Deloitte.

zscaler™

Enterprise Recovery

Taking Back Control of Your Network When You're Compromised

2024

What's inside

We begin by putting ourselves in the shoes of an enterprise that has suffered a major breach. By 'major breach' we liken the situation to a domain takeover, compromise of the hypervisor or, at its worst, deployment of ransomware. Fundamentally, a situation where trust and control has been lost in your digital systems and core infrastructure.

As an enterprise your business-critical services are disrupted. Your organisation has come to a halt. As a business, you are not able to generate revenue.

This is the reality business leaders and employees find themselves facing - you are no longer operational, and you need your services back yesterday.

So, the challenge set before you is to answer a simple yet extremely difficult question; What is the fastest path to recovering safely? In this paper, we answer this question through discussing our experiences.

Enterprise Recovery – What do we need to do?

How do we define the fastest path to recovery?

Our response and recovery teams frequently encounter catastrophic cyber-attacks, particularly in the form of ransomware, as detailed in the Digital Resilience and Enterprise Recovery whitepaper[1]. In these situations, where IT systems are completely shut down, the most pertinent question becomes 'What is the fastest path to recovering safely?'

To address the 'fastest path', our team uses the concept of the Minimum Viable Company (MVC) in Enterprise Recovery scenarios. We do this because the goalpost must be set on what is essential to keep the enterprise functioning. Concentrating all teams on a singular objective is crucial, as the scale of devastation can be so extensive that recovery can take months and is a deeply costly endeavour.

> The minimum viable company, MVC, is defined as, "The minimum services required to ensure the survival of the enterprise".

Predominantly, the MVC is made up of customer facing services because they are revenue generating services. Within industrial environments, we must include Operational Technology (OT), to ensure quality and due to the importance of protecting life and the environment.

By determining the MVC for Enterprise Recovery, a target of approximately 30-60 days (depending on company size) is set. Before we can recover the business services, the core technology and infrastructure elements must be considered. These elements form the focus of this paper. Core technology services and infrastructure can be broadly categorised into the following components:

1. **Identity Services**
2. **Production Infrastructure**
3. **Workplace Services**
4. **Applications**
5. **Networks**

All components are necessary to achieve the MVC. In this whitepaper, we will focus on recovering trust and control of the network. Traditional network recovery methods must address deficiencies in common network security approaches and technologies. These methods are time-consuming, which is impractical when time is of the essence. However, this paper introduces an innovative and faster approach developed in collaboration with Zscaler.

[1] Deloitte Digital Resilience and Enterprise Recovery Whitepaper

Enterprise Recovery – Network challenges

Why do traditional network security methods fall short?

Currently the dominant control points of the network and transport layer are **firewalls, Virtual Private Networks (VPNs) and segmentation**. Over the last three years we have observed that these consistently **do not provide the right level of cyber resilience to an enterprise**. These controls are not ageing well, whether through operational difficulty or conceptual flaws, they fail to effectively achieve resilience to unauthorised access attempts. Each has various challenges:

CHALLENGE 1 – SEGMENTATION

The concept of a single all-encompassing VLAN might simplify network management and user accessibility to data and applications. However, it also inadvertently provides a welcome mat for adversaries.

Knowing this, organisations have invested significantly in network segmentation, but our red teams have consistently demonstrated its inadequacy in thwarting adversaries.

Segments often prove traversable due to overly permissive gaps, offering limited blast radius reduction instead of robust access control.

CHALLENGE 2 - FIREWALLS

Moving onto firewalls, how often does an IT Administrator ask:

"What is that rule for?"

Firewalls, while fundamental to network security, often pose more questions than answers.

The sheer volume of rules can lead to inadvertent permission of undesirable traffic and facilitate lateral movement within networks. While effective in traffic transport, firewalls sometimes struggle with enforcing a default deny approach, hindering their ability to provide comprehensive security.

