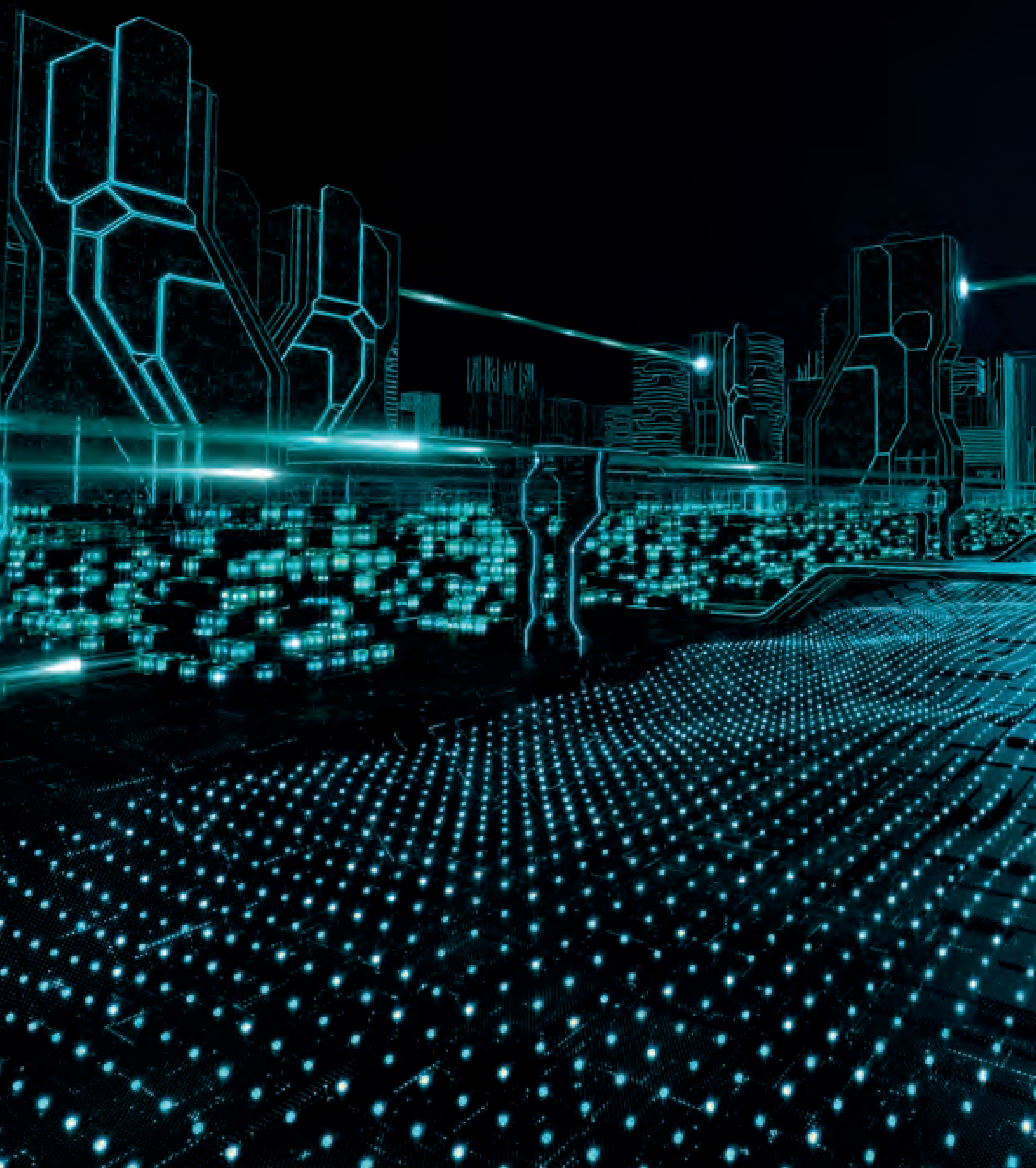
SOLUTION OVERVIEW

SECURE AUTHENTICATION

Multi-factor authentication from a leading cybersecurity provider that is easy to implement and use

CYBERSECURITY
EXPERTS ON YOUR SIDE



What is **multi-factor authentication?**

Multi-factor authentication (MFA), also known as two-factor authentication (2FA), is an authentication method which requires two independent pieces of information to verify a user's identity. MFA is much stronger than using a traditional, static password or PIN authentication. By complementing traditional authentication with a dynamic second factor, it effectively reduces the risk of data breaches caused by weak or leaked passwords.

