DATASHEET

Defender

Two-factor authentication made easy

Benefits

- Enhanced security for virtually any system or application
- Leverages the scalability, security and compliance of Active Directory
- Enables token self-registration and renewal by end users
- Accelerates helpdesk resolution of user authentication issues
- Supports any OATH-compliant hardware token
- Delivers a comprehensive audit trail for compliance and forensics

Overview

Our 2FA solution, Defender, enhances security by requiring two-factor authentication to gain access to your network resources. Defender uses your current identity store within Microsoft Active Directory (AD) to enable two-factor authentication. It takes advantage of AD's inherent scalability and security to eliminate the time and expense involved with setting up and maintaining proprietary databases. Defender's web-based administration, user self-registration and ZeroIMPACT migration capabilities ease implementation for administrators and users. Plus, Defender hardware tokens utilize their full battery life and provide software tokens that never expire.

Features

Active Directory-centric

Use the scalability, security and compliance of Active Directory (AD) to provide a two-factor authentication to any system, application or resource. You can take advantage of the corporate directory already in place, instead of creating an additional proprietary one — and save time and money. User token assignment is simply an additional attribute to the user object within AD.

Token self-registration

Enable users to request a hard or soft token based upon policy defined by administrators, and then quickly and easily assign that token to their account through a secure mechanism. Token self-registration removes the entire administrative burden and associated costs of conventional manual token assignment.

Help desk troubleshooter

Enable help desk and Defender administrators to troubleshoot, diagnose and resolve user-authentication-related problems with just a couple of mouse clicks from any browser. View a current list of authentication attempts and routes, with associated results, possible reasons for failures and one-click resolution steps. In addition, Defender enables you to view user account details and assigned tokens, quickly test or reset the pin, provide a temporary token response, reset or unlock the account.

Web-based administration

Provide Defender administrators, help-desk administrators and end-users options for token management, token deployment, real-time log viewing, troubleshooting and reporting using the web-based Defender Management Portal.

Token flexibility

Make use of the full battery life of hardware tokens — typically 5 to 7 years — rather than having a vendor-defined term. This enables you to replace tokens as they expire, in a business-as-usual process, instead of to all users at one time and incurring the costs associated with such a project. In addition, Defender offers smartphone tokens that never expire.

ZeroIMPACT migration

Defender can run in tandem with legacy systems. All user-authentication requests are directed to Defender. If the user is not yet defined within Defender, the authentication request is passed via the proxy feature to the incumbent authentication solution. This allows administrators to migrate users to Defender as their legacy tokens expire, with virtually no overhead from an administrator or end-user perspective.

Universal soft tokens with Push-to-Authenticate

The Defender two-factor authentication solution offers a wide range of software tokens for most popular and widely deployed mobile platforms. By offering a universal software token license, the administrator can easily reissue the appropriate device license when a user decides to switch mobile platforms. Defender smartphone tokens now offer Push-to-Authenticate feature, requiring a single tap to authenticate.

Pluggable Authentication Module (PAM)

Specify that services and users defined on your Unix/Linux systems be authenticated by Defender with its Pluggable Authentication Module (PAM).

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Identity and Access Management (IAM), Privileged Access Management (PAM) and Active Directory Management and Security (ADMS) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 250 million identities for more than 5,000 organizations worldwide. For more information, visit oneIdentity.com.

Datasheet-2022-Defender-PG-70907