WHITE PAPER

Remote Safely: A New Kind of Security Solution for Remote Teams

Contents

Overview

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

What is Remote Safely?

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.

What is Zero Trust?

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.

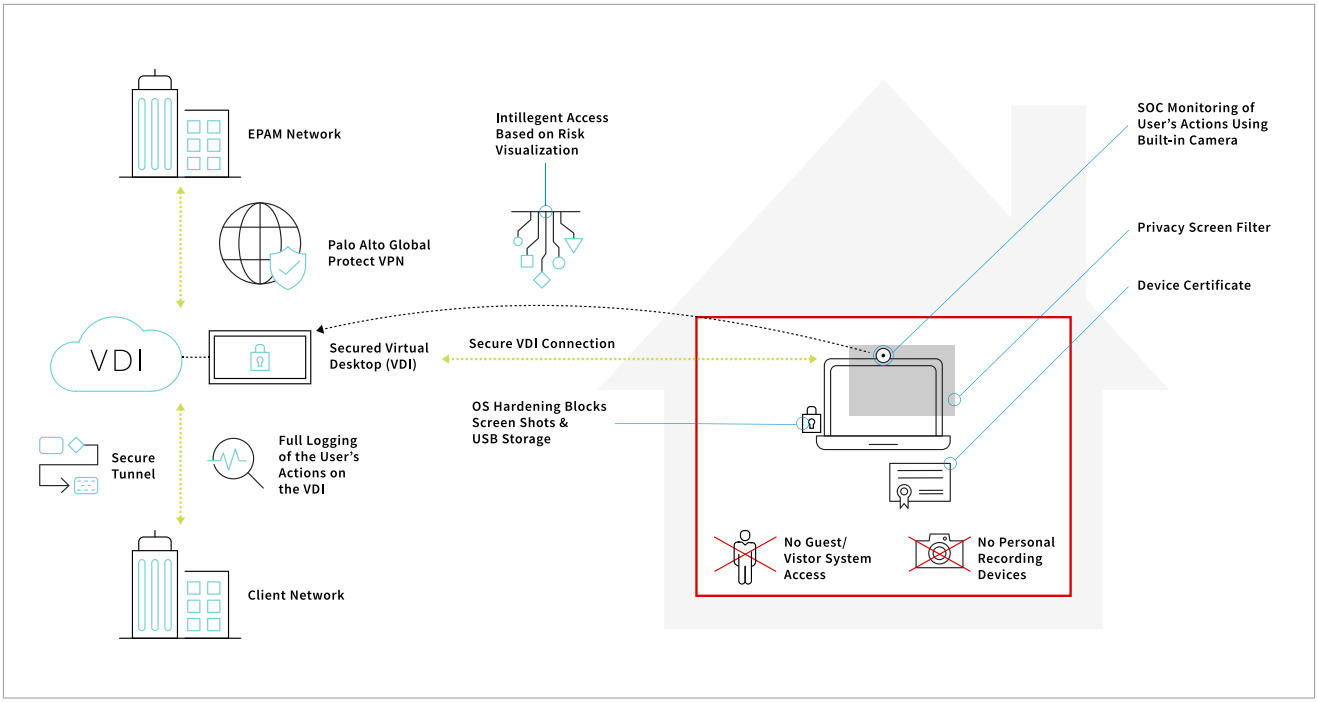
KEY PHYSICAL CONTROLS FOR RESIDUAL RISK MANAGEMENT

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.

How Remote Safely Works

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.

How Remote Safely Works

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 (180^0) 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 • Ban on personal devices • Laptops have standard endpoint hardware configuration & hardening	• Shift to VDI environment • Standard endpoint hardware configuration & hardening • AI monitoring by local, dedicated camera device • Reporting only triggered when an incident occurs
Data Leakage	• Staff work within closed perimeter r oom with a guard • Closed-circuit television (CCTV) monitoring • Ban on personal devices	• SOC/VDI environment • Privacy screens • AI-based risk visualization • Biometric identity verification • Session recording, when risk event triggers it
Physical Security	• Staff work within closed perimeter room with a guard • CCTV monitoring • Advanced access content system (AACS)	• AI-based risk visualization • 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 • Emergency events could interfere with the ability to work from the ODC location	• Increased resilience to local & regional disasters • Critical work can still be performed remotely, without sacrificing safety

