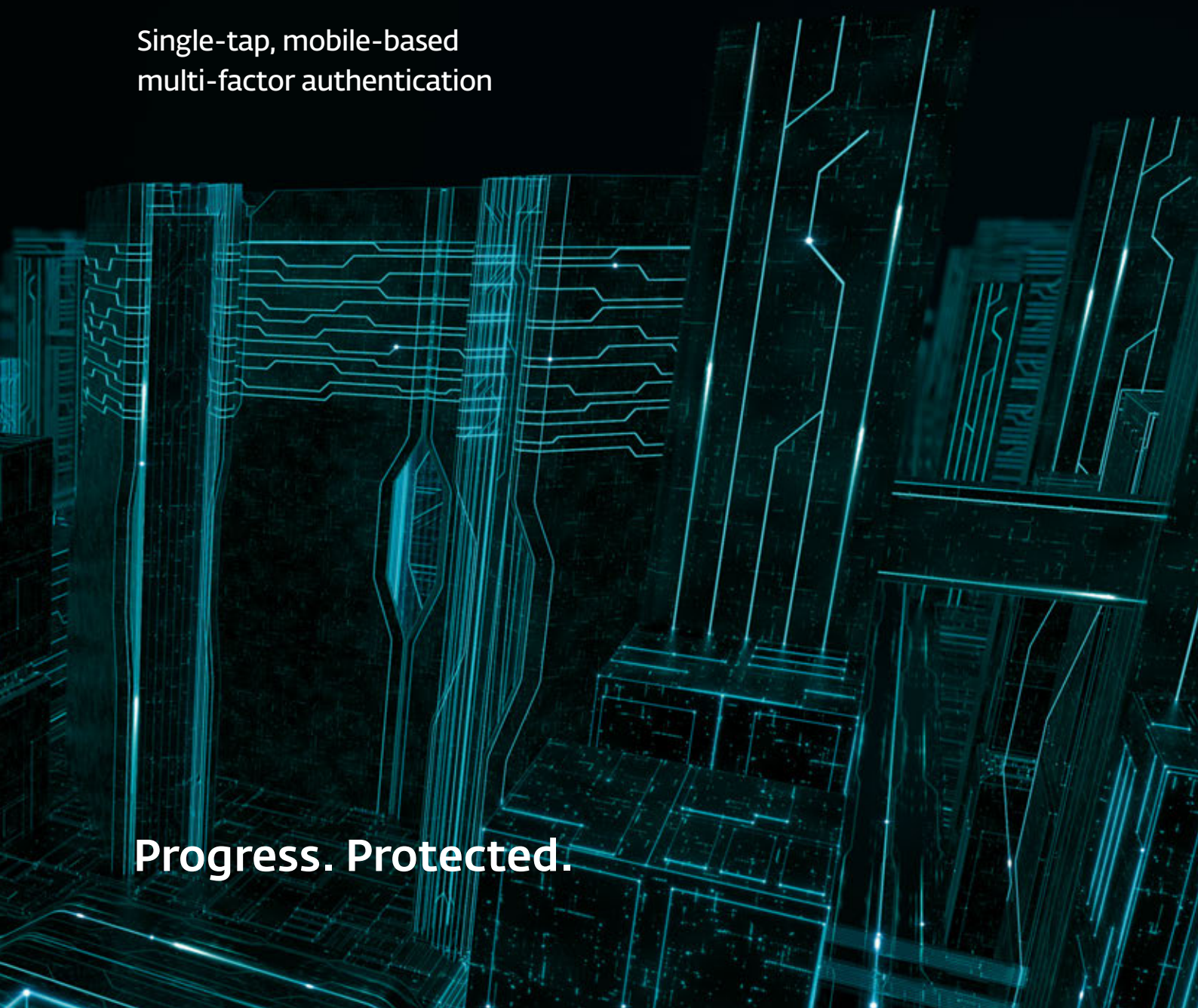
SOLUTION OVERVIEW

SECURE AUTHENTICATION CLOUD EARLY ACCESS PROGRAM

Single-tap, mobile-based
multi-factor authentication



Progress. Protected.

What is **multi-factor authentication?**

Multi-factor authentication (MFA), also known as two-factor authentication (2FA), 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, Outlook Web Access, operating system login and more.