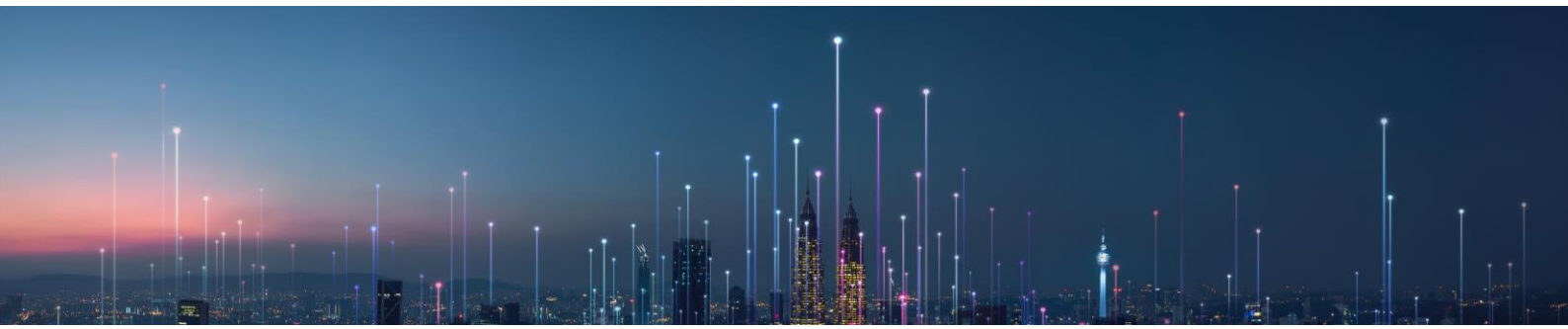
CHALLENGE 3 - VPNs

One of the most common point of compromise for initial access is via VPN, which is subsequently followed by enumeration and then lateral movement.

VPN services, whilst crucial for remote access, present a common entry point for adversaries. Once authenticated, users are granted access to the "trusted network," exposing sensitive applications and data.

When combined with ineffective segmentation and firewall practices, this creates an optimal environment for adversaries to escalate their access and compromise further resources.

Moreover, recent **zero-day attacks targeting major VPN vendors** have underscored the vulnerability of this access point, resulting in global **widespread compromise**.



An enhanced network security recovery method

A pioneering approach to recover trust in networks using SSE

Unique to a recovery scenario is the need for speed. Experience demonstrates that network architects and engineers need weeks (sometimes months) to segment a network, and firewall specialists need days to clean up vulnerable rules. Recovery through traditional control points is cumbersome and it is indicative of why these vulnerabilities come to be and persist.

Since the legacy control points pose serious challenges to establishing and maintaining trust and control, in a response and recovery scenario we need to look beyond them to achieve our goals. Instead, we look at a **modern architectural approach commonly referred to as Zero Trust Network Access, delivered through SSE.**

The result is that it overcomes deficiencies of the three underperforming controls points: VPNs, Firewalls and Network segments, which protect networks in a traditional perimeter-based approach. Simply trying to remediate these shortcomings does not solve the root problem – VPNs and firewalls control access in enterprises that look drastically different today, than to the ones they were made for.

To solve the problems of the past and present our approach recovers a company into a better future state.

To solve the problems of past and present, our approach recovers a company into a better future state. We do not simply turn 'things' back on but recover and transform the network while maintaining speed.

Zscaler becomes the security overlay, and the network focuses on data transfer. This allows our response and recovery teams to side-step security remediation work and focus on recovery. In this way, we can:

- Recover enterprises at speed.
- Provide immediate return on investment.
- Provide effective security through our innovative approach developed over the last three years.

Deloitte has been at the forefront of enterprise recovery, handling some of the most complex cyber incidents in recent times. We will highlight three real-life examples where Deloitte performed enterprise recovery after a cyberattack, each of which involved restoring trust after the network became untrusted. A secure network needs to be in place before recovery of business applications, billing and financial operations can occur. **The longer the network recovery takes, the more money is lost each day and the higher the risk to safety and quality in OT environments.**

We examine differences in speed and effectiveness when using SSE with Zscaler, versus operating without it.

