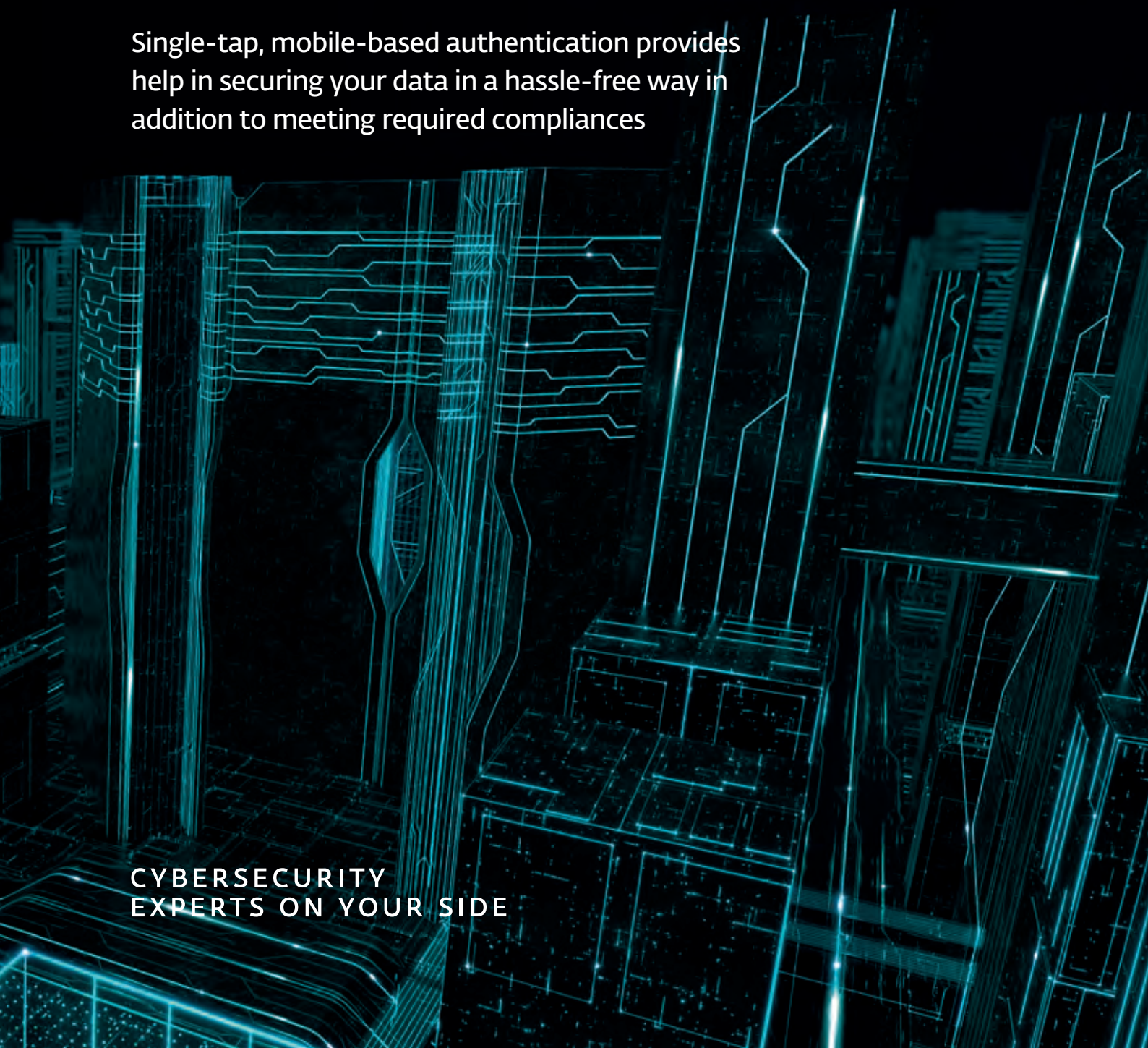
SOLUTION OVERVIEW

SECURE AUTHENTICATION

Single-tap, mobile-based authentication provides help in securing your data in a hassle-free way in addition to meeting required compliances



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 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

The saying goes, "employees are your weakest link" as usually employees put your business at risk in many ways. One of the biggest risks 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 password - 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 by simply guessing a weak password.