Why **multi-factor authentication?**

Multi-factor authentication can help to offset the risks of 'credential stuffing' - an attack using compromised employee information. This risk is driven by those who:

- Use the same password across several apps and sites
- Share their passwords with others
- Only make minor changes when updating passwords

POOR PASSWORD HYGIENE

Data is one of the most important assets of your company. But employees can put it 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 helps to prevent attackers from gaining access to your systems by guessing weak passwords or exploiting compromised employee credentials.

DATA BREACHES

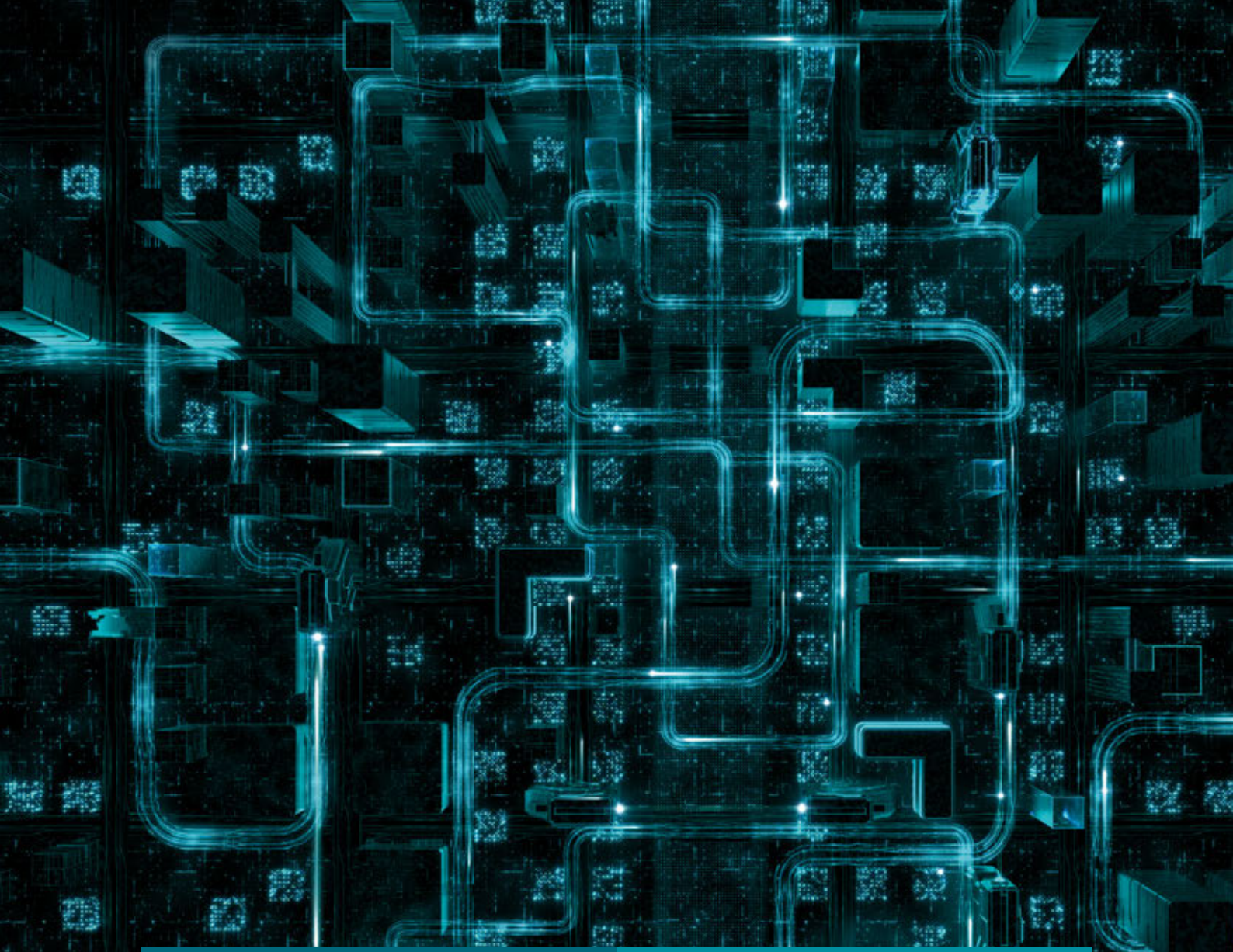
In today's cybersecurity landscape, an increasing number of data breaches occur every day. One of the most common ways hackers can gain access to your company's data is through weak or stolen passwords gathered via automated bots, phishing, or targeted attacks. In addition to just protecting normal users' 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 the GDPR and HIPAA, stress the need for stronger authentication.

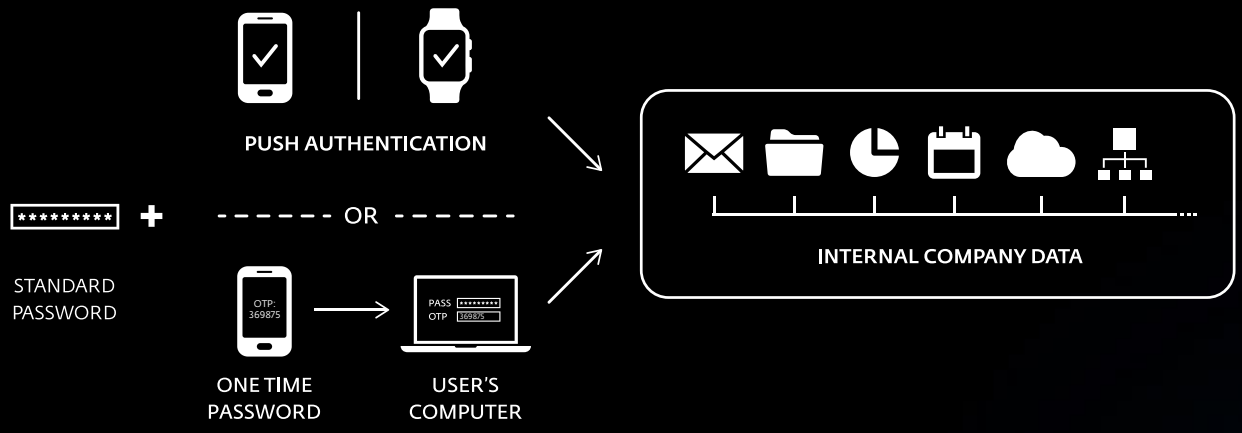
Multi-factor authentication is no longer just an option for most businesses that handle credit cards or financial transactions, but rather a required solution. All businesses should examine which laws and regulations apply to them, and ensure that they comply with their requirements.



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 helps prevent attackers from gaining access to your systems simply by guessing a static 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

The ESET Secure Authentication resource requirements are efficient - within the Early Access Program, you can use the cloud-based version so you won't need a dedicated server.

WORKS WITH EXISTING SMARTPHONES

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

EASY AND QUICK TO SET UP

We've worked hard so that you don't have to - set up only takes a few minutes. 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.

PUSH AUTHENTICATION

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

MULTITENANCY

The cloud-based version of ESET Secure Authentication has been designed with multitenant management capability in place to administer multiple companies or sites, and respectively offering flexibility of defining specific settings for individual groups of users.

CLOUD SUPPORT

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

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.

Use cases

Prevent data breaches

PROBLEM

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.

Strengthen password protection

PROBLEM

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.

Verify user login process

PROBLEM

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.

Technical features and protected platforms

FEATURE	DETAIL	ESET SECURE AUTHENTICATION	ESET SECURE AUTHENTICATION CLOUD (EARLY ACCESS PROGRAM)
MULTITENANCY	Multiple sites/companies	✗	✓
LOCAL LOGIN PROTECTION	Windows Login	✓	✓
REMOTE LOGIN PROTECTION	Radius Server for VPN Protection	✓	✓
	Remote Desktop	✓	✓
WEB APPLICATION PROTECTION	Microsoft Exchange Server	✓	✓
	Microsoft SharePoint Server	✓	✓
	Remote Desktop Web Access	✓	✓
	Microsoft Dynamics CRM	✓	✓
	Remote Web Access	✓	✓
ACTIVE DIRECTORY FEDERATION SERVICES PROTECTION (AD FS)		✓	✓
IDENTITY PROVIDER CONNECTOR (SAML)		✓	✓
PROXY		✓	✓
API		✓	✓
IP WHITELISTING	Global IP Whitelisting	✓	✓
	Per Feature IP Whitelisting	✓	✓
PROVISIONING	SMS based OTPs	✓	✓
	Mobile Application OTP	✓	✓
	Mobile Application Push Notification	✓	✓
	Hard Token	✓	✓
	FIDO	✓	✓
NOTIFICATIONS	Problem	✓	✓
	Web Console Login	✓	✓
	User Locked	✓	✓
	User Unlocked	✓	✓
	Licenses	✓	✓
THROTTLING	Time-based throttling	✓	✓
AUDIT LOGS AND REPORTS	Report	✓	✓
	Filter	✓	✓
	Export	✓	✓

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+
internet users protected

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

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.

Digital Security
Progress. Protected.