Case 1: VPN compromise and lateral movement

Replacing VPNs with a Zero Trust broker to remediate VPN compromise and lateral movement

SCENARIO

In this case study, a manufacturing client was targeted by threat actors who were able to move laterally across the corporate network without being noticed. This spanned multiple offices and three datacentres across multiple countries. The procedure was a common one; find the domain controllers, datastores and the server management system (SCCM servers).

Our forensic teams saw visible compromise to the domain controller and the Kerberos golden ticket as evidenced by Mimikatz artefacts. With a domain takeover completed and the location of the hypervisor and the Virtualisation Management Infrastructure (VMI) known, the threat actor was in a position to disrupt production services and could not be locked out.

Access to the datastores was the first step to mass data exfiltration that was not stopped by firewalls.

In this attack procedure the defender's tip-off came while an admin was watching 'the match'. An MFA prompt for access to SCCM indicated someone else had control of his account. Later forensic investigators found artefacts known to be ransomware had been staged for deployment.

In response, what would you do?

- The client identified the threat actor's location and shut the server down. Yet, it came back online.
- The VMI was shut down. Yet, it came back online.
- The VPN was shutdown. Yet, the threat actor had already created persistence and moved to the next entry point.
- The Endpoint Detection and Response (EDR) tool had been disabled and could not be re-enabled because admin rights had been removed.

The decision was made to hit the 'red button' and disconnect the network entirely. An action of last resort taken to prevent the distribution of ransomware, which would have resulted in staggering losses.

CHALLENGE

The impact of these events and the response was devastating because all revenue generating services were switched off, and the ability to perform basic business communications disappeared as did the ability to pay staff. The business problem to solve was clear... Imminent catastrophic financial loss events in the coming weeks had to be avoided by restoring the ability to transact.

The technical problem to solve was more complicated. Systems couldn't just be simply switched back online without a method of effectively restricting lateral movement and providing secure access back to data and applications.

Traditional methods of network recovery (see Scenario 3) to stop lateral movement involves investigating and rebuilding VPNs, networks, and firewalls and a host of other non-network focused security measures. It typically takes months and may not provide meaningful resilience increase in the future.

Therefore, a different approach that reduces dependence on these control points and can deliver a secure low-risk recovery of the minimum viable company in weeks is required.

Case 1: VPN compromise and lateral movement

Replacing VPNs with a Zero Trust broker to remediate VPN compromise and lateral movement

SOLUTION

The manufacturing company therefore needed a way to rapidly restore network availability to business applications to function, whilst removing the possibility of lateral movement. From the end user perspective, the company needed a way to ensure that users would only have access to the data they needed and no more.

As outlined at the beginning of this paper, a VPN solution is inefficient at delivering this outcome. A Zero Trust Network Access approach delivers this "by design", users and devices are presented a resource not a network.

The major components to achieve this are; an established SSE, application re-architecture and a working identity provider (IDP). Our client took the decision to use this approach as it permitted the incremental takeback of the network with least privilege access for all users based on a secure end-user access path to applications.

Recovering trust in the IDP is a problem of the same magnitude that needs to be simultaneously solved alongside restoring trust in networks. To achieve MVC, it was an equally necessary component. However, that is a subject for another time.

OUTCOME

Over the next 30 days the entire VPN mesh architecture was dismantled; an SSE architecture was deployed that joined 5 datacentres and 3 cloud platforms; also 5500 users across 15+ countries were onboarded to access the top 36 corporate applications. This target was significant as it defined the minimum viable business operations needed for financial stability, allowing the client to report **no material revenue loss**.

Deloitte worked together with the client and Zscaler to swiftly deploy the initial solution. Our collaborative effort resulted in the restoration of access to a critical financial clearing application in **24 hours**, and consequently preserve the enterprise's license to operate. This success was a genuine proof of value and paved the way for VPN to be replaced wholesale across the organisation with Secure Service Edge architecture built on the Zscaler solution.

Case 1: Conceptual target architecture

Replacing VPNs with a Zero Trust broker to remediate VPN compromise and lateral movement

TARGET ARCHITECTURE

To answer the weaknesses of lateral movement enabled through VPN architecture where a device is joined to a network, in this scenario, we implemented Zscaler. Zscaler enables an SSE architecture (shown in Figure 1) which minimizes attack surface by connecting users to the applications (instead of network). The Zero Trust approach with Zscaler also dictates that no user or device should be trusted by default, regardless of their location, and enforces the least privilege principle.