DATA BREACHES

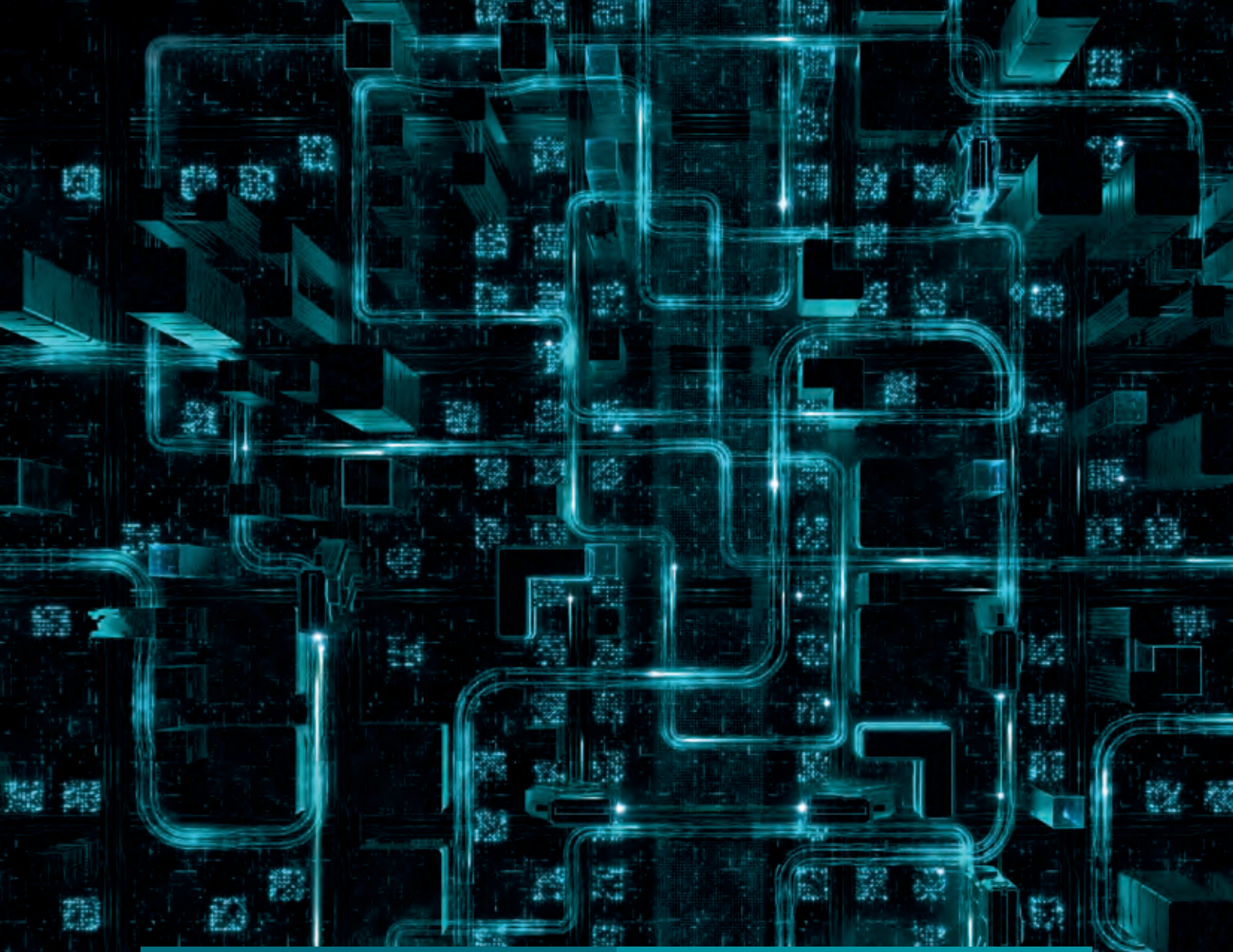
Today's cybersecurity landscape has an increasing number of data breaches happening every day. One of the most common ways hackers can gain access to your company's data is through weak or stolen passwords. In addition, to just protecting normal users logins to critical services, businesses can implement multi-factor authentication on all privilege escalation to prevent unauthorized administrative access.

By adding a multi-factor solution businesses 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 have 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 effort required versus the payoff.

COMPLIANCE

When it comes to compliance, most businesses first need to understand whether they have to meet a compliance or not. Next, they have to review what requirements the compliance recommends and mandates that their business implement. When it comes to multi-factor authentication, now several compliances mandate that it be implemented such as PCI-DSS and GLBA, and most compliances in general stress the need for stronger authentication, including GDPR and HIPAA.

