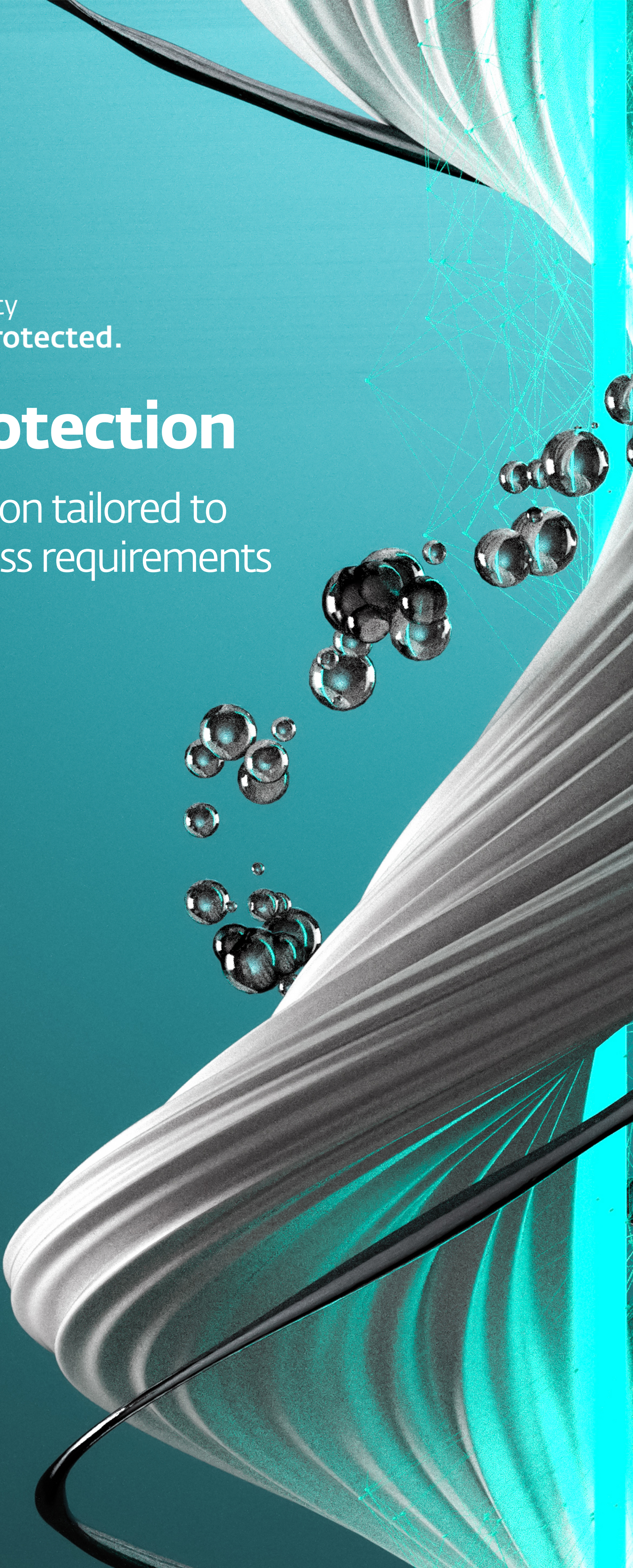
ESET® Digital Security
Progress. Protected.

