
WHITE PAPER

# REMOTE SAFELY

## A NEW KIND OF SECURITY SOLUTION FOR REMOTE TEAMS

princeton IDENTITY

CONTENTS


WHEN IT COMES TO CONFIDENTIAL COMPANY INFORMATION, SUCH AS DATA FOR SHAREHOLDER REPORTS OR OTHER SENSITIVE CLIENT INFORMATION, MANY BUSINESSES HAVE A SECURE ON-SITE ROOM WHERE DESIGNATED STAFF WORK. IT'S ESSENTIAL THAT THIS INFORMATION REMAINS CONFIDENTIAL, AS UNINTENTIONAL EXPOSURE CAN AFFECT STOCK VALUE AND BRING SERIOUS LEGAL IMPLICATIONS.

To ensure compliance, this room might feature checks from a security guard, keypad entry, a ban on cellphones and it might monitor meetings held within with video. These extra steps ensure secret data is kept secure and isn't accessed by anyone who's unauthorized to do so.

However, a growing number of challenges have upended typical business processes. The global pandemic, regional natural disasters, a globally dispersed talent pool, and the accelerating trend toward remote work opportunities have all impacted traditional security methods. It's important to be agile and responsive to these challenges while maintaining the necessary security with board and C-level staff working on restricted information.

Obviously, home offices are not hardened like an onsite secure room. This presents a number of risks, including home network vulnerabilities, unexpected guests while working on sensitive projects, and the use of personal cellphones as well as access to the internet and USB drives.

In order to adapt, businesses must be able to secure personally identifiable information (PII), protected health information (PHI), financial information, and other sensitive company information when team members are working remotely or are globally distributed.

## WHAT IS REMOTE SAFELY?

Remote Safely is a collaboration between EPAM and Princeton Identity, a global leader in biometric identity management. It uses a combination of hardware and software technologies to enable remote work on sensitive client and corporate data. This unique offering brings the best technologies and industry practices together to achieve a high-security approach to any remote work environment.

**WITH REMOTE WORK AND GLOBALLY DISPERSED TEAMS, IT'S ESSENTIAL TO HAVE A SECURITY SOLUTION THAT MAINTAINS CONFIDENTIALITY AND TRUST, AND THAT LEGALLY PROTECTS YOUR COMPANY.**

**Remote Safely capabilities include:**

- Shifting of key workstation security controls to virtual desktop (VDI) environment
- Continuously verifying identity via biometrics
- Setting up incident response capabilities
- Furnishing data visibility only with pre-authorization
- Responding with real-time threat visualizations
- Supporting an agile workforce for employers & increased flexibility for remote workers
- Enabling businesses to safely use a diverse, distributed talent pool
- Managing costs associated with build-out & growth planning within a traditional ODC
- Controlling secure access to data & shared information (allowing for another layer of Zero-Trust protection)
- Ensuring ongoing compliance with regulatory requirements

**BENEFITS OF REMOTE SAFELY**

For employers, Remote Safely provides verifiable accountability and security for their confidential information. It ensures compliance with company data security protocols and reduces overall risk. This provides the flexibility to respond to unexpected events—natural disasters, a pandemic or even personal events that otherwise might prevent an individual's attendance—with agility and safety.

For employees, it provides the flexibility to contribute to their sensitive work from home. If working on sensitive information requires travel back to the main office and ODC room, then Remote Safely saves them from flight and travel hassles. Enabling key players to participate securely despite unforeseen challenges is part of a strong overall emergency preparedness plan. Remote Safely allows employees to be considered for key roles even though they might be unable to relocate or travel.

**REMOTE SAFELY CONTRIBUTES TO AN AGILE SECURITY STRATEGY**

Many companies can maintain the minimum, baseline security protocols but struggle to implement new strategies that can cover the dynamic attack surfaces that present the most risk. The ability to identify areas of vulnerability while also protecting data and confidential information is a paramount task—one that should be approached with a zero-trust attitude.

Zero trust is a guilty-until-proven-innocent concept in cybersecurity. It centers on the premise that organizations should not trust anyone by default, inside or outside their network perimeters, but rather maintain strict access controls and verify everything first. This is based on the recognition that traditional security approaches can only do so much to protect data and the users accessing it, especially considering the reality of frequent cyberattacks and data breaches. In fact, the traditional approach's inherent trust is a systematic network weakness that's exploitable by attackers.

Zero trust requires explicit verification of anything and everything that requests a resource (IPs, machines, etc.), and takes broad precautions to limit an attacker's lateral network movement and potential damage in exploits. It uses network segmentation to isolate the resources available to corner an attacker into just a small section of your network, assign just-in-time, task-limited permissions to all resource requests and methodically deploys encryption throughout all communications and file storage.

The lesson of zero trust: Do not inherently trust anyone. Do not give access until trust is fully proven. This approach can strengthen protocols already in place to protect your sensitive information.