ESET Secure Authentication provides an easy way for businesses of all sizes to implement MFA across commonly utilized systems such as VPNs, Remote Desktop Protocol, Office 365, Outlook Web Access, operating system login and more.

Why **multi-factor authentication?**

> Not only do employees utilize the same password across multiple websites and applications, they sometimes freely share their passwords with friends, family and co-workers.

POOR PASSWORD HYGIENE

As the saying goes, “employees are your weakest link” – and employees can put your business at risk in many ways. One of the biggest dangers is poor password hygiene. Not only do employees utilize the same password across multiple websites and applications, they sometimes freely share their passwords with friends, family and co-workers. If that isn’t a big enough problem, when businesses enforce password policies it usually causes their employees to use variants of their previous password or write their passwords on sticky notes.

A multi-factor authentication solution protects business against poor password hygiene by implementing, on top of the regular password, an additional piece of authentication - e.g. by generating it on the employee’s phone. By having this solution in place, it prevents attackers from gaining access to your systems simply by guessing a weak password.

DATA BREACHES

In today’s cybersecurity landscape, an increasing number of data breaches occur every day. One of the most common ways hackers can gain access to your company’s data is through weak or stolen passwords gathered via automated bots, phishing, or targeted attacks. In addition to just protecting normal users’ logins to critical services, businesses can implement MFA on to all privilege escalations in order to prevent unauthorized administrative access.

By adding a multi-factor solution, your business will make it much more difficult for hackers to gain access to your systems and ultimately compromise them. The top industries for data breaches are traditionally ones that handle valuable data such as financial, retail, healthcare, and the public sector. However, that does not mean that other industries are safe, just that hackers typically weigh the effort required versus the payoff.

COMPLIANCE

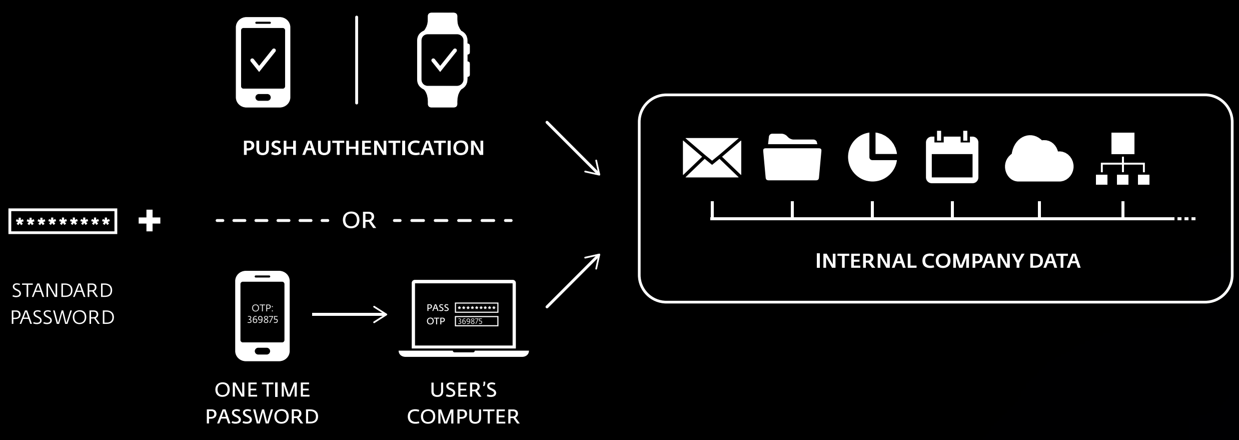
When it comes to compliance, most businesses first need to understand whether they have to meet a compliance target or not. Next, they have to review what measures and recommendations their business must implement in order to comply. When it comes to multi-factor authentication, several regulations such as PCI-DSS and GLBA require that it must be implemented, and many laws, including GDPR and HIPAA, stress the need for stronger authentication.

