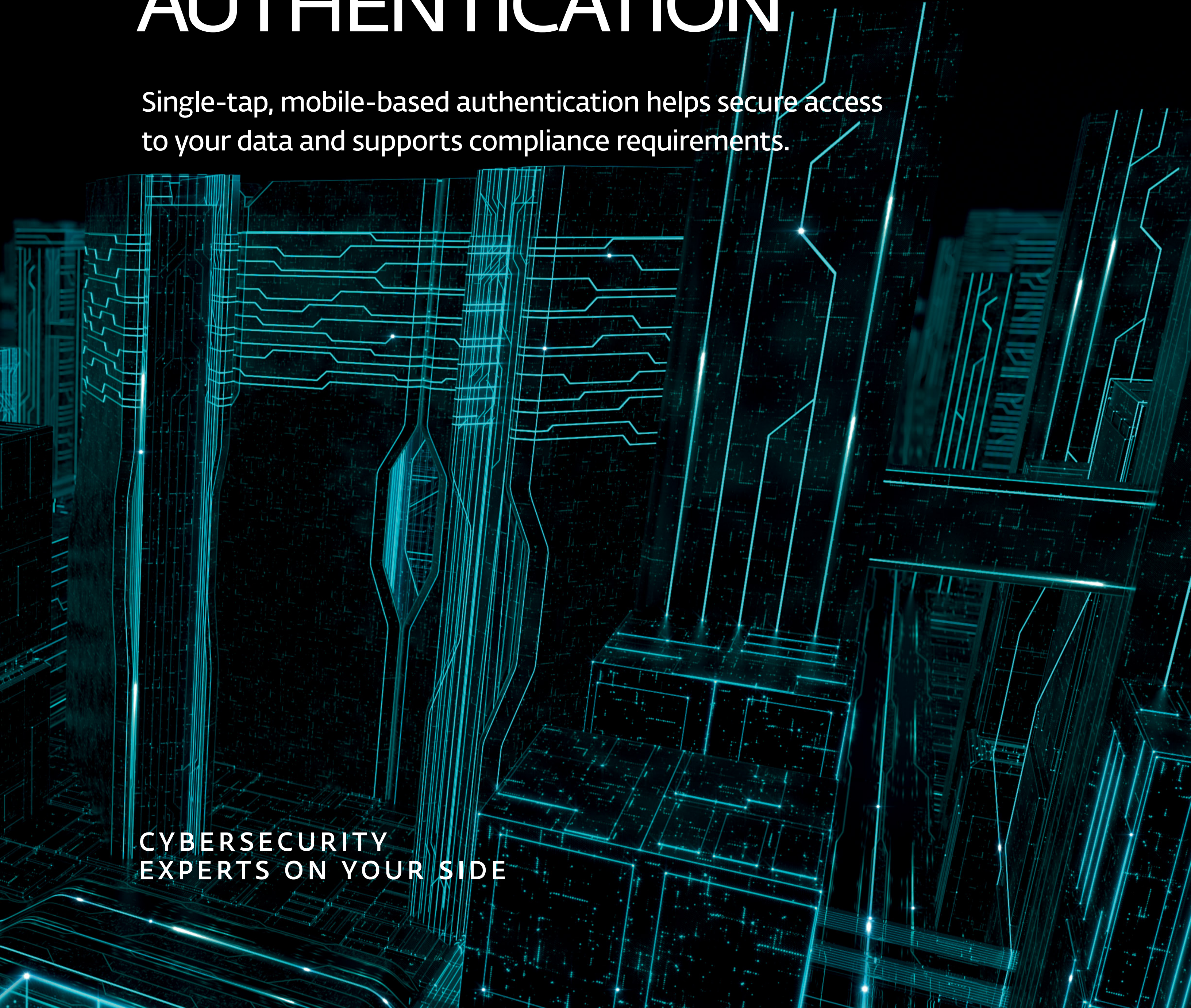
SOLUTION OVERVIEW

ESET SECURE AUTHENTICATION

Single-tap, mobile-based authentication helps secure access to your data and supports compliance requirements.



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. 2FA is much stronger than traditional, static password or PIN authentication. By complementing the 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, Office 365, Outlook Web Access, operating system login and more.