Advanced Protection

Cloud security protection tailored to meet advanced business requirements



ESET PROTECT COMPLETE

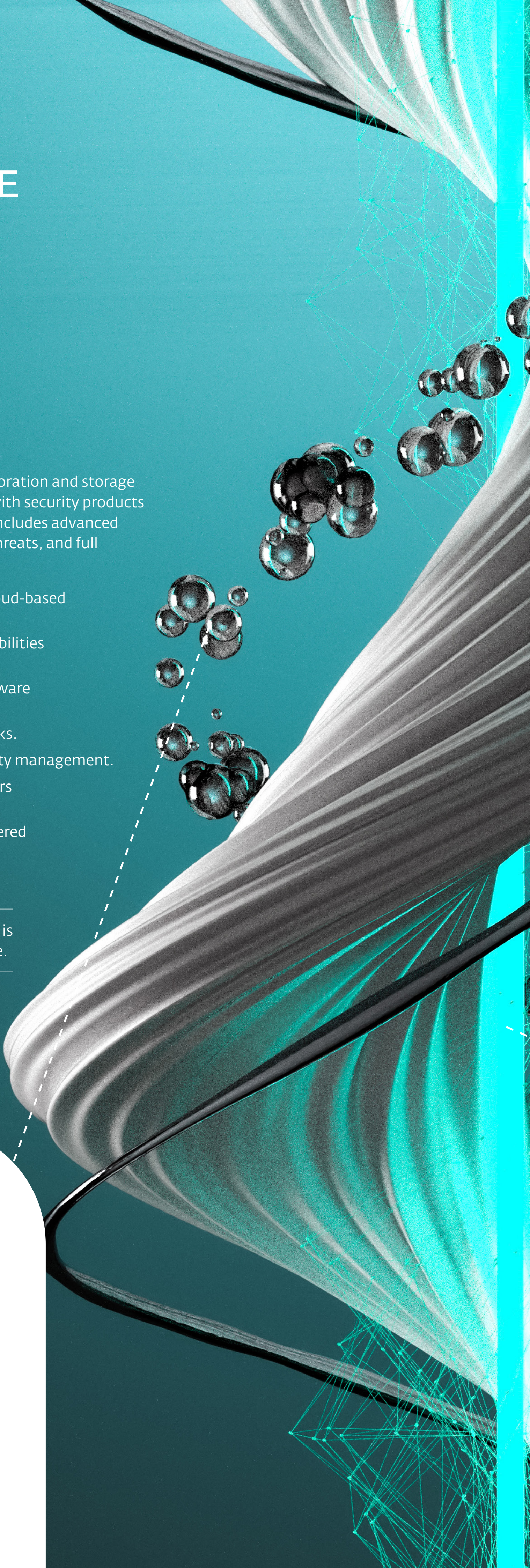
- Management Console
- Endpoint Protection
- File Server Security
- Advanced Threat Defense
- Full Disk Encryption
- Cloud Applications Protection
- Mail Security

Add an extra layer of protection to your Microsoft 365 cloud email, collaboration and storage or mail servers. Protect your company computers, laptops and mobiles with security products all managed via a cloud or on-prem management console. The solution includes advanced threat defense technology, preventing new, never-before-seen types of threats, and full disk encryption capability for enhanced data protection.

- Improved protection against ransomware and zero-day threats via cloud-based sandboxing technology.
- Helps comply with data regulation thanks to full disk encryption capabilities on Windows and macOS.
- Protection against disruption caused by email-based attacks and malware in Microsoft 365 cloud applications.
- Protection of your mail servers from malware, spam or phishing attacks.
- Easily accessible ESET PROTECT Cloud console improves TCO of security management.
- Single-pane-of-glass remote management for visibility to threats, users and quarantined items.
- Company endpoints and mobiles are protected via advanced multilayered technology, now with brute force attack protection.

Digital security on a tight budget? ESET PROTECT Complete On-Prem* is available with onsite deployment of the security management console.

