ESET

SECURE
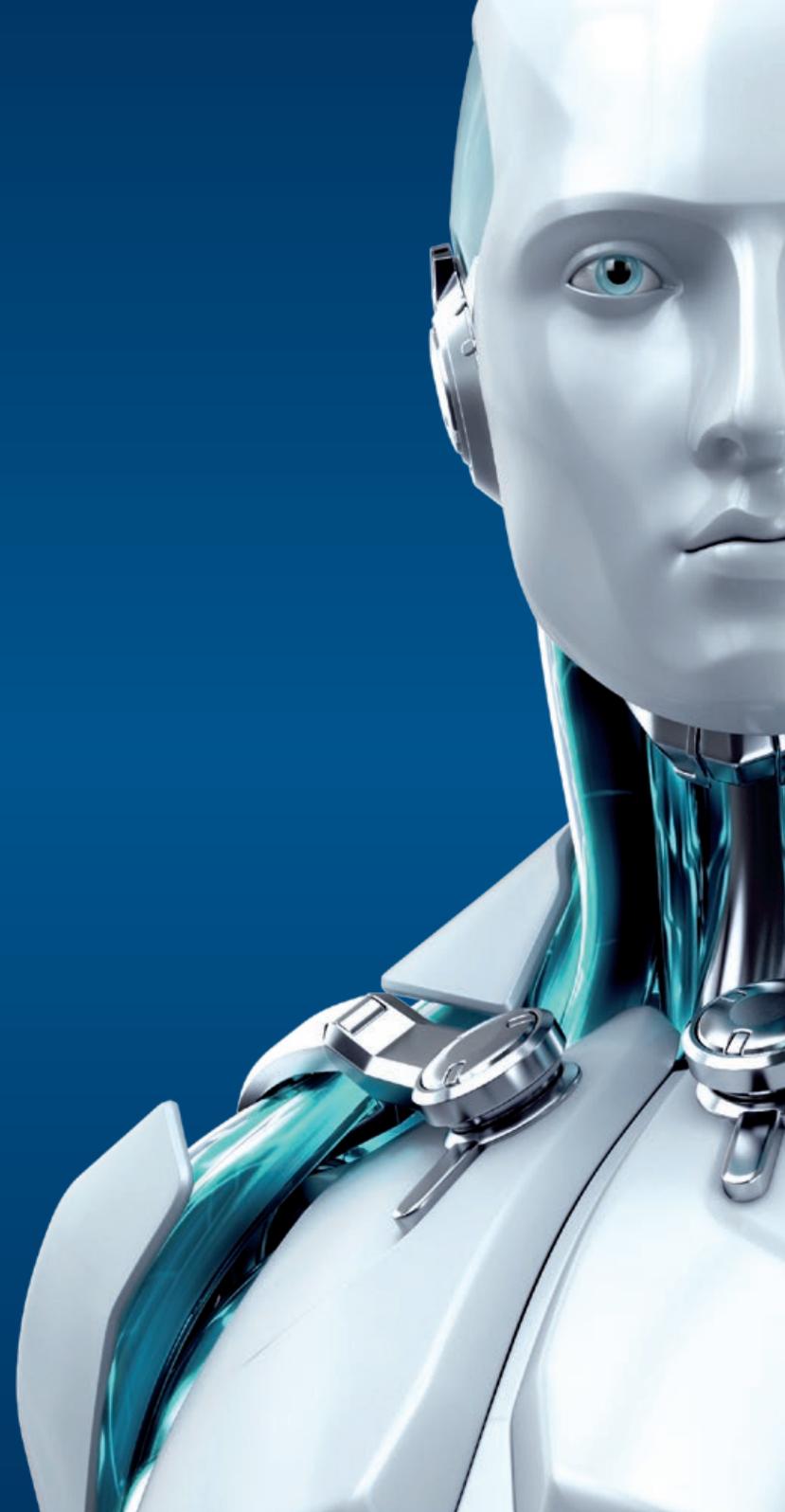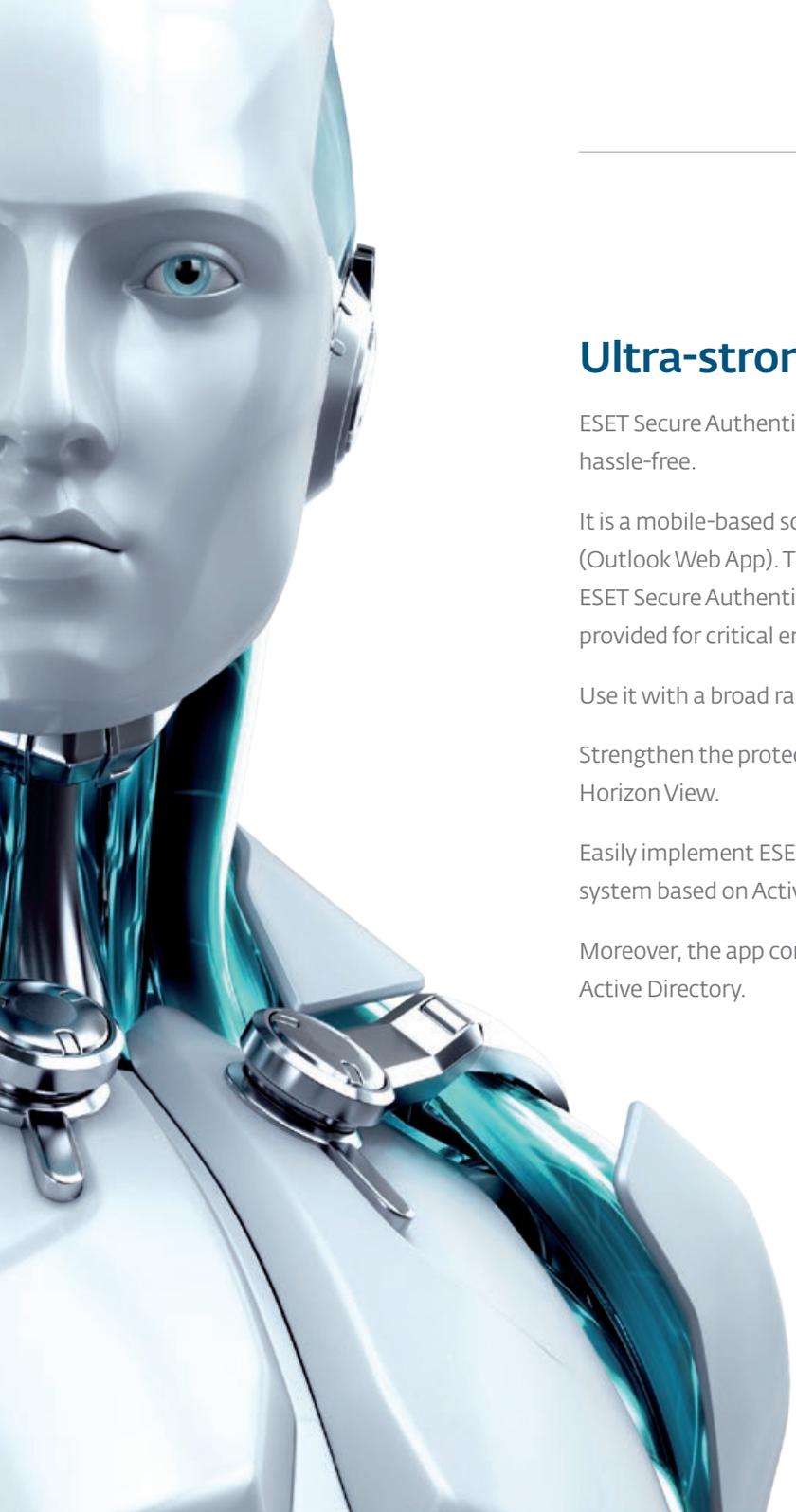## AUTHENTICATION

