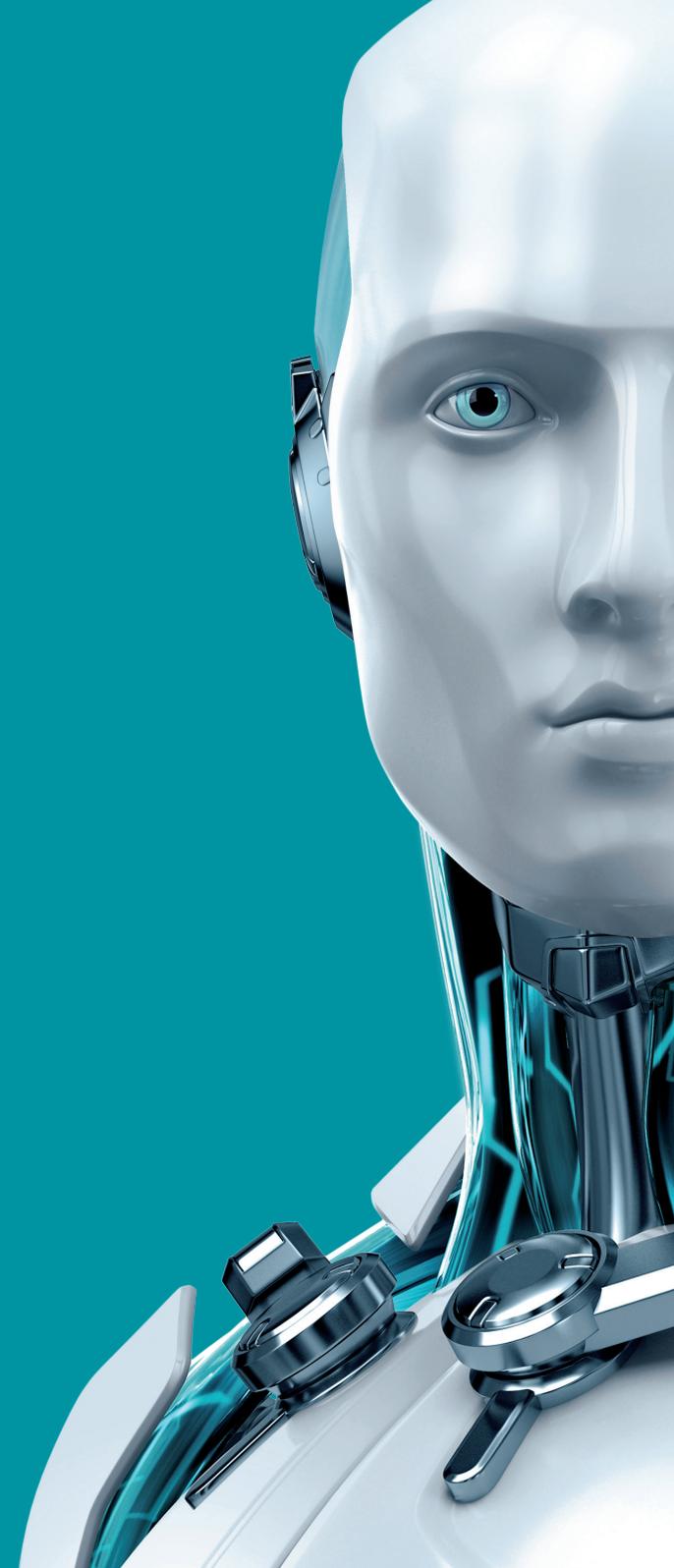# ESET

SECURE AUTHENTICATION

BUSINESS

ENJOY SAFER TECHNOLOGY™

ESET

SECURE
AUTHENTICATION

ESET Secure Authentication helps businesses to make access to their data secure. Our solution utilizes the existing Active Directory domain, allowing you to set up ESET's two-factor authentication in just 10 minutes – and thus easily reduce the risk of data breaches, caused by stolen, weak or compromised passwords.

The solution consists of the server side and the client side – the latter comes in the form of a mobile app. The authentication options include Push Authentication, as well as generation and delivery one-time passwords (OTPs) via the mobile app, but also via SMS messages or your organization's existing hardware tokens.

Two-factor authentication for extra data protection.

You can use ESET Secure Authentication for:

- Accessing your company's VPN
- Remote Desktop Protocol
- Additional authentication for desktop login (signing into an operating system)
- Web/cloud services via Microsoft ADFS 3.0, such as Office 365 and Google Apps

- Various Microsoft Web Apps, such as Outlook Web Access (OWA)
- Exchange Control Panel 2010 & Exchange Administrator Centre 2013
- VMware Horizon View
- RADIUS-based services

