



eBOOK

Remote **Safely**

Applying Zero Trust Principles to
Today's Distributed Teams

Contents

01

Introduction

02

The Traditional ODC Approach

03

Applying Zero Trust Principles in a Digital Environment

04

Putting Zero Trust Principles in Practice with Remote Safely

05

Benefits Of Remote Safely

06

How Remote Safely Works

07

Key Differences Between Traditional ODC & Remote Safely

08

Conclusion

Introduction

For businesses that regularly handle sensitive information, it's imperative to keep that information safe and restricted to only authorized users. Up until 2019, many companies relied on physical spaces to do that for them. Oftentimes, organizations would set up secure on-site rooms only accessible to designated staff with appropriate clearances when necessary. This room might have featured checks from a security guard, keypad entry, a cell phone ban and video monitoring. With a few simple measures, sensitive business information could easily and reliably stay secure. After 2020, however, that all changed.

And, it's no secret that in the preceding years – as a global pandemic raged on, cataclysmic geopolitical events occurred and an increasingly distributed workforce continued to disperse – our old ways of securing sensitive data haven't been able to keep up. To succeed in this environment, companies have had to respond quickly and agilely – sometimes at the expense of their own security.

As teams have moved from on-site security rooms to off-site sunrooms, a number of risks have been introduced to businesses' digital environments, like home network vulnerabilities, unexpected guests and the ubiquity of personal cellphone usage, among others.

In order to adapt, businesses must be able to secure personally identifiable information (PII), protected health information (PHI), financial information and other sensitive data in a highly volatile environment.



The Traditional ODC Approach

Merely a decade ago, many companies would rely on an offshore development center (ODC) – a physical room or office owned and operated by a business – to house its expansion and development efforts for certain software products or services. Because of the confidential work that goes on in them, these spaces were off-limits to all except designated personnel, like those who handle:



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 or red rooms. Whether it's yellow or red might depend on what's physically available within the facility and the sensitivity of the information.

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 the room and remote identification for each person entering the room.

In a high-security room, a red room, the controls are stricter. All the optional items for the medium security setup are mandatory. In addition, there might be security officers who monitor and control entrances and exits as well as full video surveillance. Some companies might also opt for metal detectors and to pat down personnel coming in and out of the room as well as specify procedures and rules around printing information.

Having a secure ODC is a vital, proactive measure in physical workspaces in order for businesses to guard confidential data, helping them to protect themselves against a privacy breach that could result in financial losses or a damaged reputation.

As companies trend digital-first, however, perimeter security no longer provides adequate protection for the modern enterprise. As companies employ SaaS solutions, APIs, cloud computing and other modern tooling to stay agile and competitive, their enterprise technology ecosystems become increasingly complex, leaving them more vulnerable to exploitation.

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.

Applying Zero Trust Principles in a Digital Environment

No matter the industry or company size, old-school ring-fencing and firewalls alone are no longer sufficient. Zero trust is an enterprise imperative. Enterprise cybersecurity must be just as agile as any other business practice, monitoring and adapting in a continuous loop.

Zero Trust is not a product or set of products. It's a holistic strategy; one that can and should iterate over time. With a guilty-until-proven-innocent approach, it centers on the premise that organizations should not trust anyone by default – inside or outside their network perimeters – and rather maintain strict access controls and verify everything first.

It starts with a company taking a thorough assessment of its current state to get to a true understanding of its security posture and find vulnerabilities before they can be exposed.

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.

GO DEEPER



Read the new [Zero Trust Principles in a Digital Environment](#) white paper



Boris Khazin

Managing Principal, Governance, Risk & Compliance Consulting
EPAM

Putting Zero Trust Principles in Practice with Remote Safely

Adopting a Zero Trust mindset in a digital climate requires understanding your risks holistically. That's why businesses need a new kind of solution.

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. Bringing the best technologies and modern industry practices together, Remote Safely enables businesses to reach the highest security levels in an ever-evolving workplace.