Conclusion

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 EPAM SYSTEMS

Since 1993, EPAM Systems, Inc. (NYSE: EPAM), has leveraged its core engineering expertise to become a leading global product development and digital platform engineering services company. Through its 'Engineering DNA' and innovative strategy, consulting, and design capabilities, EPAM works in collaboration with its customers to deliver innovative solutions that turn complex business challenges into real business opportunities. EPAM's global teams serve customers in over 25 countries across North America, Europe, Asia and Australia. EPAM is a recognized market leader among independent research agencies and was ranked #8 in FORBES 25 Fastest Growing Public Tech Companies, as a top information technology services company on FORTUNE'S 100 Fastest Growing Companies, and as a top UK Digital Design & Build Agency. Learn more at www.epam.com and follow us on Twitter @EPAMSYSTEMS and LinkedIn.

GLOBAL

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

P: +1-267-759-9000

F: +1-267-759-8989

EUROPE

Corvin Offices I. Futó street
47-53
Budapest, H-1082, Hungary

P: +36-1-327-7400

F: +36-1-577-2384

CIS

9th Radialnaya Street,
Building 2
Moscow, 115404, Russia

P: +7-495-730-6360

F: +7-495-730-6361

WHITE PAPER

Modern Zero Trust Enterprise: A Guide

Introduction

Enterprise digital ecosystems face more security challenges than ever before. As companies and the technology they use become web-based and more complex, traditional cybersecurity becomes more porous, leaving businesses vulnerable to exploitation. The work-from-home model has further tested the outdated notion that perimeter security is adequate protection.

Cyberattacks have become pervasive and their sophistication is growing exponentially, which makes it much harder to detect and respond to them. On average, it takes 280 days for an organization to identify and contain a data breach[1], according to a 2020 IBM report, and 52 percent of the data breaches were caused by malicious attacks (of those 53 percent were financially motivated).[2]

While digital transformation can add complexity to organizational processes, it's better to be an early adopter than fall behind the curve. Companies should employ SaaS, APIs, cloud services and other tools to stay modern and agile. But at the same time, it's vital to hit the reset button on security. Old-school ring fencing and firewalls are out; zero trust is in.

This calls for verifying every interaction for legitimacy. Trust is never assumed and access is never granted by default. No user or service, whether internal or external, is automatically granted access.

The price of not rethinking security has skyrocketed, with cybercrime costs expected to reach

$6 TRILLION

GLOBALLY IN 2021.[3]

Hackers and the malware they employ have become more sophisticated and more damaging, impacting all industries and companies of every size. As a result, enterprise cybersecurity must be just as agile as any other business practice, monitoring and adapting in a continuous loop.

[1] "Cost of a Data Breach Report," IBM Security, 2020.
[2] Ibid.
[3] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

What is Zero Trust?

The National Institute of Standards and Technology (NIST) describes zero trust as "an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources."[4]

This means the old days of ring fencing are over. NIST, a U.S. government agency, also makes it clear that building a zero-trust architecture (ZTA) is not a "one-and-done" project. As technology continues to evolve, at an alarmingly fast pace, enterprise cybersecurity must change in tandem.

ZTA is not a product or set of products. It's a *strategy*, one that can and should iterate over time. And it starts with a thorough assessment of where a company is now, because that's the only way to find and eliminate vulnerabilities before they can be exposed.

For decades, companies gave employees access to everything in their network. The assumption was everyone inside the firewall was trustworthy and everyone outside was not. That thinking doesn't fit with the current threat landscape, and assumptions now come with more risk. Companies can no longer trust the firewall because important users are outside of it and bad actors can get inside.

[4] https://www.nist.gov/publications/zero-trust-architecture

What is Zero Trust?