ENJOY SAFER TECHNOLOGY™

Ultra-strong authentication to protect network access and assets

ESET Secure Authentication provides powerful authentication to make remote access to the company network and sensitive data safe, but hassle-free.

It is a mobile-based solution that uses two-factor, one time password (2FA OTP) authentication for accessing the company's VPN and OWA (Outlook Web App). The advantage of one-time passwords (OTPs) is that they are randomly generated and can't be predicted or reused. ESET Secure Authentication natively supports Outlook Web Access/App for Microsoft Exchange 2007, 2010 and 2013. Native support is also provided for critical endpoints such as the Exchange Control Panel in 2010 and the Exchange Administration Centre in 2013.

Use it with a broad range of business tools, including Microsoft SharePoint, and Microsoft Dynamics CRM.

Strengthen the protection of your sensitive data accessed from outside the company - via a Remote Desktop Web Access login or VMware Horizon View.

Easily implement ESET Secure Authentication to your RADIUS-based services or use the API to integrate it with your existing authentication system based on Active Directory. The solution also supports integration of existing hardware tokens.

Moreover, the app comes with an SDK that enables you to implement the solution into any proprietary system, without the need to use Active Directory.

How does ESET Secure Authentication work?

Employees, upon remotely accessing the company network, receive a one-time password on their mobile phones (or use their current hardware token password). This password is then used to complement and strengthen the usual authentication process.

As a result, the company data and assets are protected against intruders, dictionary attacks, password guessing and other forms of cybercrime. The technology used is two-factor, one time password authentication.