Remote Safely capabilities include:



Shifting of key workstation security controls to a 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



Enabling an agile workforce



Managing costs associated with build-out and growth planning



Controlling secure access to data and shared information



Ensuring ongoing compliance with regulatory requirements

Benefits of Remote Safely

For employers, Remote Safely provides verifiable accountability and security for their confidential information while providing the flexibility necessary to respond to unexpected events – like natural disasters, a pandemic or even just spotty Wi-Fi – with agility and safety. Enabling key players to participate securely despite unforeseen challenges is part of a strong overall emergency preparedness plan.

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.



How Remote Safely Works

Remote Safely acts as a means of enabling zero-trust principles, helping businesses ensure compliance with all necessary security requirements. Featuring key workstation security hardening controls, this solution moves information from local machines to a virtual desktop infrastructure (VDI) delivered from your server. This enables stricter governance and control.

The VDI has enhanced hardware standards enforced via technical measures, including embedded screen protection. 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 also 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 security risks occur, the system generates an alert and immediately revokes viewing access.

An 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 devices to avoid screen recording. Actions are automatically taken based on a detected risk. Security operations center (SOC) alerts are generated and endpoint and VDI access is revoked.

Custom hardware devices can enable extra visibility with fisheye cameras (180°) with enhanced physical device security to prevent tampering. 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 to ensure user privacy as appropriate.



EPAM does not provide VDI service, but rather **assists in the seamless integration of the solution with various VDI providers.**

Key Differences Between Traditional ODC & Remote Safely

Moving from a secure corporate facility to a home environment with baseline remote work controls can introduce additional risks. With Remote Safely, however, these risks can be addressed.



ENDPOINT SECURITY



DATA LEAKAGE



PHYSICAL SECURITY



DISTRIBUTED TEAMS



DISASTER RECOVERY & EMERGENCY EVENTS

Traditional ODC Approach

- | | | | | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Staff enter closed perimeter room with a guard • Ban on personal devices • Laptops have standard endpoint hardware configuration and hardening | <ul style="list-style-type: none"> • Staff work within closed perimeter room with a guard • Closed-circuit television (CCTV) monitoring • Ban on personal devices | <ul style="list-style-type: none"> • Staff work within closed perimeter room with a guard • CCTV monitoring • Advanced access content system (AACS) | <ul style="list-style-type: none"> • Teams are limited to work in designated offices or specific geographic locations | <ul style="list-style-type: none"> • The business is vulnerable to disruption caused by local and regional disasters • Emergency events could interfere with the ability to work from the ODC location |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Remote Safely Approach

- | | | | | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Shift to VDI environment • Use of standard endpoint hardware configuration and hardening • AI monitoring by local, dedicated camera device • Reporting only triggered when an incident occurs | <ul style="list-style-type: none"> • SOC/VDI environment • Privacy screens • AI-based risk visualization • Biometric identity verification • Session recording when risk event triggered | <ul style="list-style-type: none"> • AI-based risk visualization • SOC environment privacy screens advanced, tamper-resistant hardware | <ul style="list-style-type: none"> • Teams can work from any location | <ul style="list-style-type: none"> • Increased resilience to local and regional disasters • Critical work can still be performed remotely, without sacrificing safety |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