In 2009, Forrester developed a new information security model, called the Zero Trust Model, which has gained widespread acceptance and adoption.[5] The definition has evolved over the past 12 years, and there is considerable debate about exactly how to get there. At EPAM, we see ZTA supported by three main pillars:

1 **EVERYTHING IS DYNAMIC**

The cloud, applications, data storage and networks—everything is dynamic and software-defined now. We cannot assume perimeters, identities or even APIs to be static and persistent anymore. With more nodes being ephemeral, spinning up and down runtime, and more network changes on the fly, companies need to adopt a security model that will be as strong and flexible as the ever-changing environment.

2 **LEAST AMOUNT OF PRIVILEGE**

Grant the least amount of privilege and then work your way up as users, or software services, prove themselves trustworthy. Privilege should always be time-boxed and never granted perpetually. Whenever possible, require traceable promotion processes and service accounts so that you can see when they are requested.

3 **WATCH AND VERIFY EVERYTHING**

Always watch and verify everything using fine-grain transactions (or smaller units). Do not assume the call five minutes ago will be from the same source just because the speaker claims to be—challenge it, reduce the rekey and recycle token time and make it difficult for nefarious actors to fake sources and transactions. Whether a request for access comes from inside the corporate network, using internal hybrid cloud, or corporate laptops and services, do not automatically assume the user or service is safe. Assume others have visibility into your network. Assume services could be hijacked. Assume who you are chatting with is unauthenticated until verified and proven otherwise, and even then, they should be trusted for the single transaction only.

[5] "A Practical Guide To Zero Trust Implementation," Forrester, March 3, 2021

Why Zero Trust?

In a sense, this isn't new; cybersecurity has always been risky business. What has changed is the stakes—the scale and impact of bad actors has led to some of the biggest breaches we've ever seen. Persistent and lateral attacks are real and serious.

It's the "weakest link" problem. Because companies have become interdependent with more software services, they are only as safe as their most vulnerable app or device. Thousands of SolarWinds customers found that out the hard way in 2020, when hackers breached the company's popular network management software.[6] Companies, organizations and even, alarmingly, federal agencies like the U. S. State Department were infiltrated. The attack was so grave that top federal government cybersecurity leaders are now calling for a zero-trust approach.[7]

Another high-profile breach making headlines in recent months was traced back to outdated technology from firewall vendor Accellion.[8] Data was stolen from major enterprises and institutions including Kroger Co., Washington State and Harvard Business School.

Cybercrime is becoming much more organized[9], which means increased sophistication and exploits that are harder to detect. Cybercrime-as-a-service is a booming business, as the increase in quantity and quality of tools on the Darknet makes cybercrime cheaper and easier to carry out.[10]

The way we work has changed fundamentally in recent years, most notably during the pandemic. But even before the COVID-19 pandemic prompted a sharp jump in work-from-home practices, companies were already relying increasingly on gig workers and BYOD,[11] and that flexibility raises security questions. Even with mobile device management (MDM), the new landscape makes it nearly impossible to find success with traditional security.

With 80 percent[12] of breaches involving customer personally identifiable information (PII), cyberattacks can have long-term, intangible costs that are hard to calculate. Customer trust is hard to quantify, but the consequences of violating that trust are difficult to overcome.

[6] https://www.nytimes.com/2021/02/23/opinion/solarwinds-hack.html?searchResultPosition=2

[7] https://www.govinfosecurity.com/case-for-zero-trust-approach-after-solarwinds-attack-a-16216

[8] https://www.darkreading.com/attacks-breaches/accellion-data-breach-resulted-in-extortion-attempts-against-multiple-victims/d/d-id/1340226

[9] https://securityintelligence.com/the-business-of-organized-cybercrime-rising-intergang-collaboration-in-2018/

[10] http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

[11] https://www.infosecurity-magazine.com/opinions/gig-economy-battleground/

[12] "Cost of a Data Breach Report," IBM Security, 2020.

TRANSFORMATION IS GOOD. MODERNIZATION IS GOOD. BUT...

