BROCHURE

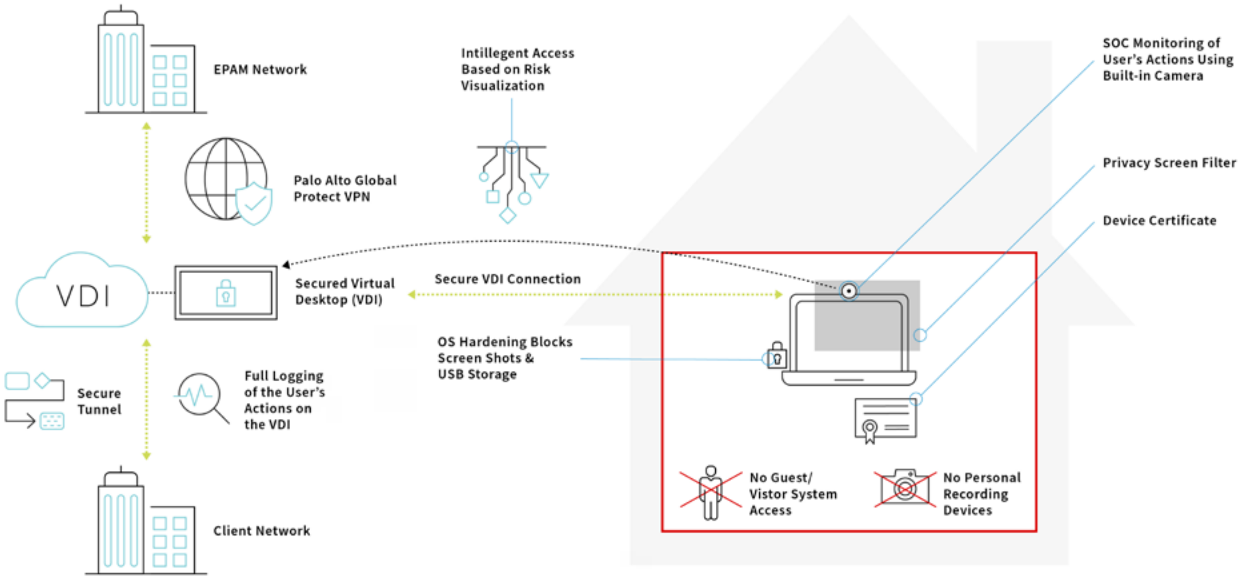
EPAM Business Information Services

REMOTE SAFELY: EPAM & PRINCETON IDENTITY'S REMOTE SECURITY SYSTEM

EPAM BUSINESS INFORMATION SERVICES

Remote Safely: EPAM & Princeton Identity's Remote Security System

In response to the growing need for remote work cybersecurity solutions, EPAM has partnered with biometric identity provider, Princeton Identity, to bring a new kind of multi-layer security solution to market.


EPAM Network
Intillegent Access Based on Risk Visualization
SOC Monitoring of User's Actions Using Built-in Camera
Palo Alto Global Protect VPN
Privacy Screen Filter
Device Certificate
VDI
Secured Virtual Desktop (VDI)
Secure VDI Connection
OS Hardening Blocks Screen Shots & USB Storage
Secure Tunnel
Full Logging of the User's Actions on the VDI
No Guest/ Vistor System Access
No Personal Recording Devices
Client Network

Remote Safely is an added layer of verification on top of an existing virtual desktop infrastructure (VDI) that combines biometrics, dedicated hardware and workforce process capabilities to address the data safety needs of remote teams.

KEY BENEFITS OF REMOTE SAFELY AS A REMOTE WORK SOLUTION

USUAL CHALLENGES	REMOTE SAFELY APPROACH
Endpoint Security	VDI environment, endpoint hardening, AI monitoring by a dedicated device—reported only when an incident occurs
Data Leakage	AI-based risk visualization, session recording, SOC/VDI environment, privacy screens, biometric identity verification
Physical Security	AI-based risks visualization, SOC, privacy screens, advanced custom tamper-resistant hardware
Team Distribution	Teams able to work from any locations, allowing flexibility that has never been an option before
Resilience to Disaster Recovery & Pandemic Events	More resilient to local & regional disasters since critical work can be performed remotely

This operating model enables businesses to:

- Develop greater flexibility in an agile, remote workforce
- Maximize productivity by utilizing a diverse, distributed talent pool
- Manage costs associated with build out and growth planning within a traditional ODC
- Control secure access to data & shared information – another layer of zero-trust protection
- Ensure ongoing compliance with regulatory requirements

This solution ensures compliance with a wide range of security requirements, adopting a zero-trust approach to data access management. Identity confirmation through biometric verification ensures that only approved employees accessing the machine can see sensitive information—improving overall security and protecting confidential data.

REMOTE SAFELY SOLVES THE IMMEDIATE SECURITY CHALLENGES THAT BUSINESSES FACE, ESPECIALLY IN TIMES OF CRISIS

Remote Safely capabilities include:

- Consolidating storage and security controls to virtual desktop environment (VDI)
- Continuous identity verification via biometrics
- Handling sensitive client data securely
- Responding with real-time threat containment and isolation
- Granting data visibility only with pre-authorization
- Setting up incident response capabilities

COMPREHENSIVE SECURITY STRATEGY

Remote Safely replaces the traditional ODC by combining key physical controls with a hardened, secure VDI with logical session recording and AI risk visualization. Our robust resources and dedicated service ensure comprehensive security coverage, with a “zero-trust beyond the keyboard” capability.

This mitigates the risk of sensitive data being access or viewed by the wrong people in a home or remote work environment. Remote Safely supports a zero-trust methodology to cybersecurity, and enables businesses to offer greater flexibility to their workforce—allowing teams to focus on what they do best and trust their data is secure.

This solution integrates with Splunk as a system for reporting security events and AppGate to facilitate the remote desktop connection.

Want to learn more about Remote Safely? **CONTACT US TODAY**

Boris Khazin // **boris_khazin@epam.com**
Global Head of Digital Risk Management

Sergey Sinkevich // **sergey_sinkevich@epam.com**
Senior Director, Business Systems & Services

Princeton Identity Solutions Team
solutions@princetonidentity.com