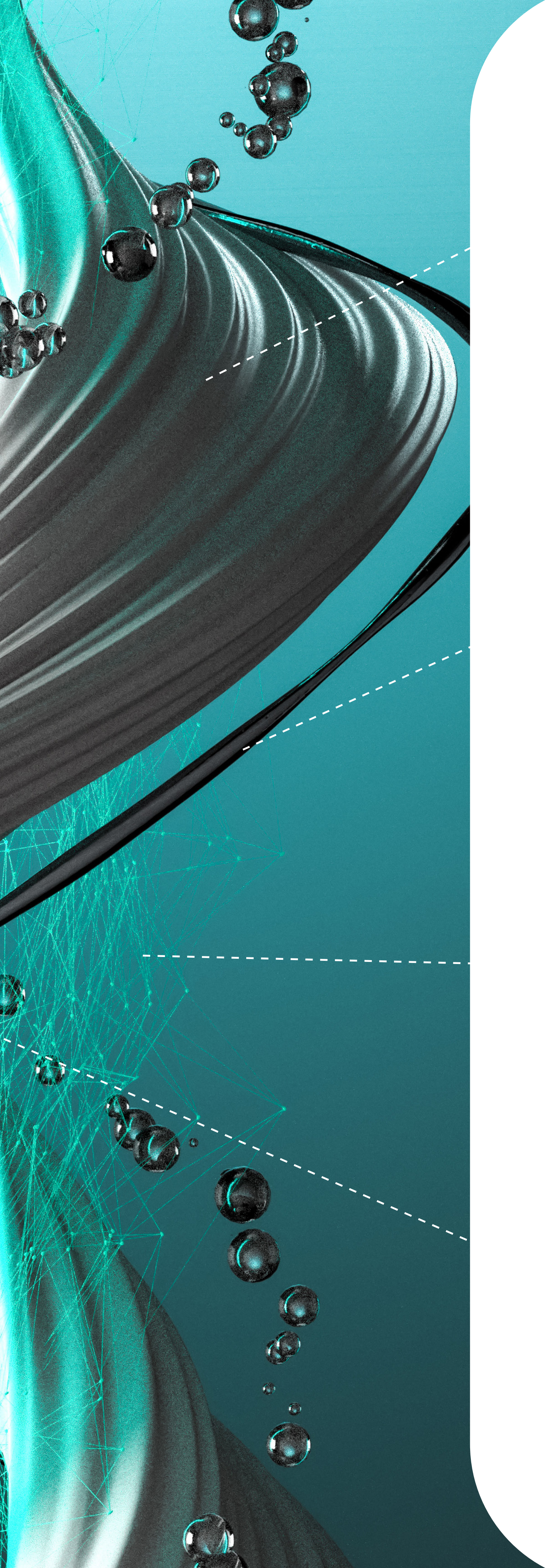
**ESET Cloud Office Security is not included in on-premises solution.*



ADVANCED THREAT DEFENSE WITH CLOUD SANDBOXING TO PREVENT RANSOMWARE

ESET LiveGuard Advanced provides proactive protection against new, never-before-seen threats, by executing all submitted suspicious samples in an isolated and powerful cloud sandbox environment, in order to evaluate their behavior using threat intelligence feeds, ESET's multiple internal tools for static and dynamic analysis, and reputation data.

- Advanced unpacking & scanning
- Cutting-edge machine learning
- In-depth behavioral analysis
- Cloud sandboxing



MULTILAYERED ENDPOINT PROTECTION INCLUDING FILE SERVER SECURITY

ESET Endpoint Security provides strong malware and exploit prevention and can detect malware before, during and after execution. Now it also features anti-password guessing technology.

ESET Server Security provides lightweight multilayered server protection, to ensure business continuity.

- Block targeted attacks
- Prevent data breaches
- Stop fileless attacks
- Detect advanced persistent threats

ADVANCED PROTECTION FOR EMAIL AND CLOUD COLLABORATION OR STORAGE

ESET Cloud Office Security provides advanced protection for Microsoft 365 applications by means of an easy-to-use cloud console. The combination of spam filtering, anti-malware scanning and anti-phishing helps to protect your company communication and cloud storage.

- Includes advanced threat defense capability with ultimate protection against new, never-before-seen threat types, especially ransomware.
- Visibility in detections and quarantine via anytime-accessible console.
- Automatic protection of new user mailboxes.
- Immediate notification when detection of malware occurs.

ESET Mail Security provides an additional layer of defense on server level to prevent spam and malware from ever reaching users' mailboxes.