The components of digital transformation are worth it, but they also necessitate security updates:

- **API Economy**
  Application programming interfaces (APIs) give us an easy way to communicate among systems, which fosters innovation—however they also expand the attack surface substantially and make room for new vectors for bad actors.[13]
- **Digital Supply Chain and SaaS**
  Software as a service (SaaS) has become standard, making the tech landscape more fluid as constant updates keep companies agile. But how well do you know any third party?
- **Elastic and Dynamic Cloud**
  The cloud is dynamic, giving us unprecedented flexibility, which is also harder to secure.
- **Software-Defined Networks**
  Network changes are now software-defined and fluid, another potential weak point.
- **Data is the New Currency**
  Data analytics give us access to insights never before within reach, but data is also a lucrative prize for hackers.

Agility and innovation are good and necessary to compete in the modern digital landscape, but they come with a security debt that must be settled.

[13] https://www.infosecurity-magazine.com/opinions/api-security-vulnerabilities-1-1/

High-Level Guidelines for Moving Towards a Zero Trust Model

Although ZTA has developed to include a wide range of practices, depending on who you ask, it doesn't have to be overwhelming. Underlying the model are straightforward concepts that can be broken down into the following guidelines:

1 **GATE WITH LEAST PRIVILEGE / "NEED-TO" ONLY ACCESS**

Start from no-access/no-privilege, and then grant limited access upon verification that the user actually needs it and build up from there. Need-to-know, need-to-access, need-to-share; permission is only granted when necessary.

2 **VERIFY CONSTANTLY AND USE SMALLER UNITS**

Make sure that your transaction and access tokens are verified and constantly challenged. Break up large units of work into smaller ones to both help reduce any one-time loss, and also to give your detection and response team more data and time.

3 **AUTOMATE AND MICROSEGMENT NETWORK+WORKLOAD+DATA**

Build security into your process and architecture and automate as much as possible. Isolate and segment network, workload and data to reduce the blast radius and speed up containment when necessary. A solid review process will go a long way.

4 **SECURE ENDPOINTS**

Companies are habituated to assuming client endpoints are secure. They should do their best to secure endpoints, while simultaneously anticipating there could be a breach, so transfer only what is needed to endpoints.

5 **VERIFY SERVICES**

Do not use static bindings on services. Instead, companies should make sure they have a resource access model that is aligned with their identity access management (IAM) strategy across all SaaS, online applications and API providers.

6 **REVIEW CORPORATE SERVICES**

Corporate tools must support fine-grain controls aligned with the enterprise identity model, regardless of whether the host is internal or external (SaaS).

7 **SECURE DEVELOPMENT PRACTICES**

Companies should employ the Secure Software Development Model (SSDM) and constantly monitor the continuous integration/continuous delivery (CI/CD) pipeline and, when possible, keep the infrastructure immutable.

8 **TRUST NO RUNTIME**

Runtimes must be hardened and, when possible, immutable.

9 **TRUST NO NETWORK**

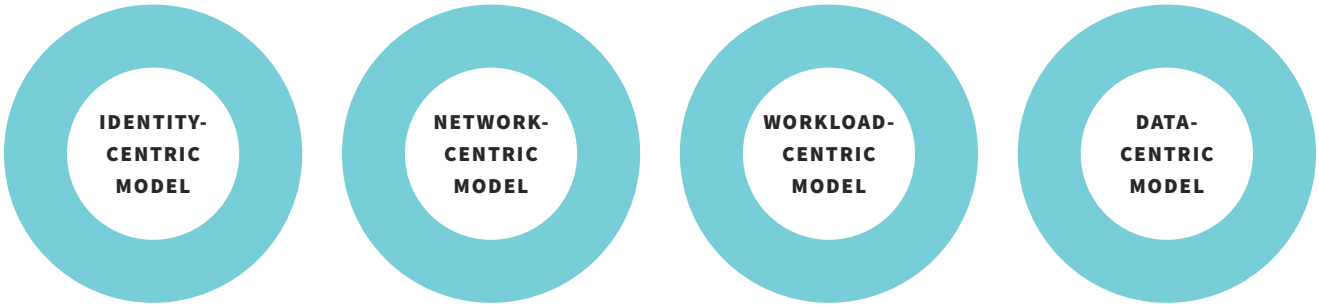
Companies should assume others can monitor their packets, regardless of whether they are in their corporate network, using a virtual private network (VPN) or bridged, and security controls should be layered. (Traditionally, a VPN grants a trust zone to an endpoint or another trust zone but that's no longer recommended.)