PUSH AUTHENTICATION

STANDARD PASSWORD

OR

ONE TIME PASSWORD

USER'S COMPUTER

INTERNAL COMPANY DATA
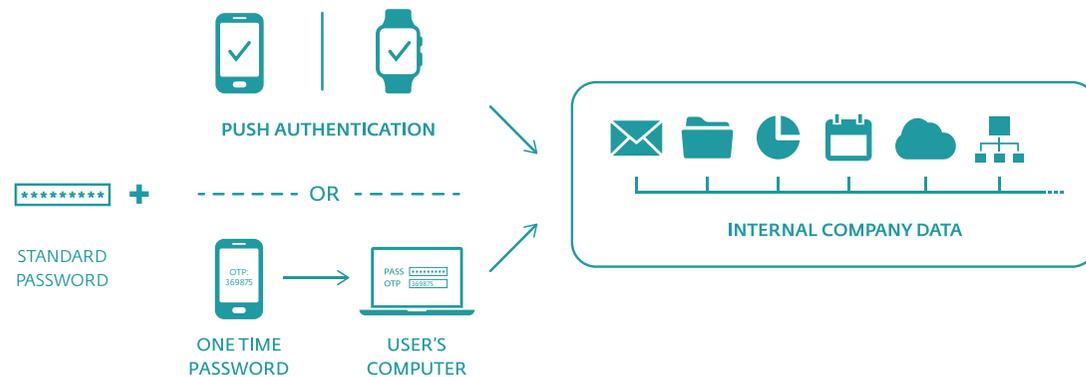
Business benefits

- Helps prevent breaches by employing unique passwords for each access
- Protects against poor password practices
- Improved productivity and user experience - thanks to one-tap push authentication
- Saves costs – no additional hardware needed
- Easy to migrate to and use
- Supports existing hardware tokens to meet compliance requirements
- Also adds 2FA to your cloud applications, such as Office 365 or Google Apps

IT benefits

- API/SDK for easy integration into proprietary software and business tools
- App works without internet connection (once downloaded)
- Supports most types of mobile operating systems
- Global technical support in local languages
- Out-of-the-box solution
- Increases productivity and reduces unnecessary friction when accessing trusted sites, thanks to IP whitelisting
- Tools for deployment and configuration in large user environments

Datasheet

Two-Factor Authentication	Mobile-based, two-factor (2FA) authentication for a higher level of security
	Native support for a broad range of platforms (see Supported platforms overview, below)
	Software-based solution – no need to carry an additional device or token
	Convenient for your mobile workforce
	Support for hardware tokens
	Compatible with any mobile phone that supports SMS messaging
Client Side (mobile app)	One-tap installation, simple and effective user interface
	Supports a broad range of mobile operating systems
	PIN-protected access to prevent fraud in case of device theft or loss
	Apps available in 16 languages, including English, German, Russian, French and Spanish
Authentication Methods	Mobile client app – generates one-time passwords (OTPs); no internet connection required
	Push Authentication – single-touch authentication via mobile phone (requires mobile client app; works with Android and iOS devices)
	SMS delivery of one-time passwords
	Hardware tokens (while the solution does not require hardware tokens to work, it supports all event-based HOTP tokens that are OATH-compliant)
	Custom methods (e.g. via email)
Server Side	Out-of-the-box solution
	Easy double-click installation and setup
	The installer automatically recognizes the OS and selects all suitable components
	Interactive installer, drop-in installation into ADFS
Custom Integration Options	In Active Directory environment, use either ESET Secure Authentication API or User Management API for easy integration into proprietary systems
	SDK allows for implementation for non-Active Directory users
Remote Management	Via Microsoft Management Console (MMC)
	Active Directory integration for easy user management
	ESET Secure Authentication extends Active Directory Users & Computers (ADUC plugin) with additional features to enable management of users' two-factor authentication settings

Supported platforms overview

For detailed technical requirements, please consult the ESET Secure Authentication product manual, available at this address:
http://download.eset.com/manuals/eset_esa_product_manual_enu.pdf

Remote Login Platforms	**Remote Desktop Protocol**	
	VPN Protection: Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall	
Local Login Protection (Windows)	Windows 7, 8, 8.1, 10	Windows Server 2008 R2 and later
Active Directory Federation Services	Microsoft ADFS 3.0 (Windows Server 2012 R2)	
Supported VDI Platforms	VMware Horizon View	Citrix XenApp
Microsoft Web Applications	Microsoft Exchange 2007	Microsoft Dynamics CRM 2011, 2013, 2015, 2016
	— Outlook Web Access	Microsoft SharePoint 2010, 2013, 2016
	Microsoft Exchange 2010	Microsoft SharePoint Foundation 2010, 2013
	— Outlook Web App	Microsoft Remote Desktop Web Access
	— Exchange Control Panel	Microsoft Terminal Services Web Access
	Microsoft Exchange 2013, 2016	Microsoft Remote Web Access
	— Outlook Web App	
	— Exchange Admin Center	
Custom Integration	ESET Secure Authentication easily integrates with your RADIUS-based services, as well as via the ESET Secure Authentication API or the User Management API to your existing Active Directory-based authentication. Non Active Directory customers with custom systems can use the easy-to-deploy SDK.	
Operating Systems (Server Side)	Windows Server 2003 (32&64bit), 2003 R2 (32&64bit), 2008 (32&64bit), 2008 R2, 2012, 2012 R2, 2016	
	Windows Small Business Server 2008, 2011	
	Windows Server 2012 Essentials, 2012 R2 Essentials, 2016 Essentials	
	Management tools are also supported on client operating systems from Windows XP SP3 onwards, in both 32-bit and 64-bit versions.	
Supported Mobile Phone Platforms (Client-Side App)	iOS	BlackBerry
	Android	Symbian – all supporting J2ME
	Windows Phone	All J2ME enabled phones
	Windows Mobile	