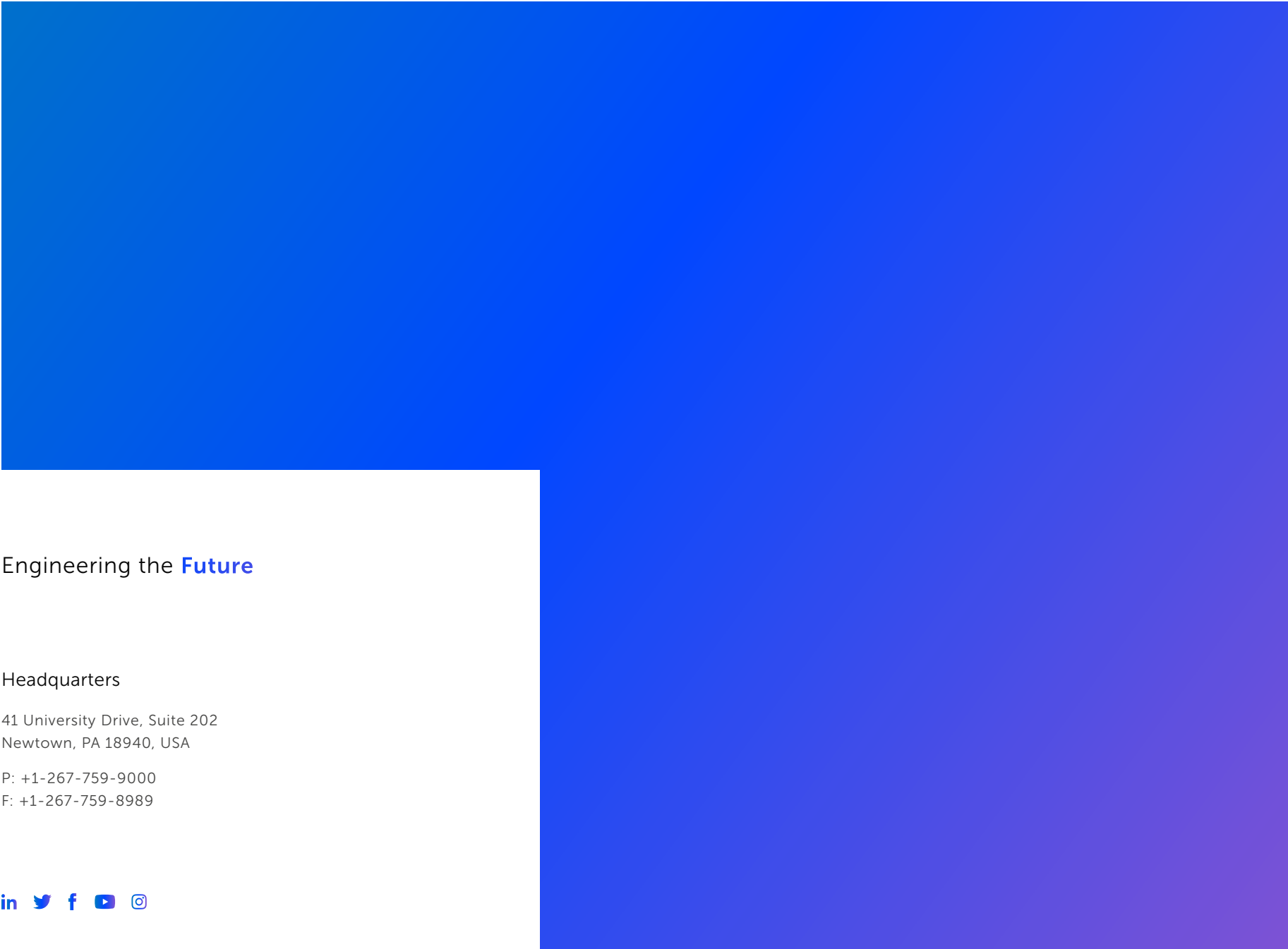
Conclusion

With recent events and trends creating a digital-first workplace, it's critical that organizations have the necessary tools in place to enable an agile workforce and protect their sensitive information — from anywhere.

While traditional ODCs have been effective in the past, with these new considerations, they are no longer sufficient in securing sensitive data.

By implementing a solution like Remote Safely, businesses can employ Zero Trust principles to replace the ODC model with a secure VDI, helping you to confront and mitigate risks and threats. By breaking away from the physical necessities of an office environment, your business is equipped to become more agile and stay competitive in an ever-evolving market.





Engineering the **Future**

Headquarters

41 University Drive, Suite 202
Newtown, PA 18940, USA

P: +1-267-759-9000

F: +1-267-759-8989