10 **THINK LIKE A HACKER**

Think from an outside-in perspective. Look at your system and think of what could (and would) others do with it? Don't focus only on your own assets because you could be a stepping stone to a bigger prize. Either way, think defensively.

Multiple Paths to Zero Trust

There are four main pathways to ZTA and advice varies on what's best. In general, we advise starting with an identity-centric model and adding in pieces of the other models, as needed, after a solid foundation is established. Here is a snapshot of the four:



- Unified identities: customers, employees, partners
- Multi-factor authentication
- Policies around identities and weighted attributes

- Micro-segmentation and isolation
- Distributed firewalling
- Dynamic, software-defined networks and perimeters

- Fine-grain API transaction controls
- Layered, secure and contained execution environment
- Immutable pipelines and environments
- Segment-bound workload and sandboxes

- Fine-grain, classified and segmented data
- Distributed object-level encryption
- Data immutability

1 IDENTITY-CENTRIC MODEL

In this model, which is a typical starting point, a company would unify and control identities across its entire ecosystem, including all partners, customers and employees. With so many day-to-day business operations defined by the internet, it's impossible to verify security credentials without breaking down transactions into smaller units. ZTA exerts control by linking the identity of the user, device, service or network to the requested transaction.

In this model, it's vital to strengthen how we authenticate each identity using multi-factor authentication (MFA) and challenge-response authentication (CR). Machine learning (ML) should be deployed to help detect anomalies in user behavior. And it's important to limit token access and reduce the time granted with any token.

However, a pure identity-centric model would put an extra level of stress and focus on your identity store and strategy. The pandemic worsened identity theft and account takeover, which increased by at least 10 percent to 15 percent from 2019 to 2020.[14] Forrester predicts another 8 to 10 percent increase in identity theft and account takeover fraud in 2021.

Once a solid foundation is in place with the identity-centric approach to security, it's usually advisable to add pieces of the other three models as warranted.

[14] "Top Cybersecurity Threats in 2021," Forrester Research, Inc., March 9, 2021.

2 NETWORK-CENTRIC MODEL

The key to a network-centric ZTA model is building distributed and layered network isolation structures. That largely comes down to microsegmentation, which means building small and well-defined boundaries using a next generation or distributed firewall that is logically distributed across your entire enterprise, with both on-premise and hybrid cloud coverage. The effect is to limit and increase the difficulty of lateral attacks and reduce the "blast radius" when there is a breach (and it's when, not if).

And as enterprise network boundaries start to fade and extend right up to the edge, using a secure access service edge (SASE) solution could improve your company's ability to react and respond with a relative real-time cadence.

SASE is an offering that simplifies wide-area networking (WAN) and security by focusing on a distributed model that stretches out directly to the edge.

3 WORKLOAD-CENTRIC MODEL

Securing applications and APIs during runtime is paramount because this is where hackers are hitting paydirt. The execution environment must be layered and secured, similar to the network-centric model, by breaking everything up into smaller units.

Companies should segregate runtimes on multiple levels:

- Make sure each computer cluster is bound to a distinct microsegmentation
- Ensure each node is contained properly with the right configuration
- Use sandboxes for testing code or monitoring for malware

Containerization, a way of virtualizing the runtime environment, is compatible with ZTA because it calls for breaking down an operating system into smaller units so that applications can be segregated and run independently. That means if bad actors gain access to one app, they won't automatically get access to everything else.

4 DATA-CENTRIC MODEL

Encryption is key to providing a level of protection against unauthorized access and visibility for company assets. However, your crypto scheme is only as good as your secrets or key management policy would protect or allow. It is extremely risky for any organization to trust their entire data store and lakes to only a handful of crypto keys (root keys). This is where BORE (break once run everywhere) attacks could compromise an entire system in a short period of time. ZTA calls for understanding how and where data is coming in and going out. Then, organizations can limit liability by breaking up all data into smaller units and giving them unique tags so that each transaction is siloed.

