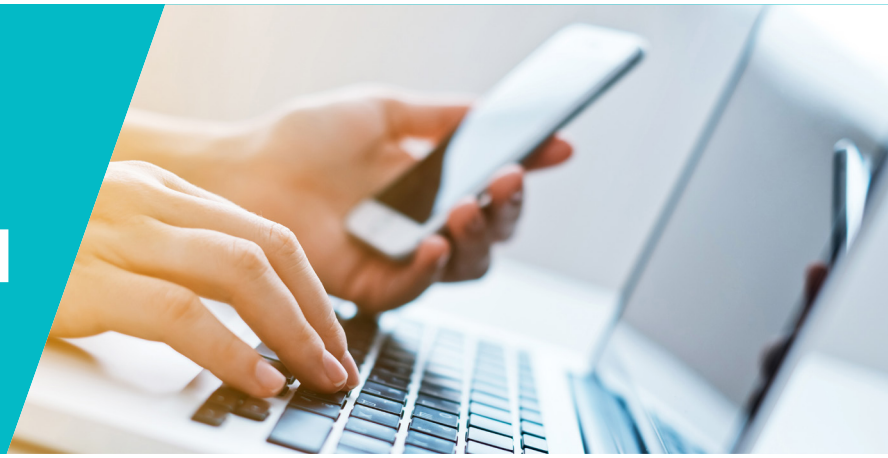
CONTACT SALES
1-844-824-3738

ESET SECURE AUTHENTICATION



What it is

ESET Secure Authentication (ESA) is a mobile-based solution for two-factor authentication (2FA).

2FA adds an essential layer of protection against data breach by requiring two independent pieces of information to verify a user's identity when they attempt to log in or access data. In addition to their usual password, users must enter a one-time password generated on their mobile device.

ESET Secure Authentication provides an easy way for businesses of all sizes to implement 2FA across commonly used systems such as VPNs, Remote Desktop Protocol, Office 365, Outlook Web Access, etc. Compatible with all iOS and Android smartphones, it can also integrate with the devices' biometrics (Touch ID, Face ID, Android fingerprint) for increased security and better user experience.

Why you need it

One of the most common ways hackers can gain access to your company's data is by guessing weak passwords; stealing passwords via automated bots, phishing and targeted attacks; or purchasing leaked credentials in bulk via the Dark Web.

By deploying ESA, your business makes it much harder for hackers to gain access to your systems and data. The stolen password won't work without the one-time code generated on the authorized user's phone or tablet.

Key benefits

- Works with iOS, Android and Windows mobile phones
- Push authentication lets you authenticate with a single tap
- Saves money—no dedicated hardware necessary
- Supports compliance requirements for multi-factor authentication
- Supports desktop logins, VPN and cloud applications

80%: Hacking-related breaches in 2018 that involved weak, compromised or stolen credentials

(Verizon 2019 Data Breach Investigations Report).

$3.92M: Global average total cost of a data breach in 2019

(IBM Security Cost of a Data Breach Report 2019)

$1.42M: Average cost to a company of lost business due to data breach

(IBM)