Deloitte transformed the organisation from a network centric approach to an SSE architecture, which significantly reduced time to recover from the attack, enhanced overall security posture and responsiveness.

In Figure 1, we can see;

- Zscaler Private Access (ZPA) provides secure access to internal apps hosted on-prem and in the cloud[2]
- Zscaler Internet Access (ZIA) is a secure web gateway to secure internet traffic
- The Zscaler Zero Trust Exchange acts as the Zero Trust broker for access requests which go through ZIA and ZPA

In this scenario, we accomplished a critical rollout of SSE for access to the enterprise's core infrastructure and all applications required to support the MVC in an exceptionally short timeframe of just four weeks.

The organisation was transformed to a Zero Trust Network architecture and able to ensure that users only have access to apps they need; the risk of lateral movement and ransomware is reduced; integrating new companies in a merger and acquisition scenario is made much easier; and the complexity of IT operations is reduced.

This recovery approach using an SSE architecture is in contrast with traditional firewall remediation approach as it reduces recovery time and restores access without the vulnerabilities that existed previously.

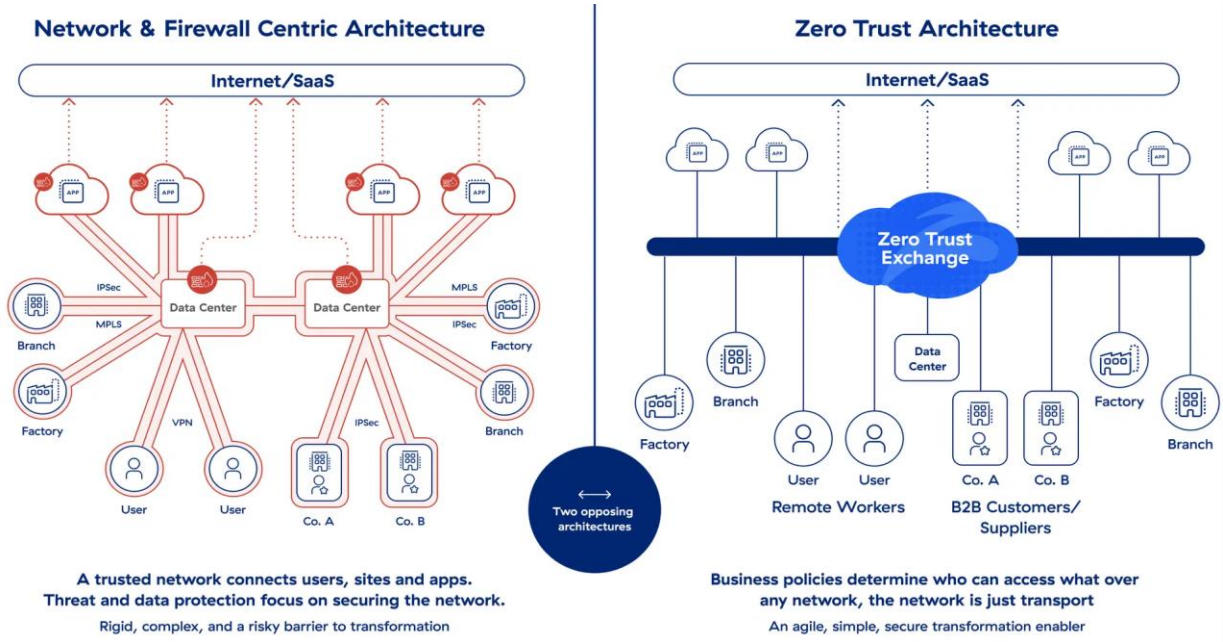


Figure 1: Example Zscaler Zero Trust architecture to reduce the risk of lateral movement

[2] Zscaler – Extend SSE Beyond Your Users

Case 2: Secure remote access

Leveraging ZPA for secure remote access to Operation Technology (OT) control systems

SCENARIO

In the second case study, a client was faced with a scorched earth scenario. This means everything has been encrypted and put out of action. Almost no asset escaped the impact of the malicious code encrypting its storage.