The complexity of modern data dissemination across the net makes it much harder to protect data visibility. Every data lake, every copy of a data set, every persistent login and cache presents a new attack surface for an organization's data. You have to protect not just your central store, but also the entire data set. For example, in 2018, Twitter was forced to ask its more than 330 million users to change their passwords, due to data that became visible through internal logs.[15]

THE FUNDAMENTAL PIECES OF THIS MODEL INCLUDE:

- First, classify all your company data assets and label each unit. This will help you understand what needs to be protected and how. Follow the data movement and provide end-to-end protection across all usage (in transit, at rest and in use).
- Create a strong and granular access model that binds working data labels to specific identities and make sure these fine-grain transactions can be continuously verified. Do not rely on simple "trusted zones" but instead verify the authentication.
- Include controls to scan for usage of data that is potentially out of compliance. For example, flag data sets moving out of a particular geography or in use by applications that aren't whitelisted.

The benefit of breaking everything up into units is that it increases work for bad actors. Without ZTA, all too often a successful hack yields the keys to the kingdom—breaking into a database means access to all data. With ZTA, a hacker would still have to decrypt each unit if they got through, significantly decreasing the ROI for the bad actor.

The data-centric model also helps manage standards such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

The approach that works best for most companies is a combination of the above four models, which we refer to as a hybrid approach to ZTA.

[15] https://money.cnn.com/2018/05/03/technology/twitter-password-bug/index.html

MOVING TOWARD ZERO TRUST CAN BE BROKEN DOWN INTO THREE (SOMETIMES OVERLAPPING) STAGES:

1	2	3
HOLISTIC ASSESSMENT	SECURE TRANSFORMATION	STRONG DETECTION AND RESPONSE

HOLISTIC ASSESSMENT

Moving to ZTA requires an honest assessment of a company's existing identity strategy, network design, all business processes (including data flows and workflows), storage topology, application deployment and more. Without this information, it's impossible to identify vulnerabilities. Three key steps are a must for any transformation:

1. **Identify, classify and document the interfaces to your assets.**
   You must identify what you care about, including sensitive, valuable or regulated assets. Know where they are and how they could be reached.

2. **Threat model your inputs and outputs.**
   Start looking at interfaces as not just features but liabilities as well. Reducing the attack surface means controls will more naturally map to the interfaces.

3. **Understand the business impact.**
   Prioritize and understand the liabilities and risks from a business perspective. Are you holding data keys or root keys? Sensitive information? Personally identifiable information (PII)? Honor it. Honor the trust.

With this information, it's then possible to map out what is needed to move to a dynamic, zero-trust enterprise security model.

SECURE TRANSFORMATION

Security is always a continuous practice. And it's a cat-and-mouse game: Nefarious actors are always looking for gaps and new ways to breach our defenses, and that's why it's so important to improve our security posture, consistently and constantly.

However, most organizations are still stuck in the old segregated, audit-based security model. For a company to be secure while transforming, security must be built into the organization process, culture and digital platform in order to be able to function in our digital age.

It's not just about buying more tools or solutions. Constantly evaluating new options is helpful if you can afford the effort and investment, but it's much more important to have a set of security initiatives that are tied to specific business objectives. And they need to be structured for a successful transition:

- **Get Commitment at the Top**
  The executive level must understand and commit to transforming enterprise security initiatives in order to successfully move towards a zero-trust model.
- **Start with a Healthy "Run" State**
  Make sure you have a concrete set of practical security policies and procedures. Nothing is perfect, but it's important to have the necessary policies aligned with your annual loss expectancy (ALE) calculation.
- **Invest in Continuous Improvements**
  Invest in a continuous improvement program that includes an Incident Retrospective Process, procedure and policy change management, etc.
- **Employ Practical Validation**
  Use a practical, continuous red-teaming process.
- **Invest in Detection and Response**
  You must have an agile cyber detect and incidence response team (CIRT) that has the capability and capacity to handle the existing annual rate of occurrence (ARO) plus enough time to implement any necessary improvements.
- **Align Digital Risk Management**
  Align risk management and governance toward a software-defined model, while automating as much of the verification and audit process as possible. Build compliance into your system.

