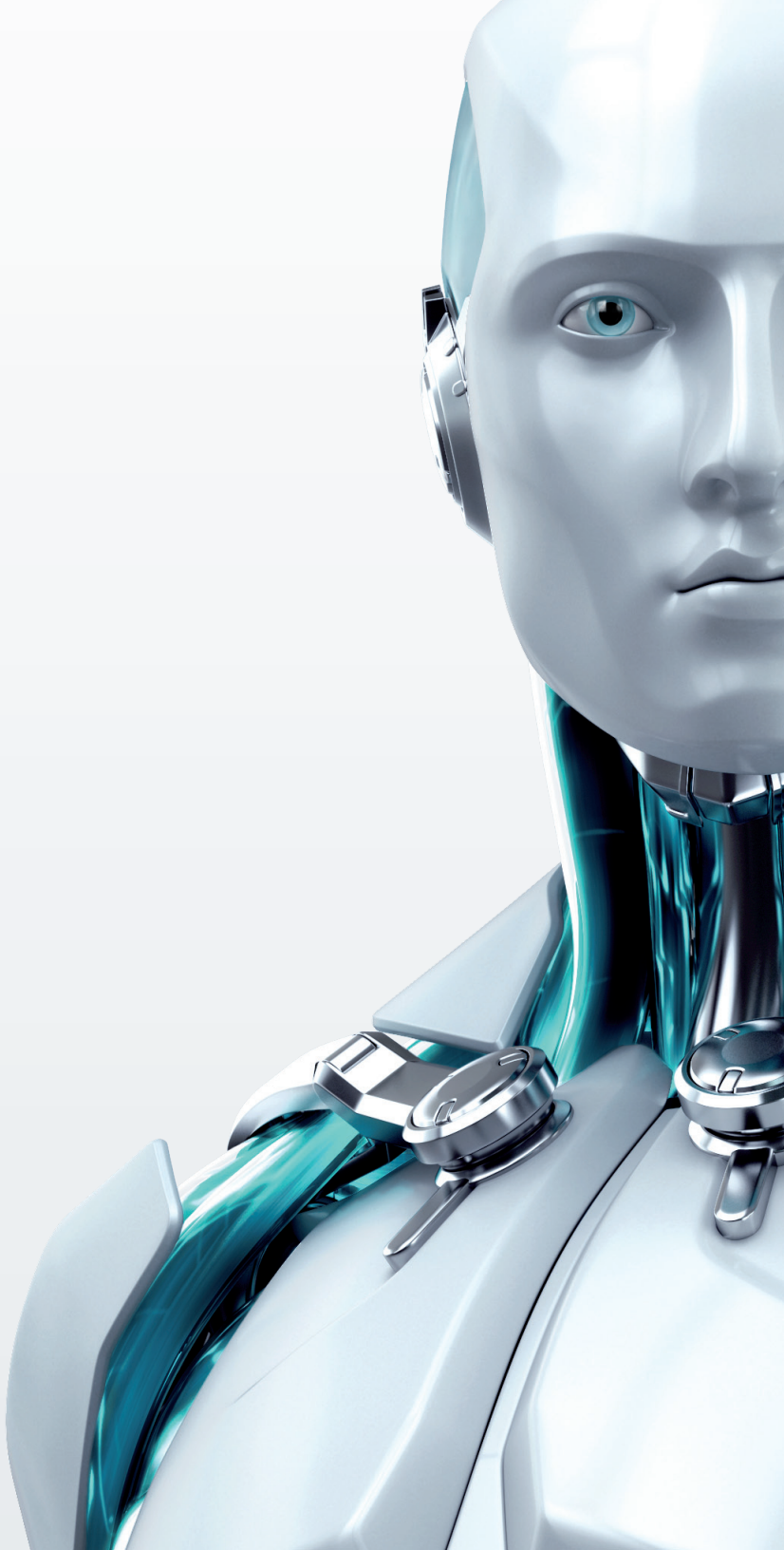
Solutions Overview

ESET® SECURE AUTHENTICATION



eset Proven. Trusted.

