EPAM REMOTE SAFELY™ Battlecard

MARKET BACKGROUND & PRODUCT HISTORY

As a direct response to the global COVID-19 shutdown of facilities, EPAM was immediately focused on tactical restoration of production and delivery capabilities (98% remote work achieved within 10 days). Focus has shifted back to strategic risk management associated with remote work on sensitive client data.

Physical relocation from a hardened commercial facility (ODC) to an individual's home naturally results in an overall decrease in security (if controls remain unchanged).

Any company that provides access to sensitive information wants to ensure the following:

- The person viewing sensitive data is the employee who is authorized to see this data.
- The risk of stealing visible data with low-tech visual hacking is nihilated.

In a traditional work environment, these points may be achieved by protecting the workspace with a security guard, installing CCTV, and banning personal devices. However, these security controls are impossible to implement outside an office due to privacy and ethical reasons.

Given this, there is a demand for a technical solution replacing traditional physical security controls and adapted for remote work.

As result, Remote Safely was designed as a replacement of traditional physical security controls by the combination of virtual ones such as AI-based risk detection and visualization, SOC Monitoring capabilities and Remote Safely Application with access to employee's webcam.

WHAT IS REMOTE SAFELY

Remote Safely is a B2B digital solution for mitigating risks of data leakages associated with human-based "low tech" attacks. It ensures that sensitive data being accessed or viewed by the wrong people in a home or remote environment.

Remote Safely replaces the traditional offshore development center (ODC) by combining key physical controls with AI risk visualization. The AI-based service evaluates the risk profile based on recognized visual indicators such as:

- Who is present? How many people are present?
- Are there unauthorized devices in the room?

TARGET MARKET

Remote Safely is another layer of Zero Trust that in positioned when people need to access sensitive data (PII, PHI, Financial, Secret and above). Remote Safely surpasses the current understanding of the zero-trust approach by only allowing access to critical data with continuous identity confirmation using biometric screening of the remote work environment. This ensures that the people accessing information on the system have the right permissions, taking zero trust beyond the local network and to the next level—right up to the chair.

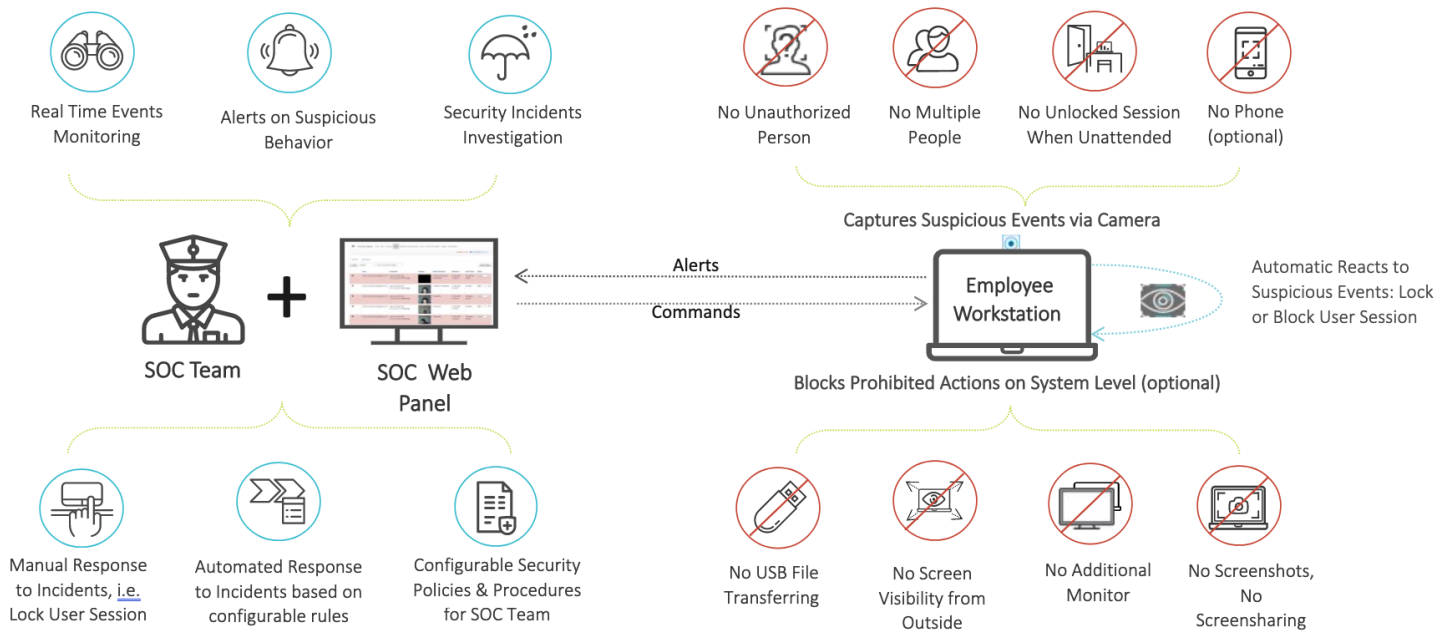
Remote Safely is positioned for companies that want:

- to utilize a remote workforce;

AND

- to mitigate the residual risks of data leakages for valuable digital assets (PII, confidential business information, intellectual property) associated with no-/low-tech attacks;
- to foster better compliance with data protection regulations;
- to introduce a zero-trust security strategy and need to close the security gap associated with inability to introduce traditional physical security control in remote workplaces.