Technical and administrative controls at endpoints provide another crucial layer of security that could help improve a company's overall cybersecurity posture. When pulled together with your other security measures, it could also give your CIRT a better level of visibility, as well as more tools to identify and mitigate threats.

Employee education has to be part of any secure transformation to zero trust. Internal users who don't understand the risk of downloading a suspicious attachment in an email or trusting their local coffee shop's wi-fi add risk to the organization. So it's incumbent on companies to provide ongoing and thorough risk management training to staff.

STRONG DETECTION AND RESPONSE

Defense is really about time—increasing the amount of time you have to respond, reducing the time needed to narrow down and respond, and cutting the time needed to recover and bring your organization back to a normal, strong state. This is why security operations are so important.

Detection, both the speed and breadth of it, is critical in order to reduce the time needed for the CIRT to contain, mitigate and recover. Detection and response in the new zero-trust architecture is a much more agile process, and it has to be since you are working with finer-grain transactions. Therefore, you have access to a higher volume of data, and you must be ready to identify patterns across small transaction units. It's not so much about patching a route, or managed detection and response (MDR) services, although those are still part of your critical baseline security. You will also need to be able to detect and react to a much more dynamic and software-defined environment.

Finally, you must move closer to real-time data, analytics and response capabilities. All this needs to be adapted to an agile model so your team can learn and pivot quickly.

BRINGING AGILITY TO CYBERSECURITY

Zero trust is not about eliminating threats because no one can promise that. It's about re-designing security by automating and embedding security measures in your development process. Zero Trust will dramatically improve the prevention of breaches and contain the damage that can be done with any successful hack, making companies better equipped to thrive in a software-defined environment.

Digital transformation is no longer optional, but organizations can choose how to do it safely. Cyberattacks have become more common and more costly than ever before, and that means you have to bring the same agility you use in any business process to security.

No product or suite of products can guard adequately against increasingly sophisticated bad actors. But by adopting a zero-trust mindset and following the guidelines that will keep your company thinking like a hacker, you can protect your business—your customers, your employees *and* your bottom line.

ALTHOUGH NOTHING IS EVER 100% SECURE, A COMPANY'S SECURITY POSTURE SHOULD BALANCE RISK TOLERANCE AND BENEFITS. HAVE A BASELINE, THEN PRIORITIZE THE REST PROACTIVELY, CONSTANTLY ADJUSTING.

FOR THE GOOD GUYS, OUR PRIMARY TARGET IS TO BUY TIME: TIME TO DETECT, TIME TO RESPOND, TIME TO CONTAIN, TIME TO RECOVER.

WE SHOULD START WITH BALANCING OUR PRIORITIES BASED ON BUSINESS OBJECTIVES. AND JUST AS A BUSINESS WILL GROW AND PIVOT, SO SHOULD THE RISK PROFILE AND SECURITY POSTURE.

Increase Level of Effort
And expertise and time needed by nefarious actors to breach

Cost
Security is never free. There are costs in time and design, in tools, in CPU, in storage, etc.

Reduce Yield
And damage radius in case of an incident, both short- and long-term

Usability and Performance
To make something "relatively" secure, useable and high performing is difficult

Improve Recovery and Evidence
To make it harder to get away ("clean exit")

Sustainability
To maintain, detect and respond constantly is a must, and it's often costly

ABOUT EPAM

Since 1993, EPAM Systems, Inc. (NYSE: EPAM) has leveraged its software engineering expertise to become a leading global product development, digital platform engineering, and top digital and product design agency. Through its 'Engineering DNA' and innovative strategy, consulting, and design capabilities, EPAM works in collaboration with its customers to deliver next-gen solutions that turn complex business challenges into real business outcomes. EPAM's global teams serve customers in more than 30 countries across North America, Europe, Asia and Australia. As a recognized market leader in multiple categories among top global independent research agencies, EPAM was one of only four technology companies to appear on Forbes 25 Fastest Growing Public Tech Companies list every year of publication since 2013 and was the only IT services company featured on Fortune's 100 Fastest-Growing Companies list of 2019.