The client runs industrial systems that deal with very high volumes of goods and majority of the OT control systems were impacted by ransomware. The impact was clear, goods were not moving, and conveyor belts were at a standstill.

As a recovery team we were faced with zero documentation. As a result, we needed to reverse engineer systems functionality from the on-site team's memory, and then rebuild it. Amongst that was the need to provide the industrial operators with remote access to the operational technology.

The attacker gained access via the client's VPN connection using compromised credentials. From there the attacker was able to move laterally across the flat network, compromise a domain administrator account and distribute the ransomware. A summary of the kill chain is shown in Figure 2.

As one might expect, the desire to restore VPN access, the initial entry point, was not favourable. However, any new solution had to overcome all the usual constraints within an OT environment and adhere to the core recovery principle – always recover into a secure future state and not the vulnerable past state.

1. **Initial Access**
   Attacker gained access to the client's VPN connection using previously compromised credentials.
2. **Privilege Escalation**
   Attacker used default credentials to escalate to Domain Administrator.
3. **Command and Control**
   Attacker used legitimate remote access software to establish interactive command and control channels.
4. **Lateral Movement**
   Attacker used tools to pivot and move between hosts across the network.
5. **Exfiltration**
   Attacker stole a large volume of data containing IP and Personal Data through multiple methods.
6. **Ransomware Execution**
   Attacker executed ransomware encrypting systems and data.

Figure 2: A simplified version of the kill chain in this case

Case 2: Secure remote access

Leveraging ZPA for secure remote access to Operation Technology (OT) control systems

CHALLENGE

Constraints	Security requirements
OT network segmentation is limited due to (i) incomplete understanding of data flows and (ii) the need to maintain integrity of OT communications, as IP addresses are frequently hardcoded into applications without feasible options for IP address changes.	There must be no lateral movement between hosts.
The operators need to have a high stability connection to the target system.	There must be an additional authentication request (MFA prompts) on access attempts where the context is insufficient (no valid time-bound session cookies).
The operators need to have remote access to systems in the event of on-site disruption.	There must be a way to enforce security across managed and unmanaged devices.
The operators need to transfer code and software packages to the target system.	There must be available a secure file transfer mechanism with low latency and high stability.
The operators need to access Kiosk and Human-Machine Interface (HMI) systems with their existing workflow of common credentials.	There must be a way to verify all access requests explicitly and inject the specific OT authorised credential.

SOLUTION

The identity team focused on segregating identities to enforce least privileged authorisations and the network team focused on creating a secure access path that gave a point-to-point access to OT systems and prevented lateral movement over a flat network. The resulting conceptual architecture (see Figure 3).

OUTCOME

To restore third party administrator access, the Deloitte team provided a suitable architecture based on the above concept and implemented the Zscaler-based Privileged Remote Access (PRA) solution **within 60 days**, and over 2000 access paths to applications were made available through this.

The design and implementation of the solution took weeks instead of months, facilitating remote support and expediting the restoration of business operations. Consequently, the client witnessed a rapid return on their investment as services were restored faster.

Case 2: Secure remote access

Leveraging ZPA for secure remote access to Operation Technology (OT) control systems

Benefits of Zscaler PRA solution include:

- Ability to include Multi-Factor Authentication for OT access via a PRA web-based console
- Removing direct and permanent access to target OT systems with pixel scraping, and reducing the amount of network re-architecture required
- Protecting against malware for files uploaded by users in the remote access session