POWERFUL ENCRYPTION MANAGED NATIVELY BY ESET PROTECT

ESET Full Disk Encryption is a feature native to the ESET PROTECT management console. It allows one-click deployment and encryption of data on connected Windows and Mac endpoints. ESET Full Disk Encryption significantly increases your organization's data security and helps you comply with data protection regulations.

- Manage encryption on Windows and macOS machines
- Encrypt system disks, partitions or entire drives
- Deploy, activate and encrypt devices in a single action

REMOTE MANAGEMENT CONSOLE

ESET PROTECT is a cloud-based or on-prem, multifunctional remote network security management tool for ESET business security products across all operating systems. It enables one-click security deployment and the cloud console gives you network visibility without the need to buy or maintain additional hardware, reducing total cost of ownership.

- Seamless setup and deployment
- Cloud deployment does not require additional hardware or software
- Single point of network security management
- Saves time with automated tasks

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

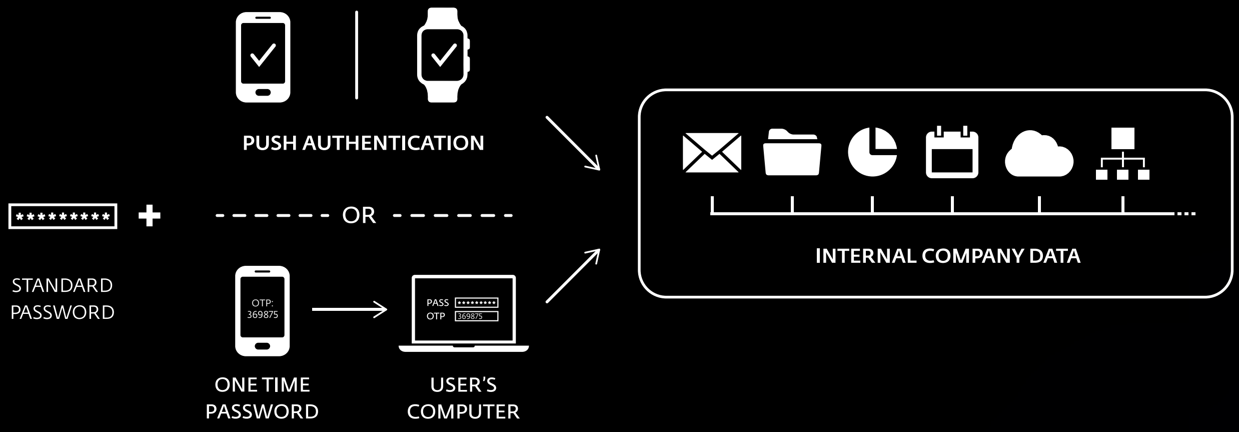
When it comes to compliance, most businesses first need to understand whether they have to meet a compliance target or not. Next, they have to review what measures and recommendations their business must implement in order to comply. When it comes to multi-factor authentication, several regulations such 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.



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

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

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

ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

ESET IN NUMBERS

1bn+
protected internet users

400k+
business customers

200+
countries & territories

13
global R&D centers

SOME OF OUR CUSTOMERS

MITSUBISHI MOTORS
Drive your Ambition
protected by ESET since 2017
more than 9,000 endpoints

Allianz Suisse
protected by ESET since 2016
more than 4,000 mailboxes

Canon
Canon Marketing Japan Group
protected by ESET since 2016
more than 32,000 endpoints

T · ·
ISP security partner since 2008
2 million customer base

COMMITTED TO THE HIGHEST INDUSTRY STANDARDS

AV comparatives
APPROVED
Business Security
DEC 2021

ESET received the Business Security APPROVED award from AV - Comparatives in the Business Security Test in December 2021.

G2
Leader
WINTER
2022

ESET consistently achieves top rankings on the global G2 user review platform and its solutions are appreciated by customers worldwide.

FORRESTER®

ESET solutions are regularly recognized by leading analyst firms, including in "The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021" as a sample vendor.

eset®
Digital Security
Progress. Protected.