Learn more at **www.epam.com** and follow us on **Twitter @EPAMSYSTEMS** and **LinkedIn.**

GLOBAL

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

P: +1-267-759-9000

F: +1-267-759-8989

C347_v1_05/2021

Data Privacy Preserving Engine

Protecting personal data has become more important and more challenging for companies than ever before. Data access carries major regulatory and financial risk for companies, yielding large insurance premiums for data loss as well as regulatory fines. While there are methodologies available on the market to reduce data access, many are labor intensive, lack sufficient security or have low data accuracy.

To address these challenges, EPAM developed the Data Privacy Preserving Engine (PPE) – a tool that generates synthetic, quantifiably private data that preserves high utility on the data generated. By limiting access to production data and maintaining statistical properties of synthetic data, PPE provides a more realistic test environment so your business can reduce liability and human error.

EPAM'S PRIVACY PRESERVING ENGINE FEATURES

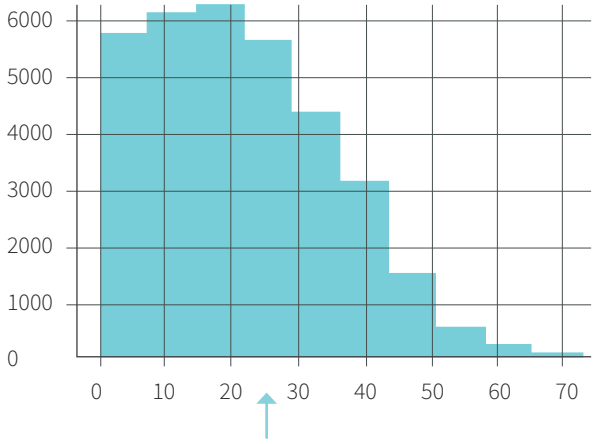
- Moderate complexity based on machine learning
- Automated, content-agnostic approach so humans do not access sensitive data
- Generic solution requiring moderate effort that can process most structured data tables
- Quantifiable privacy properties that are secured by differential privacy mathematical proof
- Ability to be hosted on premises so sensitive data doesn't need to leave a secure environment
- Backed by a global team of digital risk management product engineers and consultants, data strategists, business analysts and data scientists

Data Privacy Preserving Engine

To illustrate how PPE preserves statistical properties, the example below highlights two data sets on age – an original data set and a generative adversarial network (GAN) data set that matches the original data set on a statistical basis. By allowing companies to run individual and group analyses while maintaining statistical properties, PPE provides the characteristics of production data without the security risk.

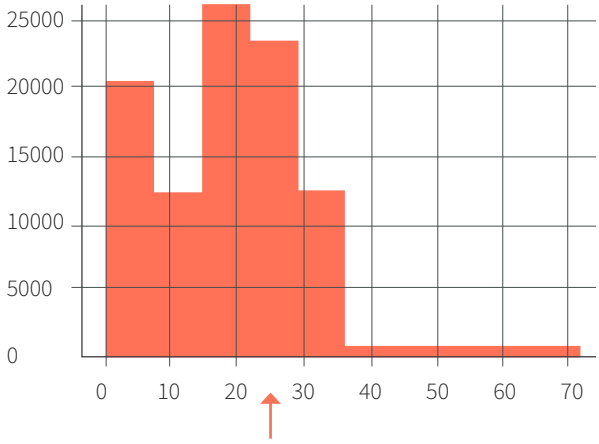
ORIGINAL

Original age



SYNTHETIC

GAN age



As you can see above, the synthetic data has the same statistical calculation result as the original data, both at 90%.

RELEVANT USE CASES FOR PPE

- Cloud migration acceleration
- Data sharing within the enterprise
- Data retention & GDPR
- Application testing & development
- AI/ML models training & data analysis
- Product development, data publication & sharing

Interested in learning more about how EPAM can customize PPE to fit your unique business needs?

Contact Boris Khazin
EPAM's Global Head of Digital Risk Management Services
boris_khazin@epam.com

www.epam.com/drm

<epam>