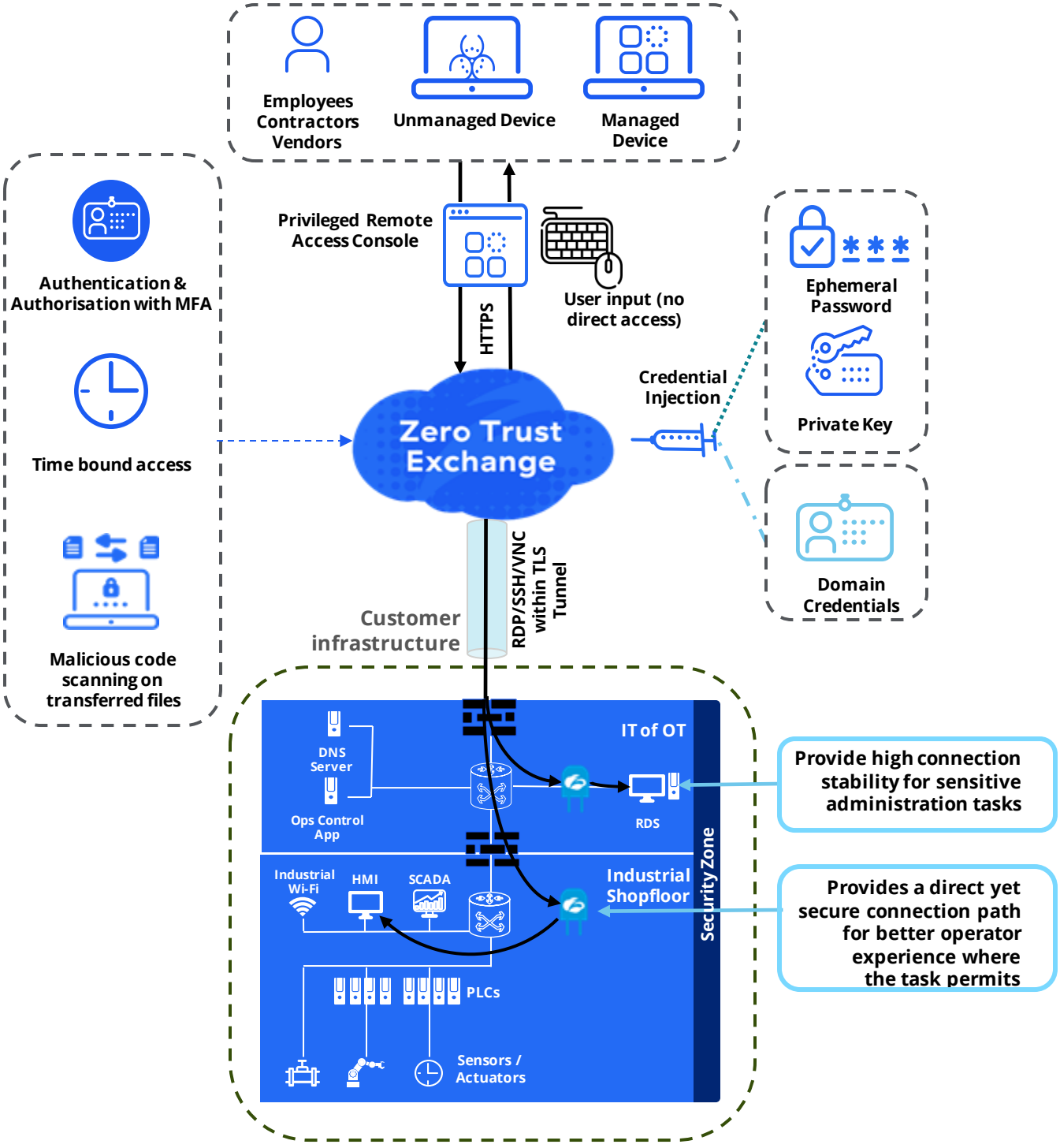


Figure 3: Conceptual architecture deployed in Case 2 using Zscaler Privileged Remote Access capability for OT Control Systems

Case 3: Recovery before SSE technology was available

Recovering networks back to the status-quo using traditional methods

SCENARIO

In this case our client suffered an attack of equal devastation as in the previous examples.

As a result of a ransomware attack, the client faced challenges in managing its shipping and terminal operations, booking systems, and communication networks. The company reported substantial financial losses due to the impact on its business operations of around $300 million.

SOLUTION

In this instance, the client did not adopt a Zero Trust or SSE architecture as part of the recovery. This is mainly because the event happened before this approach gained significant industry recognition.