**REMOTE SAFELY BRINGS ZERO TRUST TO THE CHAIR, SAFELY ALLOWING ACCESS WITH ACCOUNTABILITY AND SMART ALERTS FOR SUSPICIOUS ACTIVITY.**

There has been a significant shift from past security stances where one assumes there's an impenetrable perimeter, and once authenticated, a user is safe and trusted to access a broad spectrum of network resources. Zero trust must cover a wide scope—and this applies to people, computers, networks & platforms.

While the Zero Trust perspective is a relatively new approach to cybersecurity, when it comes to working with sensitive data, an offshore development center (ODC) is typically seen as the height of safety and security.

## THE TRADITIONAL ODC APPROACH

An ODC is a physical room or office that is owned and operated by a business to house their expansion and development efforts for certain software products or services. Because of the confidential work that goes on here, these spaces are usually off limits except for designated personnel.

Professionals who work with personally identifiable information (PII) and protected health information, or those with roles in the financial services and insurance industries might work in an ODC or similar environment.

A common vulnerability in a corporate workspace is eavesdropping on sensitive information that's verbally or digitally shared within the office. While ODCs are often associated with specific tasks to facilitate business development, there are many job roles with potential access to sensitive information, such as those handling:

- Private company or customer data with Non-Disclosure Agreements (NDA)
- Financial information, bank transfers, and routing/account numbers
- Information or correspondence regarding corporate mergers, acquisitions, and sales
- Legal documents like contracts or service agreements

The facility might have different levels of security, sometimes described as yellow and/or red room levels. Whether it's yellow or red might depend on what's physically available within the facility and the information's sensitivity.

The options for a medium security room, also known as a yellow room, include video surveillance for entry and exit, the prohibition of personal cell phones and cameras inside and remote identification for each person entering the room.

In a high security room, also called a red room, the controls are stricter. All the optional items for the medium security set up are mandatory in a red room. In addition, there are security officers there in person to monitor and control entrance and exit, and full video surveillance of the working area. And cell phones, both personal and corporate, are banned.

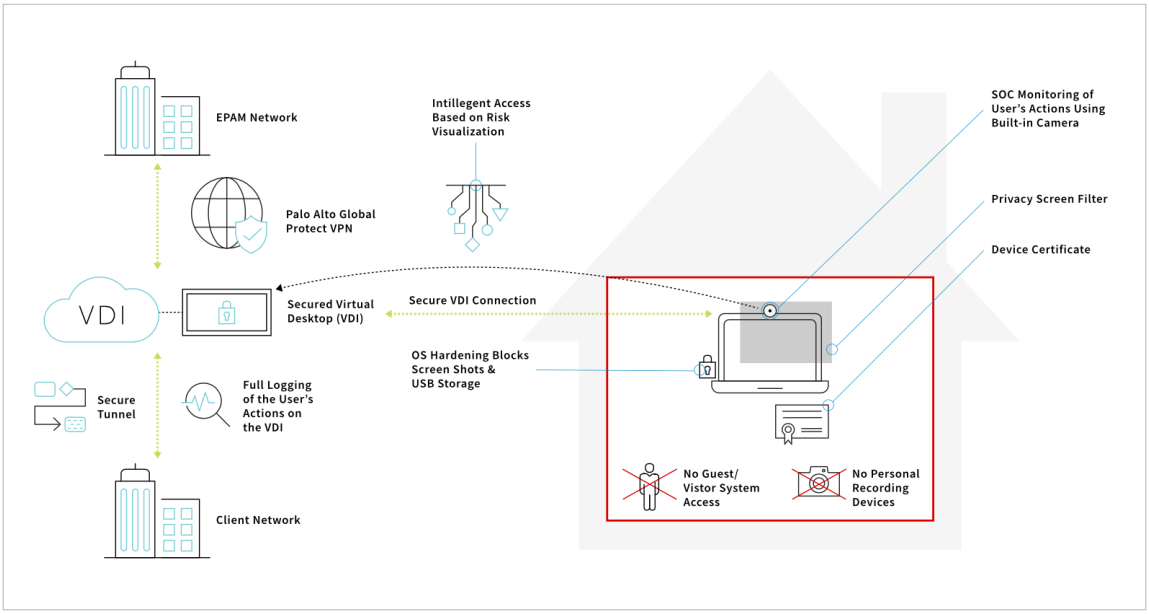
Some companies might also opt for metal detectors and to pat down personnel coming in and out of the room. There might also be specific procedures and rules around printing off of any device in the high security red room. For smaller rooms, an RF shield might be implemented.

## KEY PHYSICAL CONTROLS FOR RESIDUAL RISK MANAGEMENT

ODC security applies to not only development done offshore, but also to on-site isolation areas within your corporate offices, where secure and secret information is accessed and worked on. Having a secure ODC area is a proactive measure toward guarding confidential data, helping to protect against a privacy breach that could result in financial loss, or a damaged reputation.

While ODCs will always exist within certain businesses, the current climate calls for a new approach—one that would allow for secure work to be conducted from home or a remote location.

Remote Safely is equally, or maybe even more, secure than the traditional, hardened commercial facility (ODC) approach. It's a means of ensuring compliance with all necessary security requirements—employing a zero-trust process to be utilized with data-access management.