Why **multi-factor authentication?**

> Not only can 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

The saying “Employees are your weakest link” comes from their potential to put your business at risk—for example, with poor password hygiene. Some workers use the same password across multiple sites and applications, and share passwords with friends and co-workers. Enforcing password policy can also be difficult, as employees often use variations of similar words or write 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 password by generating it on the employee’s phone. Having this solution in place prevents attackers from gaining access to your systems by guessing weak passwords.

DATA BREACHES

Implementing multi-factor authentication (also known as two-factor authentication, or 2FA) is an effective way to reduce data breaches. It mitigates weak or stolen passwords, both of which are used by hackers to gain access to your data. Multi-factor authentication can also be implemented to limit privilege access and control privilege escalation to prevent unauthorized administrative access by employees.

The top industries for data breaches are traditionally ones that have valuable data: financial, retail, healthcare and the public sector. This doesn’t mean other industries are safe; it’s simply that hackers typically weigh effort required versus the potential payoff.

COMPLIANCE

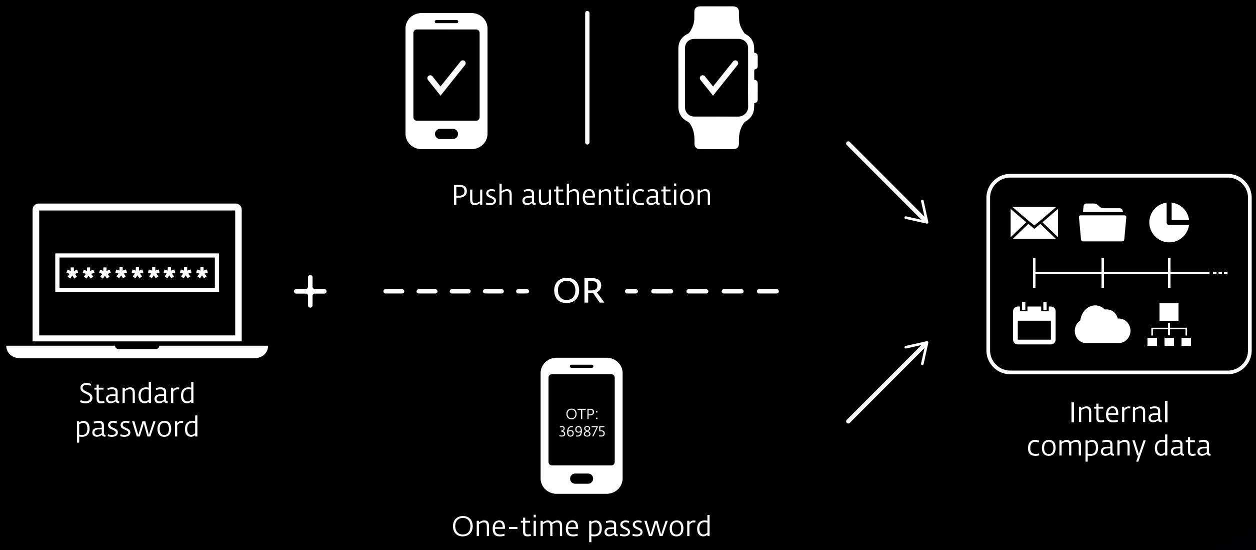
When it comes to compliance, businesses need to determine whether they are subject to compliance requirements. Next, they must review the specific actions that compliance regulations either recommend or require. A number of compliance regulations require the use of 2FA, including PCI-DSS and GLBA. Others, like HIPAA, simply recommend using it.

For most businesses that handle credit cards or financial transactions, 2FA is no longer an optional solution but a requirement. No matter what business you’re in, it pays to know which compliance regulations affect you and how to meet them.

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 by simply guessing a weak password.

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



Push authentication

Standard password

+ ------ OR ------

One-time password

Internal company data

The ESET difference

SIMPLY CHOOSE YOUR INTEGRATION METHOD

ESET Secure Authentication was designed to work as a standalone solution, operated via a web console. In a Windows Domain environment, you can choose to integrate with Active Directory. This makes setup and configuration quick and easy, and eliminates any additional training to deploy 2FA in your organization.