Multi-factor authentication is no longer an option for most businesses that handle credit cards or financial transactions, but rather a required solution. All businesses should examine which laws and regulations apply to them, and ensure that they comply with their requirements.

One of the most common ways hackers gain access to your company's data is through weak or stolen passwords.

Having this solution in place prevents attackers from gaining access to your systems simply by guessing a weak password.

Authenticate with a single tap, with no need to retype the one-time password.



PUSH AUTHENTICATION

********** +

OR

STANDARD PASSWORD

OTP: 369875

PASS **********
OTP 369875

ONE TIME PASSWORD

USER'S COMPUTER

INTERNAL COMPANY DATA

The ESET difference

SIMPLY CHOOSE YOUR INTEGRATION METHOD

ESET Secure Authentication offers two integration modes - Active Directory integration for organizations using Windows domain, or standalone mode, which is suitable for those without it. Either way, setup and configuration is quick and easy, and the solution is managed via the solution's web console.

NO DEDICATED HARDWARE REQUIRED

All the costs of ESET Secure Authentication are built in as it requires no dedicated hardware. Simply install the solution on a server and start provisioning.

WORKS WITH EXISTING SMARTPHONES

No need for special tokens or devices for employees. ESET Secure Authentication works smoothly on all iOS and Android smartphones, and can integrate with the devices' biometrics (Touch ID, Face ID, Android fingerprint) for increased security and better user experience.

SETS UP IN 10 MINUTES

Many development hours were put into the creation of ESET Secure Authentication to ensure that setup is as easy as possible. We set out to create an application that a small business with no IT staff could set up and configure. Whether your business has five users or thousands of users, ESET Secure Authentication, due to its ability to provision multiple users at the same time, is quick and easy to set up.

FULL API AND SDK INCLUDED

For organizations that want to do even more with ESET Secure Authentication, we include a full-featured API, as well as SDK, that customers can utilize to extend MFA to the applications or platforms that they use - even without a dedicated plugin.

PUSH AUTHENTICATION

Lets you authenticate with a single tap, with no need to retype the one-time password. Works with iOS and Android smartphones.

> *"Single server install, ease of setup, integration with Active Directory and one of the major pluses, an application we could give our staff members so there was no need for constant SMSs. On top of this, the fact it works seamlessly with open VPN made us very happy as we didn't have to change our VPN setup to accommodate the software."*
>
> Tom Wright, IT Service Officer, Gardners Books

Use cases

Prevent data breaches

Businesses appear in the news every single day to alert their customers that a data breach has occurred.

SOLUTION

- ✓ Protect vulnerable communications such as Remote Desktop Protocol by adding multi-factor authentication.
- ✓ Add multi-factor authentication to all VPNs that are utilized.
- ✓ Require multi-factor authentication in order to log in to devices that contain sensitive data.
- ✓ Protect sensitive data with ESET Endpoint Encryption.

ESET PRODUCTS

- ✓ ESET Secure Authentication
- ✓ ESET Endpoint Encryption

Strengthen password protection

Users tend to employ the same passwords across multiple applications and web services, thus putting businesses at risk.

SOLUTION

- ✓ Restrict access to company resources by leveraging multi-factor authentication.
- ✓ Multi-factor authentication reduces the worry and danger associated with shared or stolen passwords by requiring an additional piece of authentication, such as push-message approval.

ESET PRODUCTS

- ✓ ESET Secure Authentication

Verify user login process

Businesses utilize shared computers in shared workspaces and require verification on all parties logging in throughout the workday.

SOLUTION

- ✓ Implement multi-factor authentication for desktop logins on all devices in shared workspaces.

ESET PRODUCTS

- ✓ ESET Secure Authentication

Technical features and protected platforms

PUSH AUTHENTICATION

A single-tap authentication with all iOS and Android smartphones.

OTHER WAYS TO AUTHENTICATE

ESET Secure Authentication supports mobile applications, push notifications, hard tokens and SMS for OTP delivery, as well as FIDO keys and custom methods.

MANAGEMENT FROM ONE PLACE

Via the ESET Secure Authentication web console. Integrates with Active Directory for easy management, or works standalone for organizations without a Windows domain.

PROTECTION SUPPORT

Virtual Private Networks (VPN), Remote Desktop Protocol (RDP), Outlook Web Access (OWA), VMware Horizon View and RADIUS-based services are all natively supported by ESET Secure Authentication.

ADDITIONAL OS PROTECTION

Additional authentication for desktop logins and privilege escalation are also protected by multi-factor authentication.

Supports Windows as well as macOS and Linux.

CLOUD SUPPORT

Add MFA to strengthen access to services such as Google Apps, Office 365, Dropbox, and many others. ESET supports integration via the SAML-2 authentication protocol used by major identity providers.

HARD TOKEN SUPPORT

Even though hard tokens are not required, all event-based HOTP tokens that are OATH-compliant are supported, as well as FIDO2 and FIDO U2F hardware keys.

SUPPORTED VDIS AND VPNS

VMware Horizon View, Citrix XenApp, Barracuda, Cisco ASA, Citrix Access Gateway, Citrix NetScaler, Check Point Software, Cyberoam, F5 FirePass, Fortinet FortiGate, Juniper, Palo Alto, SonicWall.

Support for custom integration with any RADIUS-based VPN.

About ESET

ESET – a global leader in information security – was named as a Challenger in the 2019 Gartner Magic Quadrant for Endpoint Protection Platforms* for the second successive year.

For more than 30 years, ESET® has been developing industry-leading IT security software and services, delivering instant, comprehensive protection against evolving cybersecurity threats for businesses and consumers worldwide.

ESET is privately owned. With no debts and no loans, we have the freedom to do what needs to be done for the ultimate protection of all our customers.

ESET IN NUMBERS

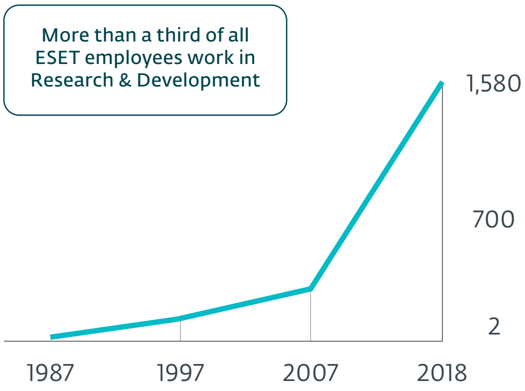
110m+ users worldwide

400k+ business customers

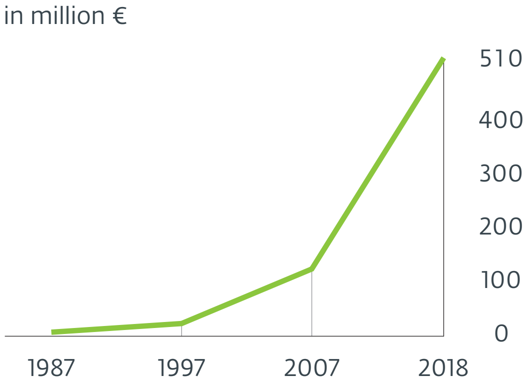
200+ countries & territories

13 global R&D centers

ESET EMPLOYEES



ESET REVENUE



* Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, August 20, 2019. Gartner does not endorse any vendor, product or service depicted in its research publications. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

SOME OF OUR CUSTOMERS

MITSUBISHI MOTORS
Drive your Ambition

Protected by ESET since 2017

more than 14,000 endpoints

Canon
Canon Marketing Japan Group

Protected by ESET since 2016

more than 9,000 endpoints

Allianz
Suisse

Protected by ESET since 2016

more than 4,000 mailboxes

T · ·

ISP security partner since 2008

2 million customer base

SOME OF OUR TOP AWARDS

AV TEST av-test.org 10/2019 APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS

G2 Leader FALL 2019

THE CHANNEL CO. CRN ★★★★★ PARTNER PROGRAM GUIDE WINNER 2019

AV comparatives APPROVED Business Security JUL 2019

SC MEDIA RECOMMENDED

> *“Given the good features for both anti-malware and manageability, and the global reach of customers and support, ESET should be on the shortlist for consideration in enterprise RFPs for anti-malware solutions.”*
>
> KuppingerCole Leadership Compass
> Enterprise Endpoint Security: Anti-Malware Solutions, 2018

ENJOY SAFER
TECHNOLOGY™