsanforderung transparent über die Proxy-Funktion an die abzulösende Authentifizierungslösung weitergegeben. So können Administratoren Benutzer zu Defender migrieren, wenn ihre Legacy-Token ablaufen.

Zentrale Verwaltung: Integrieren Sie Defender in Active Directory und profitieren Sie von einer zentralen Verwaltung von Verzeichnisinformationen über eine zentrale, vertraute Benutzeroberfläche. Die Zuordnung von Benutzertoken ist ein zusätzliches Attribut in den Benutzereigenschaften in Active Directory, was die Sicherheitsverwaltung effizienter macht.

Verschlüsselung: Sichere Kommunikation durch Zuweisung eines Management-DES (Data Encryption Standard) für Defender Security Server. Defender unterstützt AES, DES oder Triple DES Verschlüsselung.

Pluggable Authentication Module (PAM): Mit dem Defender-Modul für PAM können Sie festlegen, dass Dienste und Benutzer auf Ihren UNIX/Linux Systemen von Defender authentifiziert werden.

Über One Identity

Die One Identity Lösungen für Identitäts- und Zugriffsmanagement bieten Identitäts- und Zugriffsmanagement für den Praxiseinsatz und umfassen geschäftsorientierte, modulare, integrierte und zukunftsfähige Lösungen für Identity Governance, Zugriffsverwaltung und Verwaltung privilegierter Konten.

Weitere Informationen finden Sie unter OneIdentity.com

Datasheet-Defender-US-KJ-DE-WL-25672

ONE IDENTITY