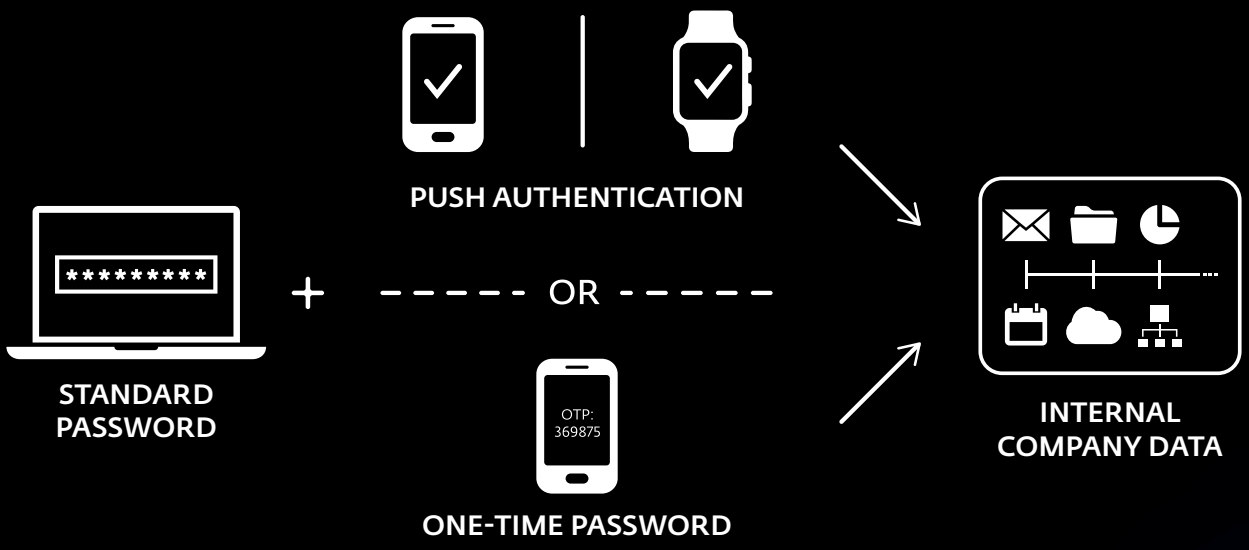
Multi-factor authentication has become no longer an optional solution for most businesses who handle credit cards or financial transactions, but rather a required solution. All businesses should do research and evaluate if they need to abide by certain compliances.



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.



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 a broad range of smartphones.

SETS UP IN 10 MINUTES

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, due to its ability to provision multiple users at the same time, keeps setup time as quick as possible.

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

Businesses are in the news every single day notifying their 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 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 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

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, 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.

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

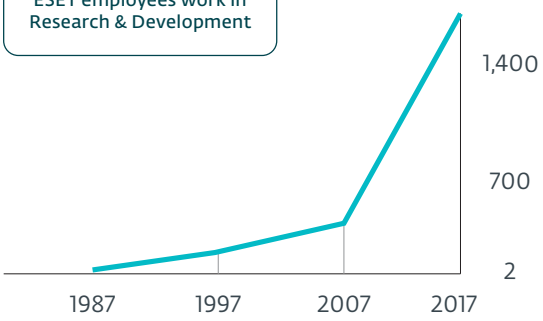
400k+
business customers

200+
countries & territories

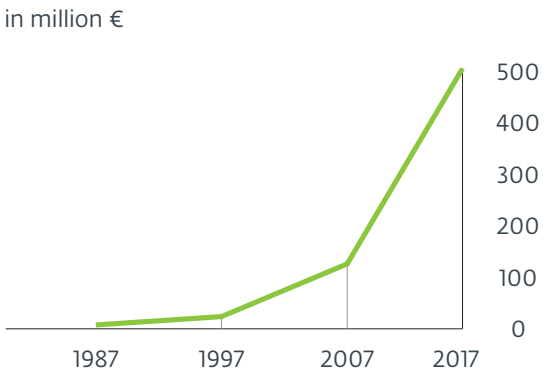
13
global R&D centers

ESET EMPLOYEES

More than a 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 3x, enlarged 2x

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

T

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™

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION