REMOTE™
BY DESIGN

Remote Safely

Digital Monitoring and Security Software.

January 2023

<epam>

Remote Safely: Agenda

1 REMOTE SAFELY: ABOUT THE PRODUCT

2 REMOTE SAFELY: NEW LAYER OF “ZERO TRUST” APPROACH

3 REMOTE SAFELY: HOW IT WORKS (SOC / EMPLOYEE INTERACTION)

4 REMOTE SAFELY: KEY FEATURES

5 REMOTE SAFELY: E2E BUSINESS JOURNEY

6 REMOTE SAFELY: EXTRA MATERIALS AND CONTACTS

About the product

EPAM has partnered with biometric identity management provider, Princeton Identity, to develop Remote Safely, a **multi-layer security solution** that can address the immediate **cybersecurity challenges** businesses face in the era of the **dispersed workforce**.

Remote Safely is a **B2B digital solution** for mitigating **risks** of data leakages associated with **human-based "low tech" attacks**.

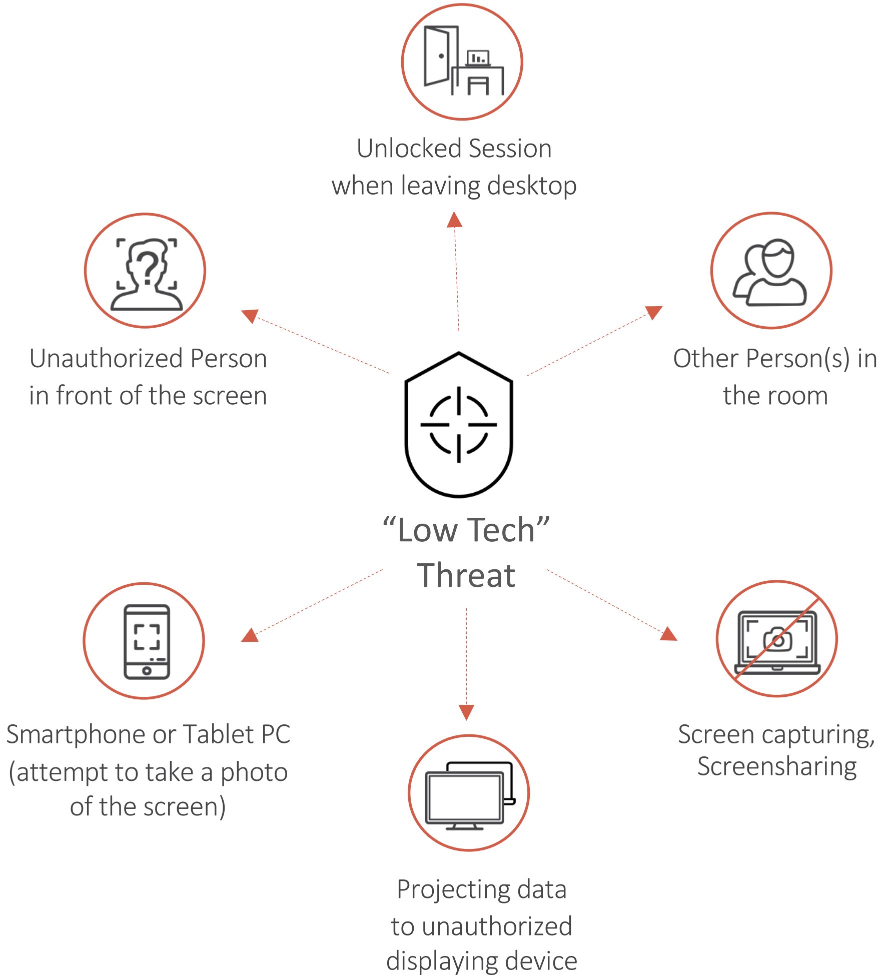
Remote Safely replaces **physical security controls** (security guards, CCTV, door locks, etc.) with **virtual capabilities** built on cloud software, artificial intelligence, uniquely designed hardware, VDI and secured network configurations.

Remote Safely is designed for **companies** that **want**:

- to utilize a **remote workforce**

AND

- to mitigate the risk of **data leakages** for valuable digital assets, such as PII, confidential business information and intellectual property
- to foster **better compliance** with data protection regulations
- to introduce an additional **Zero Trust** security layer and strategy.


"Low Tech" Threat
Unlocked Session when leaving desktop
Unauthorized Person in front of the screen
Other Person(s) in the room
Smartphone or Tablet PC (attempt to take a photo of the screen)
Projecting data to unauthorized displaying device
Screen capturing, Screensharing

Remote Safely: Zero Trust Added value

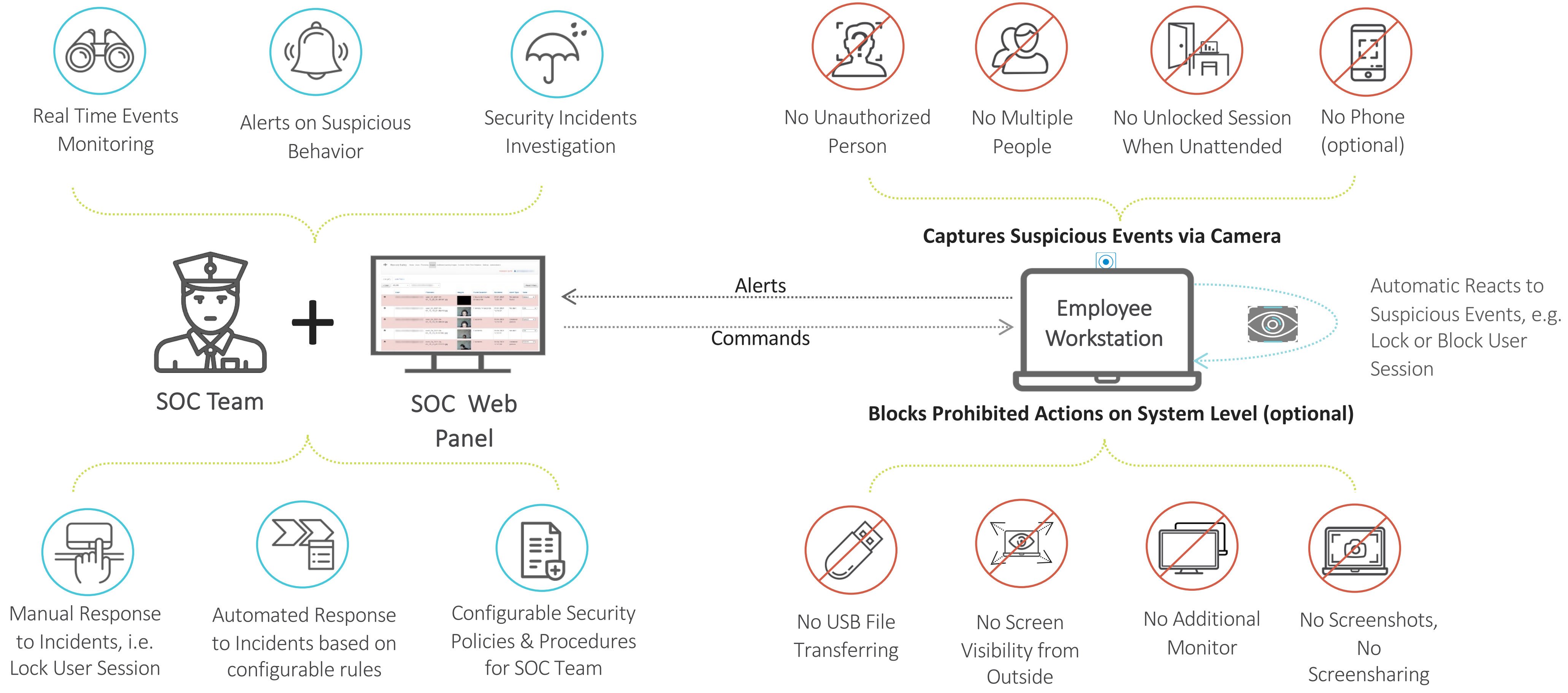
In May 2021, an executive **order was issued** by the White House to **address** the persistent and increasingly sophisticated **malicious cyber campaigns** that threaten the public and private sector. The U.S. Government is mandated to advance toward a **Zero Trust Architecture**. Within 60 days of the date of the order, all agencies must develop a plan to **implement Zero Trust Architecture**. Similar initiatives are taking hold around the globe and all organizations must prepare for a **Zero Trust** world.

Remote Safely is another layer of **Zero Trust** that in positioned when people need to access **sensitive data** (PII, PHI, Financial, Secret and above). Giving **extra verification** for that type of data is very much **inline** with the direction of **Zero Trust** is moving in.

First level is password and authentication.

If you want to access Sensitive data, you now need to pass through Remote Safely.

Remote Safely: How it works (SOC / Employee Interaction)



Real Time Events Monitoring

Alerts on Suspicious Behavior

Security Incidents Investigation

SOC Team

SOC Web Panel

Manual Response to Incidents, i.e. Lock User Session

Automated Response to Incidents based on configurable rules

Configurable Security Policies & Procedures for SOC Team

Alerts

Commands

No Unauthorized Person

No Multiple People

No Unlocked Session When Unattended

No Phone (optional)

Captures Suspicious Events via Camera

Employee Workstation

Automatic Reacts to Suspicious Events, e.g. Lock or Block User Session

Blocks Prohibited Actions on System Level (optional)

No USB File Transferring

No Screen Visibility from Outside

No Additional Monitor

No Screenshots, No Screensharing

Remote Safely: Key Features

SEAMLESS USER IDENTITY VERIFICATION

- Verifies employee identity via AI face one-to-one verification algorithm.
- Ensures that a person located in front of screen is the authorized person to access the data.

DETECT & ALERT SUSPICIOUS EVENTS

- Monitors the remote employee's workplace over the camera and generates alerts if the following events detected in front of the screen:
  - Unknown person;
  - No person is found;
  - Multiple persons;
  - Spoofing attempt;
  - Smartphone or Tablet PC is detected (optional feature).

SOC TEAM MONITORING

- SOC Web Panel for real time digital monitoring of anomalies detected in front of employees' screen and mitigating security risks when necessary.
- Real time notifications via email.
- Integration with third-party monitoring systems i.e., Splunk (on demand).

MULTIPLE DEPLOYMENT OPTIONS

- Can be delivered as EPAM cloud-based solution or deployed on customer's infrastructure.
- Windows and macOS Desktop Applications.

PREVENTING DATA LEAKAGE

- Two levels of response to mitigate security threats: screen lock or permanent block of employee's desktop.
- Customized rules for automatic execution of actions as response to security events.
- Controls access to corporate environment based on the state of digital monitoring (optional feature).
- Blocks attempts to capture the screen (take a screenshot, record video of the screen) and share the screen during online calls (optional feature).
- Blocks attempts to project data to unauthorized monitors (optional feature).
- Blocks attempts to connect to the desktop via RDP (optional feature).
- Optional extra physical security hardening via privacy screens and custom designed wide-angle camera (optional feature).

COMPLIANCE AND ETHICAL DIGITAL MONITORING

- Compliant with the strongest data protection regulations.
- Champions principles of ethical digital monitoring: minimum impact to employees' privacy, AI-based risk calculation without the necessity to store excessive personal data.
- Customizations to fulfil country-specific data protection regulations.

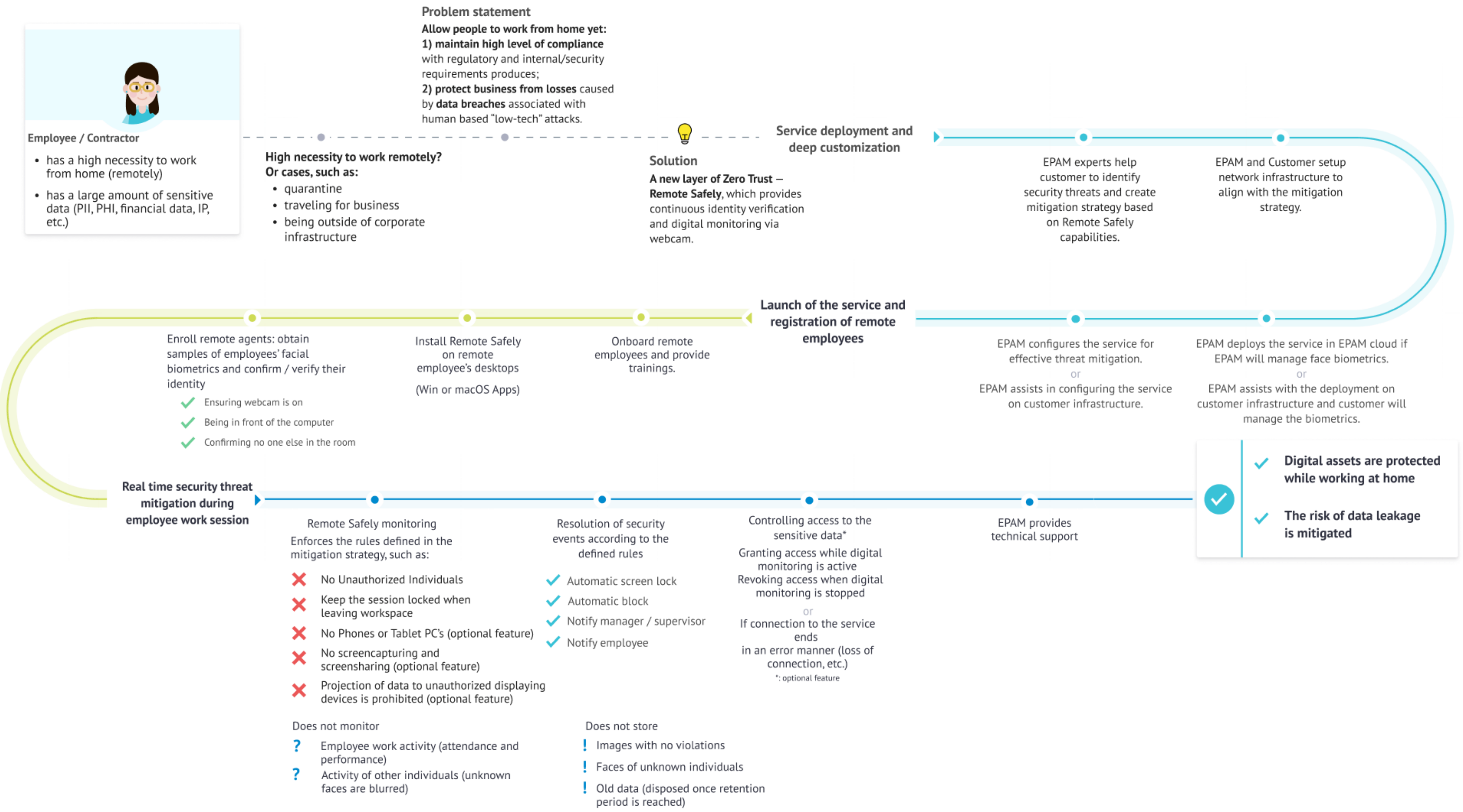
AUDITED SOC 2

AUDITED SOC 3

ISO 27701

IOActive Security Assessment

Remote Safely: How it works (E2E Business Journey)



Employee / Contractor

- has a high necessity to work from home (remotely)
- has a large amount of sensitive data (PII, PHI, financial data, IP, etc.)

Problem statement

Allow people to work from home yet:
1) maintain high level of compliance with regulatory and internal/security requirements produces;
2) protect business from losses caused by **data breaches** associated with human based "low-tech" attacks.

High necessity to work remotely?
Or cases, such as:

- quarantine
- traveling for business
- being outside of corporate infrastructure

Solution

A new layer of Zero Trust – Remote Safely, which provides continuous identity verification and digital monitoring via webcam.

Service deployment and deep customization

EPAM experts help customer to identify security threats and create mitigation strategy based on Remote Safely capabilities.

EPAM and Customer setup network infrastructure to align with the mitigation strategy.

Launch of the service and registration of remote employees

EPAM configures the service for effective threat mitigation.
or
EPAM assists in configuring the service on customer infrastructure.

EPAM deploys the service in EPAM cloud if EPAM will manage face biometrics.
or
EPAM assists with the deployment on customer infrastructure and customer will manage the biometrics.

Onboard remote employees and provide trainings.

Install Remote Safely on remote employee's desktops

(Win or macOS Apps)

Enroll remote agents: obtain samples of employees' facial biometrics and confirm / verify their identity

- ✓ Ensuring webcam is on
- ✓ Being in front of the computer
- ✓ Confirming no one else in the room

Real time security threat mitigation during employee work session

Remote Safely monitoring

Enforces the rules defined in the mitigation strategy, such as:

- ✗ No Unauthorized Individuals
- ✗ Keep the session locked when leaving workspace
- ✗ No Phones or Tablet PC's (optional feature)
- ✗ No screencapturing and screensharing (optional feature)
- ✗ Projection of data to unauthorized displaying devices is prohibited (optional feature)

Does not monitor

- ? Employee work activity (attendance and performance)
- ? Activity of other individuals (unknown faces are blurred)

Resolution of security events according to the defined rules

- ✓ Automatic screen lock
- ✓ Automatic block
- ✓ Notify manager / supervisor
- ✓ Notify employee

Does not store

- ! Images with no violations
- ! Faces of unknown individuals
- ! Old data (disposed once retention period is reached)

Controlling access to the sensitive data*

Granting access while digital monitoring is active
Revoking access when digital monitoring is stopped
or
If connection to the service ends
in an error manner (loss of connection, etc.)

*: optional feature

EPAM provides technical support

- ✓ **Digital assets are protected while working at home**
- ✓ **The risk of data leakage is mitigated**

Remote Safely: Extra Materials and Contacts

See more about Remote Safely at:

- EPAM offering page
- Solutions Hub
- Product Demo Video
- Zed Presentation

Contact:

Sergey Sinkevich (EPAM)

Senior Director, Business Systems and Services

Head of Enterprise Services

Sergey_Sinkevich@epam.com

Boris Khazin (EPAM)

Global Head of Digital Risk Management

Boris_Khazin@epam.com

Princeton Identity Solutions Team

solutions@princetonidentity.com

THANK YOU