Two-factor Authentication (2FA) explained

As opposed to the standard password authentication, 2FA OTP uses two elements. These are "something that the user knows", such as a password or a PIN code, and "something that the user has", typically a mobile phone or hardware token. Used in combination, they provide greatly enhanced security for data access.
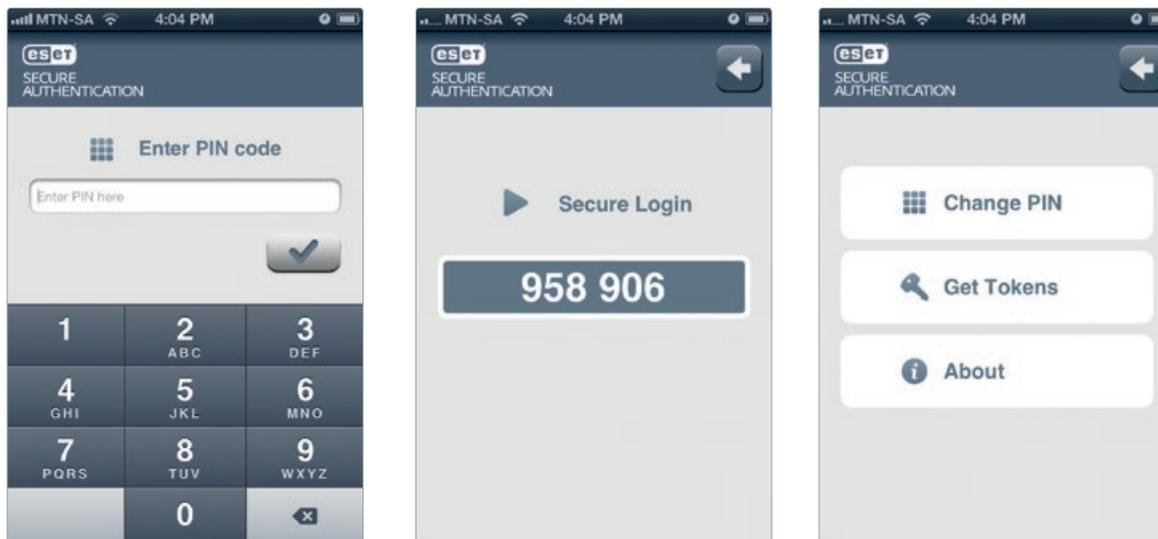
Solves the problem of:

- Static passwords that can be intercepted
- User-created passwords that are not a random combination of characters and can be easily guessed
- Re-use of passwords intended for access to company assets for private accounts
- Passwords containing user-specific data – e.g. a name, a date of birth
- Simple patterns to derive new passwords, such as "peter1", "peter2", etc.

Business benefits

- Helps prevent the risk of breaches with unique passwords for each access
- Protects from poor password practices
- Saves costs - no additional hardware needed
- Easy to migrate to and use
- Supports existing hardware tokens to meet compliance requirements
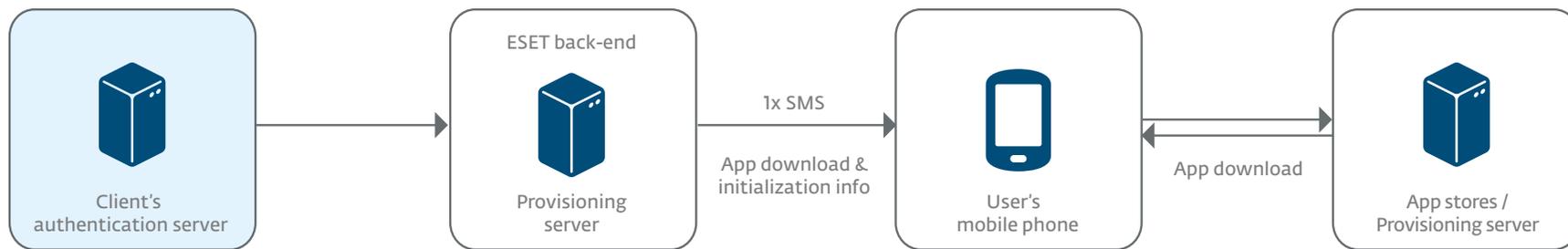
IT benefits