NO DEDICATED HARDWARE REQUIRED

All the costs of ESET Secure Authentication are built in as it requires no dedicated hardware. Simply install the 10MB application on any server and start provisioning.

WORKS WITH EXISTING SMARTPHONES

No need for special tokens or devices for employees. ESET Secure Authentication works with all types of smartphones.

QUICK AND EASY SETUP

Many development hours were put into the creation of ESET Secure Authentication to ensure that setup was 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 a business has five users or 100,000 users, ESET Secure Authentication, with its ability to provision multiple users at the same time, keeps setup time to a minimum.

FULL SDK AND API INCLUDED

For enterprises or companies that want to do even more with ESET Secure Authentication, we include a full SDK and API that businesses can use to extend the functionality to fit their needs.

PUSH AUTHENTICATION

Lets you authenticate with a single tap, with no need to retype the one-time password. Works with iOS, Android and Windows 10 mobile phones.

> *“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

Every day, it seems another business is having to notify customers that a data breach has occurred.

SOLUTION

✓ Protect vulnerable communications such as Remote Desktop by adding multi-factor authentication.

✓ Add multi-factor authentication to all VPNs being 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

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

Strengthen password protection

Users utilize the same passwords across multiple applications and web services, putting a business at risk.

SOLUTION

✓ Restrict access to company resources by leveraging multi-factor authentication.

✓ Requiring multi-factor authentication reduces the worry associated with shared or stolen passwords by requiring an OTP in addition to a password.

ESET PRODUCTS

✓ ESET Secure Authentication

Technical features and protected platforms

PUSH AUTHENTICATION

A single-tap authentication with all iOS, Android and Windows 10 mobile smartphones.

OTHER WAYS TO AUTHENTICATE

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

REMOTE MANAGEMENT

Via the ESET Secure Authentication web console or Microsoft Management Console (MMC). 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

In addition to on-premise applications, ESET Secure Authentication also supports web/cloud services such as Google Apps and Microsoft ADFS 3.0 (including Office 365).

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 VPNS

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

About ESET

ESET—a global player in information security—has been named as the only challenger in the 2018 Gartner Magic Quadrant for Endpoint Protection Platforms.*