Following the incident, the company faced the difficult task of rebuilding its digital infrastructure. The organization embarked on a thorough and time-intensive IT overhaul, involving meticulous reviews of numerous firewall rulesets, implementation of intrusion detection/prevention systems, and the reconstruction of multiple VPN entry points.

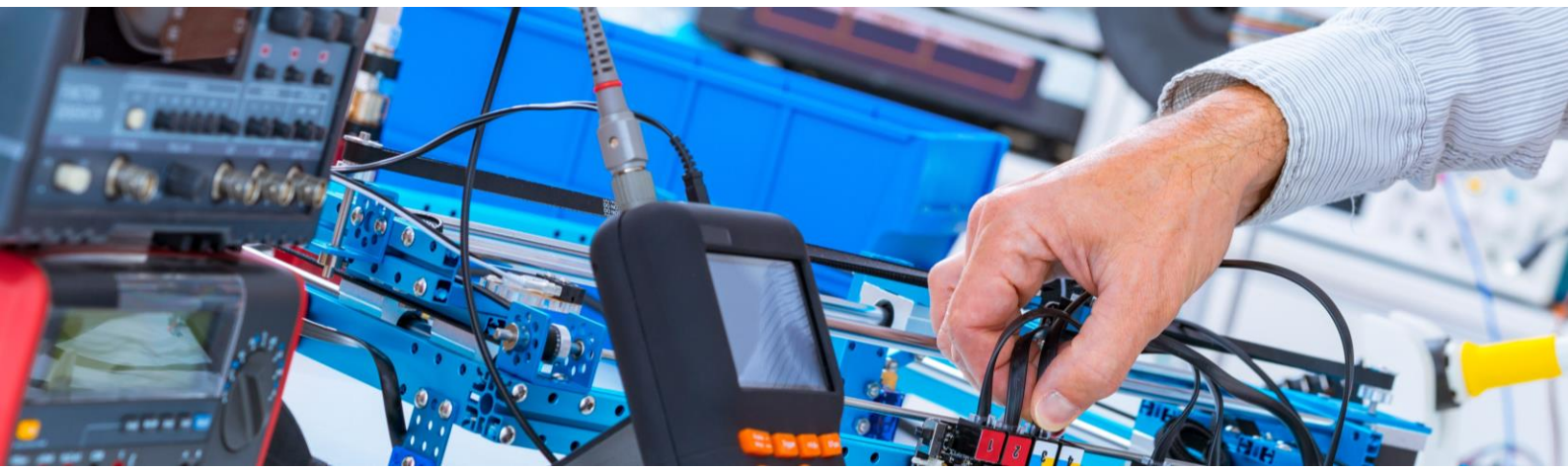
All this was started in the first 90 days of the incident. Yet work continued in the subsequent months to complete the recovery and meet the new security standards. Far longer and more complex than an SSE approach requires.

OUTCOME

Following an extensive and challenging process, the enterprise achieved greater resilience. However, the recovery period spanned months rather than weeks.

COMPARISON

An SSE-based recovery approach offers several significant time-saving benefits. The primary advantage is the reduced time and urgency needed for reviewing internal routing rules. Inherent in this approach is to funnel network traffic to a Zscaler Private Access (ZPA) broker. This means an access broker becomes the enforcement point and the network is for transport only. Put simply, the access broker functions as the primary gateway for all traffic, while the firewall directs traffic to its authorized destinations.



Conclusion – Recovering at speed

Deloitte and Zscaler recover enterprises and migrate you to a modern, safer Zero Trust approach rapidly and allow you to build back better

RECOVERING AT SPEED

Comparing each of these three enterprise recovery scenarios, we can see that the time taken to recover differs dramatically. In the first and second enterprise recovery scenarios we deployed SSE architecture and created secure access paths using Zscaler, which took 30 days and 60 days respectively; however, in the third scenario where we had to recover VPNs and Firewalls, it took over 90 days to restore trust in secure connectivity.

Recovery of the network is on the critical path to re-establishing the Minimum Viable Company. The longer the network takeback takes, the more money is lost each day. Therefore, having a proven, fast recovery method directly impacts the bottom line positively. Recovering control and trust in a network is achieved much faster when adopting an SSE-based architecture. This approach allows us to allows us to create secure access paths for users and administrators back to systems and data and reduces the risk of lateral movement.