- API/SDK for easy integration into proprietary software and business tools
- App works without internet connection (once downloaded)
- Works with most VPN appliances
- Supports most types of mobile operating systems
- Global technical support in local languages
- Out-of-the-box solution
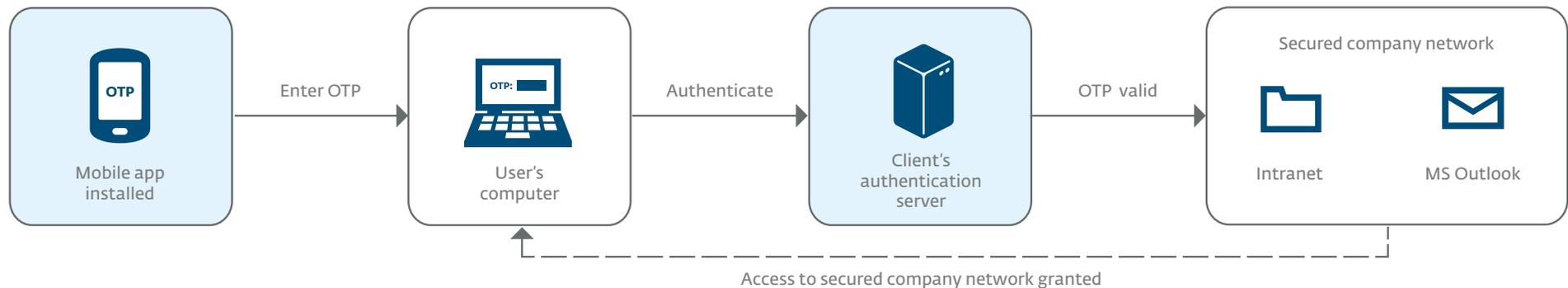
ESET ENJOY SAFER TECHNOLOGY™

A closer look

The architecture of ESET Secure Authentication is designed to only use your existing company infrastructure. In addition to the ESET Secure Authentication app on employee mobiles – the client side – it contains a server application that seamlessly integrates with the familiar network administrator environment of the MMC (Microsoft Management Console) and ADUC (Active Directory Users & Computers). With the authentication API, you can integrate ESET Secure Authentication with an existing authentication system. Moreover, the app's SDK enables integration of the solution into any proprietary system, without the need to use Active Directory. Take advantage of native support of Microsoft Exchange Server 2013, VMware Horizon View, Citrix XenApp and many VPNs. The solution is also easily implemented with hardware tokens (used in place of employee mobile phones).

To distribute the ESET Secure Authentication app on mobile phones, all you need to know is the employee phone number. ESET Secure Authentication will send the user an SMS with an activation link. Clicking on the link automatically downloads an installer for that mobile platform.

Installation and first initialization

Client side communication

Datasheet

Two-factor Authentication	Mobile-based, two-factor (2FA) one-time password (OTP) authentication for a higher level of security
	Native protection of Outlook Web App (OWA), Remote Desktop Protocol, VPNs and all RADIUS-based services
	Native support of Microsoft Exchange and other business tools
	Software only solution – no need to carry additional device or token
	Convenient for the mobile workforce
	Support for hardware tokens
Client Side (mobile app)	One-tap installation, simple and effective user interface
	Delivery of OTP via client application, SMS or hardware token
	OTP generation works independently of an available internet connection
	Compatible with any mobile phone supporting SMS messaging
	Supports a broad range of mobile operating systems
	PIN-protected access to prevent fraud in case of device theft or loss
	Serves multiple OTP zones, e.g. OWA access, VPN access, and others
	Apps available in these languages: English, German, Russian, French, Spanish, Slovak
Server Side	Out-of-the-box solution
	Easy double-click installation and setup
	The installer automatically recognizes OS and selects all suitable components
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	Supports Microsoft Management Console (MMC)
	Active Directory integration
	ESET Secure Authentication extends Active Directory Users & Computers (ADUC plugin) with additional features to enable managing the users' two-factor authentication settings

ESET   ENJOY SAFER TECHNOLOGY™

Supported platforms overview

Remote Login Platforms	Remote Desktop Protocol	
	VPN Protection:	
	Barracuda	F5 FirePass
	Cisco ASA	Fortinet FortiGate
	Citrix Access Gateway	Juniper
	Citrix NetScaler	Palo Alto
	Check Point Software	SonicWall
	Cyberoam	

Supported VDI Platforms	VMware Horizon View	Citrix XenApp

Microsoft Web Applications	Microsoft Web Applications	Microsoft Dynamics CRM 2011, 2013
	Outlook Web Access	Microsoft SharePoint 2010, 2013
	Microsoft Exchange 2010	Microsoft Remote Desktop Web Access
	Outlook Web App	Microsoft Terminal Services Web Access
	Exchange Control Panel	Microsoft Remote Web Access
	Microsoft Exchange 2013	
	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
	Windows Small Business Server 2008, 2011
	Windows Server 2012 Essentials, 2012 R2 Essentials
	Management tools are also supported on client operating systems from Windows XP SP3 onwards, in both 32-bit and 64-bit versions.

Mobile Phone Operating Systems (Client Side App)	iOS 4.3 or higher (iPhone)	BlackBerry 4.3 to 7.1 and 10 and higher
	Android 2.1 or higher	Symbian - all supporting J2ME
	Windows Phone 7 or newer	All J2ME enabled phones
	Windows Mobile 6	

For full compatibility details please contact your ESET representative or consult the product manual

Contact information:

eset ENJOY SAFER TECHNOLOGY™