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

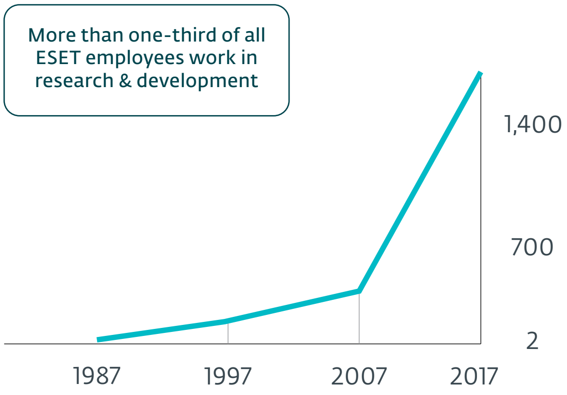
110M+
users worldwide

400K+
business customers

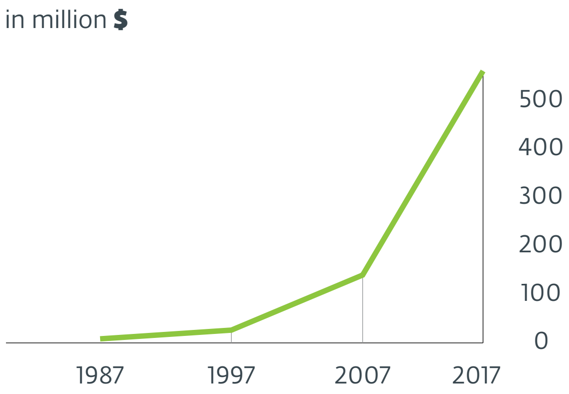
200+
countries & territories

13
global R&D centers

ESET EMPLOYEES


More than one-third of all ESET employees work in research & development

ESET REVENUE



*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

HONDA

protected by ESET since 2011
license prolonged 3 times and expanded 2 times

Canon
Canon Marketing Japan Group

protected by ESET since 2016
more than 14,000 endpoints

Allianz
Suisse

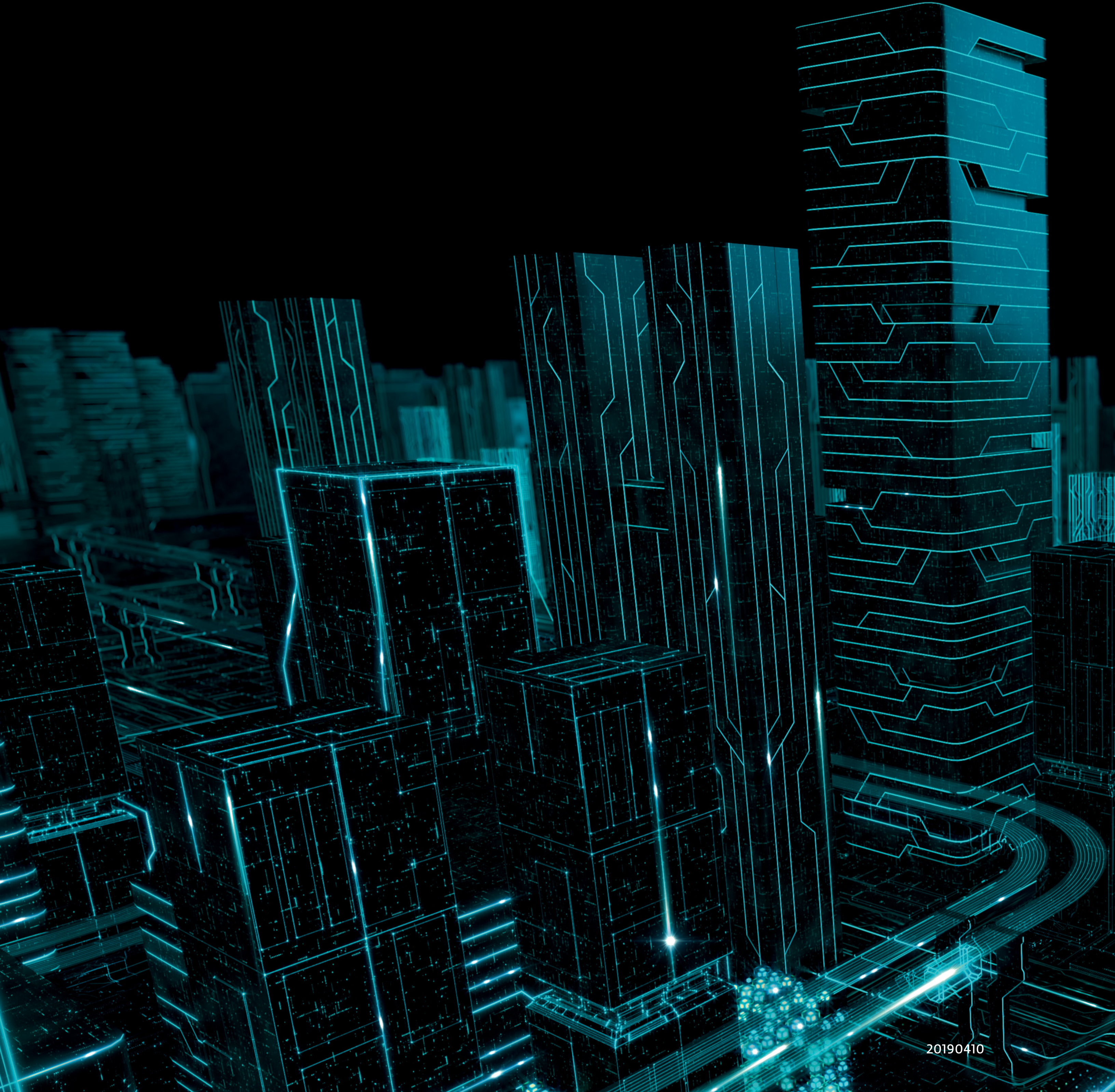
protected by ESET since 2016
more than 4,000 mailboxes

ISP security partner since 2008
2 million customer base

SOME OF OUR TOP AWARDS

> *"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®



20190410