Remote Safely features key workstation security hardening controls that are moved from local machines to a virtual desktop infrastructure (VDI) delivered from your server. This enables stricter governance and control, including control of available apps and network access.

The VDI has enhanced hardware standards enforced via technical measures including embedded screen protection (SureView technology). These network controls minimize exposure to common home network hardware risks. It disables the use of USB drives and provides additional precautions to reduce vulnerabilities, including verifying who's viewing a specific session and activated monitoring when something suspicious happens during a session.

By leveraging software, hardware and artificial intelligence (AI) learning, the system can verify if an attendee walks off camera and leaves sensitive data potentially exposed to others, or if another, unauthorized person can see the session.

The system can detect if a cellphone might be recording or taking screenshots of confidential data and ensures that only the approved attendees are attending the session. When events deemed as security risks occur, the system generates an alert and immediately revokes viewing access.

Endpoint AI-based agent evaluates sessions for risks: trains for each authorized person, verifies if the authorized person is present and that no unauthorized personnel are present, and detects unauthorized device presence to avoid screen recording. Actions are automatically taken based on a detected risk: security operations center (SOC) alerts generated, endpoint access revoked, and VDI access is revoked.

There are additional software and hardware options available, depending on your need. These include the prevention of additional threats by using key stroke monitoring, app detection, and email monitoring. Custom hardware devices are available that enable extra visibility with fisheye camera (1800) with enhanced physical device security, to prevent tampering.

It is important to note that even if opting for additional software and hardware, these features would only be activated if triggered by an event that qualifies as a security threat.

## KEY DIFFERENCES BETWEEN TRADITIONAL ODC & REMOTE SAFELY

Moving from a secure corporate facility to the home environment with baseline remote work controls (policy, privacy screen and webcam) adds residual risks, but Remote Safely can address them.

| | Traditional ODC Approach | Remote Safely Approach |
|---|---|---|
| **Endpoint Security** | • Staff enter closed perimeter room with a guard<br>• Ban on personal devices<br>• Laptops have standard endpoint hardware configuration & hardening | • Shift to VDI environment<br>• Standard endpoint hardware configuration & hardening<br>• AI monitoring by local, dedicated camera device<br>• Reporting only triggered when an incident occurs |
| **Data Leakage** | • Staff work within closed perimeter r oom with a guard<br>• Closed-circuit television (CCTV) monitoring<br>• Ban on personal devices | • SOC/VDI environment<br>• Privacy screens<br>• AI-based risk visualization<br>• Biometric identity verification<br>• Session recording, when risk event triggers it |
| **Physical Security** | • Staff work within closed perimeter room with a guard<br>• CCTV monitoring<br>• Advanced access content system (AACS) | • AI-based risk visualization<br>• SOC environment privacy screens advanced, tamper-resistant hardware |
| **Team Distributions** | • Teams are limited to work in designated offices or specific geographic locations | • Teams can work from *any* location |
| **Resilience to Disaster Recovery & Emergency Events** | • The business is vulnerable/ susceptible to disruption caused by local & regional disasters<br>• Emergency events could interfere with the ability to work from the ODC location | • Increased resilience to local & regional disasters<br>• Critical work can still be performed remotely, without sacrificing safety |

With recent events and trends pushing for more work-from-home and remote work opportunities, it becomes critical that organizations have the necessary tools in place to enable an agile workforce and protect their sensitive information—from any working location.

While traditional ODCs have been effective in the past, with these new considerations, they are insufficient at protecting company data when most employees are no longer working in the office.

Our best suggestion is to find a technology partner who will work with your organization to help balance the convenience of working remotely with both safety and agility. This will ensure a higher level of security overall, as well as accountability.

The Remote Safely solution can address these challenges and pain points by replacing the ODC model with a secure VDI, and by employing zero-trust methodologies with data-access management. This will change the way you confront risk and mitigate any instances of cybersecurity threats, cyberattacks and data breaches more effectively. By breaking away from the physical necessities of office work, this also opens up a world of possibilities for employers and employees alike.

# About Princeton Identity

Princeton Identity Inc. was formerly a division of SRI International marketed under the SRI Identity brand. SRI and SRI Identity have had a long and successful history of delivering leading-edge technology, going back to the roots of the company in Stanford University, RCA Labs, and Sarnoff Labs, where many familiar technologies were born. Some of these technologies have become household items, including color television, the computer mouse, and Siri (purchased by Apple). Others have had broader impact, such as ground-scanning satellites, automated check processing, medical devices, and cancer-fighting drugs.

Recent work in biometric technologies was applied to a wide range of government and commercial needs, as well as to mainstream applications. It is this recent work, and its potential applications to the physical security market and other related markets, that led to the formation of Princeton Identity.

The management team is comprised of staff from SRI International, having experience in operations and research and multiple years of biometrics experience.

princeton IDENTITY

ADDRESS: 300 Horizon Dr. Suite 308 Hamilton, NJ 08691
PHONE: +(609) 270-3220
EMAIL: info@princetonidentity.com
WEB: www.princetonidenity.com