In an Enterprise Recovery scenario, the focus is on delivering secure access back to data and applications to recover revenue generating services to achieve the MVC. Our approach has shifted the MVC goalpost and shortened the time by around a third. Deloitte now routinely target the **recovery of an Enterprise's MVC** to be accomplished **in approximately 30 days**.

Deloitte and Zscaler provide prompt solutions to some of the most pressing business challenges especially during incidents. We recognise that your organisation may encounter additional scenarios where a swift, secure transition to Zero Trust is advantageous. Deloitte and Zscaler are equipped to address these challenges effectively in both stable and critical times.

Accelerate your Zero Trust journey

Leverage extensive Deloitte Enterprise Recovery experience, for migration to a Zero Trust approach which can yield return on investment within months, rather than years.

ACCELERATING YOUR ZERO TRUST JOURNEY

Moving to Zero Trust through adoption of SSE has become a business imperative for the various reasons below:

- **Improve user experience –** the move towards hybrid working demands seamless access to applications and data;
- **Reduce and simplify your technology stack** – the convergence of Digital Workplace and Security in the form of SSE offers an opportunity to simplify enterprise technology stacks, licensing costs and operational staff costs;
- **Reduce cyber insurance premiums** – provides confidence to insurers that your risk of lateral movement is mitigated, and we have seen enterprises able to newly obtain cyber insurance as a result;
- **Simplify Mergers & Acquisitions –** allows organisations to be spun off or integrated easier ultimately providing speed in pre and post deal;
- **Increase security –** providing users access to resources only rather than the network, enterprises can reduce the attack surface, the risks of lateral movement and business compromise as well as protect confidential data and IP.

The Zero Trust journey is often daunting at the start. However, our approach offers you the opportunity to complete your project in months not years with rapid deployment even in normal scenarios. Thus, allowing you to realise return on investment much sooner.

Deloitte offers unparalleled expertise and experience to guide you through the most complex, time-sensitive, and large-scale challenges an enterprise may encounter. Our proven approach, tested in the most demanding scenarios, instils confidence in accelerating your Zero Trust journey. With us, you can expect smooth, on-time, and on-budget delivery.

As Zero Trust rapidly becomes the industry standard, endorsed by CISA, the US Government, and NIS regulations, we are ready to assist you in adopting SSE. Not only will this ensure compliance with standards, but it will also address the systemic security vulnerabilities inherent in existing control points within your environments.

By making life significantly more challenging for attackers, this solution safeguards your business, our livelihoods, and the global supply chain. This is a critical step forward in ensuring a safer and more resilient future for all. Contact us to start your journey.

Contact us

Sydney Grenzebach
sgrenzebach@deloitte.co.uk
Partner
Sponsor

Wil Rockall
wrockall@deloitte.co.uk
Partner
Sponsor

Kelvin Ren Jian Wong
kelvinrenjianwong@deloitte.co.uk
Director
Contributor

Jack Borg-Cardona
jborgcardona@deloitte.co.uk
Senior Manager
Author

Vikash Mukesh Laxmidas
vlaxmidas@deloitte.pt
Senior Manager
Contributor

Sadeq Ahmed
sadeqahmed@deloitte.co.uk
Manager
Author

Other Contributors, Reviewers and Thank You's

Tatai Krishnan (Zscaler), Partner Solutions Architect, tkrishnan@zscaler.com

Emma Cabban (Zscaler), Global Alliance Manager, ecabban@zscaler.com

Luis Silva Abreu (Deloitte), Partner, labreu@deloitte.pt

Anna Burrell (Deloitte), Director, aburrell@deloitte.co.uk

Tiago Pereira Marques (Deloitte), Senior Consultant, tiagomarques@deloitte.pt

Jon Lam (Deloitte), Senior Manager, jdlam@deloitte.co.uk

Craig Clydesdale (Deloitte), Marketing Manager, cclydesdale@deloitte.co.uk

Deloitte.