ESET Secure Authentication protects passwords and prevents data breaches

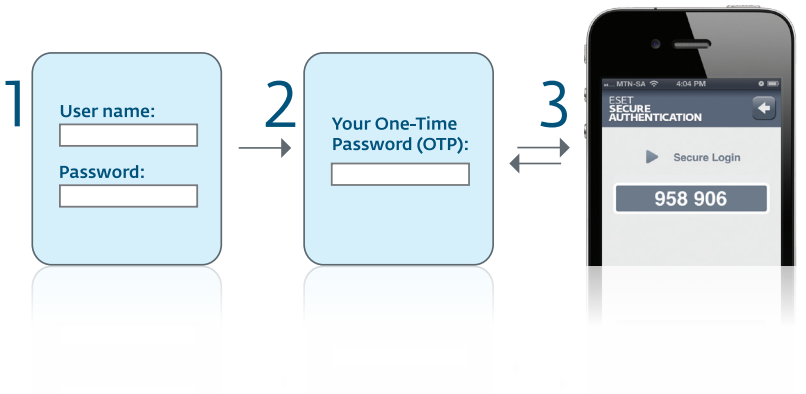
Weak passwords cause real problems. With millions of passwords compromised each year, many companies have already experienced data loss, damage to their reputations and decreased revenue. Cybercriminals don't just focus on the largest enterprises. Poor passwords and unsecured remote network access make every business a potential target. Smaller businesses can now enjoy the same level of protection that larger enterprises employ with ESET Secure Authentication: the easiest and quickest way to implement powerful two-factor authentication (2FA) for businesses of any size.

ESET Secure Authentication delivers a 100% software solution to validate each VPN and Outlook Web Access (OWA) session login with a unique one-time-password (OTP) — adding a critical layer of protection against unauthorized access to sensitive network data. It is easy to set up and manage via a simple Microsoft® Management Console (MMC) snap-in and a cross-platform mobile application. In addition to providing enhanced 2FA security, ESET Secure Authentication also helps companies comply with industry regulations that require strict controls on data privacy, such as PCI DSS, HIPAA, FFIEC Guidelines, Sarbanes-Oxley and NIST.

How does ESET Secure Authentication work?

Unlike standard password authentication, 2FA OTP requires two elements: a user's existing password and a unique OTP sent on-demand to a designated physical device like a mobile phone. Each subsequent login requires a new OTP. Should a cybercriminal compromise a user's existing password, ESET still protects the network and denies access. Without a known device providing access to the second authentication factor, a cybercriminal cannot obtain the required OTP from the ESET Secure Authentication mobile application. Access denied. Network secured.

The mobile application requires no IT help to install on the client-side and very little training to use. The server-side integration and management are equally simple, making ESET Secure Authentication much less expensive to own when compared to other 2FA solutions. Total cost of ownership (TCO) favors the ESET solution.



The makings of a risky password

- Cybercriminals can intercept static passwords and maliciously use them to gain network access
- Users seldom create strong passwords that contain the recommended length and combination of random characters
- People often use the same password for both work and personal accounts, creating risk if just one of these is compromised
- Passwords containing user-specific data such as a name or date of birth can be compromised if the cybercriminal knows this personal information
- Passwords with simple patterns such as "myname1" or "myname2" are easy to hack

Business benefits

- Reduces the risk of data breaches with a unique OTP for each session
- Validates user identity as a fraud prevention measure for those attempting to access privileged or confidential information
- Satisfies regulatory compliance where strong authentication is recommended or required
- Offers low cost of ownership because no hardware tokens, server or appliances are required

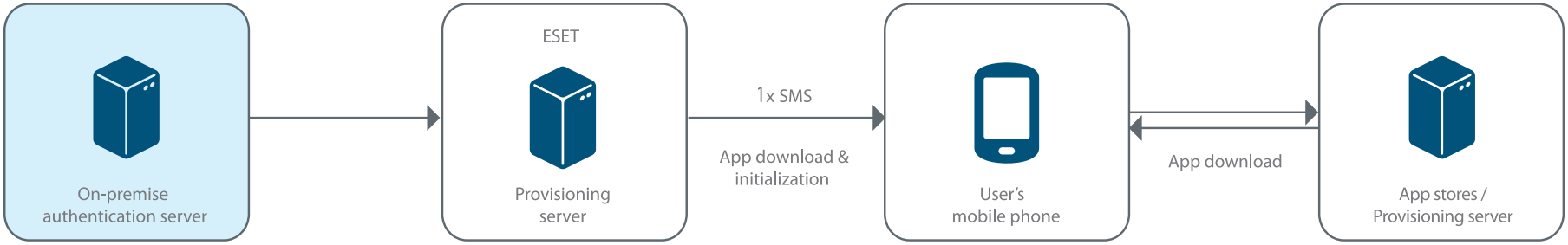
IT staff benefits

- Direct integration with Microsoft management tools
- Easy installation with self-provisioning for end users frees up IT resources
- Connectionless operation as the deployed mobile application works without Internet connection
- Multi-platform support for leading mobile operating systems
- Saves costs without additional hardware or external database requirements
- Convenient support from U.S.-based technical support team