HOW IT WORKS



Remote Safely is a set of security controls that include the application installed on remote employee's laptop or VDI, and launched automatically once the employee logs into the system. It verifies the identity of the person located in the camera view area and detects suspicious behavior that may cause data leakage.

Remote Safely takes photos of the camera view area every few seconds and passes it to the Security Operational Server. The Computer Vision processes the images to verify the user and screen for anomalous behavior. If there is a suspicious event detected on the image, the alert appears on SOC Web Panel.

Members of SOC Monitoring Team analyze the employee's images to detect any suspicious behavior and provide measure to resolve potential security incidents (for example, lock or block workstations of remote employees).

VALUE PROPOSITION: WHY REMOTE SAFELY

Remote Safely addresses the immediate cybersecurity challenges businesses face, in the era of the dispersed workforce. Through our combination of digital architecture, biometrics, hardware, software and workforce process capabilities, we employ a zero-trust process with data access management to ensure the protections of clients' sensitive information.

Remote Safely enables businesses to offer greater flexibility to their workforce, allowing their teams to focus on what they do best and trust their data is secure. For many industries, this has never before been an option, and it opens up a world of possibilities.

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.

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.
- Control access to corporate environment based on the state of digital monitoring.
- Block attempts to capture the screen (take a screenshot, record video of the screen) and share the screen during online calls.
- Block attempts to project data to unauthorized monitors.
- Block attempts to connect to the desktop via RDP.
- Optional extra physical security hardening via privacy screens and custom designed wide-angle camera.

COMPLIANCE AND ETHICAL DIGITAL MONITORING

- Compliant with the strongest data protection regulations.
- Champion 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

HOW BUSINESS CAN BENEFIT FROM REMOTE SAFELY

- Greater workforce flexibility options via utilizing WFH policy even when accessing valuable and sensitive data.
- Protect business from losses by ensuring that data is being processed securely and seen only by authorized remote employees.
- Maintain high level of compliance with the strongest data protection regulations.
- Increase employee awareness of sensitive data processing rules and policies in WFH.
- Gain more trust and loyalty of customers by enhancing the zero trust and mitigating residual risks of remote work.

WHAT TO LISTEN FOR

Remote Safely can be an upsell opportunity and value-added service for existing EPAM customers. Here's what to listen for when speaking to your client contacts:

- Your client mentions that they want to utilize remote/or dispersed workforce, but maintain the similar or higher level of processing of data.
- Your client provides access to valuable assets or customer data to employees (PII, PHI, Intellectual Property, etc.).
- Your client is aware of residual risks of remote work and wants to mitigate it.
- Your client doesn't have well defined WHF policy.
- Your client wants to introduce Zero Trust Approach in the organization.
- Your client has plan to undergo certifications/audits ISO 27001, SOC2, and need more advanced security controls to ensure secure data processing in WFH.
- Your client wants to protect itself from financial and reputational losses caused by 'remote work related' data breaches, and as result, wants to close gaps in terms of physical security of data in WFH.

WHOM TO TARGET

BUYER'S TITLES	BUYER'S DEPARTMENT/TEAM
CIO	Office of the CIO
ISO	Office of the ISO
DPO	DPO teams
CTO	Risk and compliance managers
CEO	
VP of Technology	

COMPETITION

There are a few similar offerings. Here's what we know so far:

REMOTE DESK

Various of features, the closest alternative to Remote Safely.

SESSION GUARDIAN

Gartner recognized WFH Security solution. Product Market leader.

BIO ID

Limited number of features, but has great expertise in facial recognition technologies. The product is positioned as a biometric MFA.

GLOBAL WALKERS

Product also provides the biometric authentication. It is less functional than Remote Safely, but It can detect idle time and concentration based the face expression of remote agent.

HOMEBASE

Product provides facial authentication and basic set of features. The differentiators - integration with HR systems, delayed verification and focus on remote agent's privacy (no photos are stored).

WHAT TO ASK

When discussing Remote Safely with customers and prospects, here are some questions you should ask to determine if the product is right for them:

ABOUT REMOTE WORK AND PROCESSES

- Are you utilizing or plan to utilize remote workforce?
- Do you know what benefits may bring to business by utilizing remote workforce capabilities?
- Do you provide (or planning to provide) access to valuable data (PII, PHI, Intellectual Property, etc.) to remote employees?
- Do you have any WFH policies in place or planning to create it?
- Can you be sure that remote employees work in isolated area where no one can have access to?

ABOUT SECURITY

- How do remote employee access sensitive information (via VDI, directly from local workstation)?
- Do you have logical security controls to protect data from breaches?
- Are you aware about consequences of data breaches (financial and reputational losses)
- Are you aware about residual risks associated with remote working? For example, visual hacking.
- Do you have security controls to protect data from leakages associated with visual hacking and no-/low-tech attacks?
- Do you plan (or have already) undergo security audits and certifications (ISO 27701, SOC2, etc.)?

RESOURCES & CONTACT INFO

More information
epam.com
solutionshub.epam.com

SERGEY SINKEVICH
Senior Director, Business Systems and Services
Head of Enterprise Services

Sergey_Sinkevich@epam.com

BORIS KHAZIN
Global Head of Digital Risk Management

Boris_Khazin@epam.com