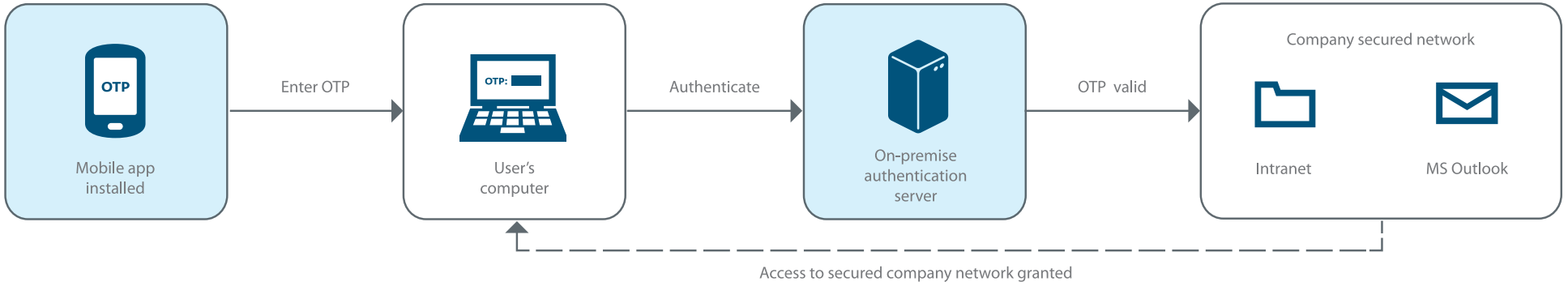
A closer look

ESET Secure Authentication is designed to only use your existing company infrastructure. In addition to installing the ESET Secure Authentication mobile application on employee mobile devices – the client side – a server application seamlessly integrates with the familiar network administrator environment of the Microsoft Management Console (MMC) and Active Directory Users & Computers (ADUC). To distribute the ESET Secure Authentication application to mobile phones, all you need is the employee's phone number. ESET Secure Authentication server application sends the user an SMS with an activation link. Clicking on the link automatically downloads an installer for that mobile platform. Access to the mobile application is also PIN-protected to prevent unauthorized manipulation.

Installation and first initialization



Client side communication



Product highlights

Two-factor authentication (2FA)

- HMAC-based OATH-compliant one-time password delivered through mobile applications
- Native protection for Outlook Web Access (OWA), VPNs and all RADIUS-based services
- Mobile application-based solution means no need to carry yet another hardware device or token
- Convenient for a mobile workforce and companies with a BYOD policy

Client side (mobile application)

- One-tap installation, simple, effective user interface
- One-time password (OTP) delivery via mobile application or SMS
- Internet connection not required for mobile application to generate OTPs
- Compatible with any mobile phone supporting SMS messaging
- Supports broad range of mobile operating systems
- PIN-protected access to prevent fraud in case of device theft or loss

Server side (Windows® application)

- Out-of-the-box solution
- Easy double-click installation and setup
- Installer automatically recognizes OS and selects all suitable components

Remote management

- Supports Microsoft Management Console (MMC)
- Active Directory Users & Computers (ADUC snap-in for managing the two-factor authentication user settings)

ESET North America
610 West Ash Street
Suite 1700
San Diego, CA 92101

Toll Free: +1 (866) 343-3738
Tel. +1 (619) 876-5400

Proven. Trusted.

System requirements:

Server side

32&64-bit versions of Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012

Client side (mobile application)

iOS 4.2.1 or higher (iPhone®), Android™ 2.1 or higher, Windows Phone 7 or newer, Windows Mobile 6, BlackBerry® 4.3 to 7.1, Symbian® – all supporting J2ME, All J2ME-enabled phones