

# Data is the New Perimeter

---

“Shift-Up” Zero Trust to  
Cover Application Data

**Karim Eldefrawy, Ph.D.**  
Co-Founder & CTO

# Introduction:

## Zero Trust is not a silver bullet.

**Think Zero Trust is infallible? Think again.**

Zero Trust (ZT) has become a central paradigm in cybersecurity, and rightly so. Today's increasingly fluid network perimeter has long rendered legacy "castle and moat" security paradigms ineffective. With cyber threats emerging from all vectors, organizations can no longer afford the implicit trust assumed by perimeter-based security measures. They need a more resilient approach to security and access control, and this is where ZTNA (Zero Trust Network Access) takes center stage.

Yet, ZTNA is not a silver bullet for solving all enterprise cybersecurity challenges. Most notably, it focuses on controlling access to the network and infrastructure holding the data, leaving the data itself less protected. As data breaches carry increasingly severe consequences, potentially crippling businesses, ZTNA must evolve. It must extend its coverage to application data itself and business logic within the application layer of the TCP/IP stack — an approach we refer to as **"Shift-Up" Zero Trust**.

In this paper, we explore the "Shift-Up" Zero Trust approach and its ability to make sensitive data inherently secure wherever it ends up. We also explain how Confidential supports this next evolution of ZT through fine-grained adaptive cryptographic controls, which can be applied directly to the data itself, or even specific portions of it.



# "Never trust, always verify"

## Understanding ZTNA's core principles

The legacy "castle and moat" approach to network security defends a well-defined corporate perimeter. It assumes implicit trust for everyone inside the perimeter, essentially treating them as verified, authorized users. This approach grants malicious actors complete freedom if they manage to breach the perimeter. Once inside, they can move laterally across the network, accessing, manipulating, exploiting, or exfiltrating data at will.

Gartner coined the term "Zero Trust Network Access (ZTNA)" in 2019. It is a different type of security perimeter architecture that replaces the traditional "trust, but verify" approach with a "never trust, always verify" philosophy. This newer approach acknowledges that threats can originate from anywhere – inside or outside the network. As a result, ZTNA mandates continuous verification of all users and devices attempting to access enterprise resources, regardless of their location.

### ○ Least Privilege Access

Users & devices can access only what they need.

### ○ Micro-Segmentation

Different network segments for different types of traffic.

### ○ Explicit Verification

Verify every user, device, or system before granting access.

### ○ Contextual Awareness

Continuous monitoring for detecting suspicious patterns and behavioral anomalies in real-time.

### ○ Continuous Adaptive Trust

Adjust trust levels based on evolving context.



# The Problem with ZTNA

Basic implementations of ZTNA focus mostly on controlling interactions between users/endpoints, the corporate network, and its resources. As such, they do not yet secure the data itself.

Here are a few scenarios where ZTNA falls short in protecting data -- ***the most lucrative target for cybercrime.***



## Scenario 1

An authenticated employee, either mistakenly or intentionally, uploads a document containing sensitive information to an authorized SaaS application. The backend of the SaaS application gets compromised, and sensitive information is exposed.



### Why ZTNA fails

SaaS applications often store or have access to critical corporate data. However, current ZTNA focus does not easily extend to third-party SaaS environments. If the SaaS vendor suffers a breach, sensitive data stored on their servers may become vulnerable.

## Scenario 2

Authorized device that is approved due to BYOD policy gets infected with a double extortion ransomware. Ransomware exfiltrates data from the device storage, including data or documents accessed during work.



### Why ZTNA fails

ZTNA cannot prevent attacks exploiting vulnerabilities in legitimate software. For instance, if a ransomware compromises a BYOD device through malicious code hidden in a verified update (think the notorious SolarWinds hack), it can disguise exfiltration attempts as legitimate traffic and bypass ZTNA controls.

## Scenario 3

A malicious insider downloads, compresses, and encrypts documents with potentially sensitive data to exfiltrate them without alarming security systems.



### Why ZTNA fails

If the insider's actions appear consistent with their usual behavior and access patterns, ZTNA will not flag the activity as suspicious. Therefore, if an employee compresses and password-encrypts sensitive data before transferring it to external storage devices or sharing it via email, all usual employee activities, it can fall under ZTNA's radar.

# Bridging gaps with “Shift-Up” ZTNA

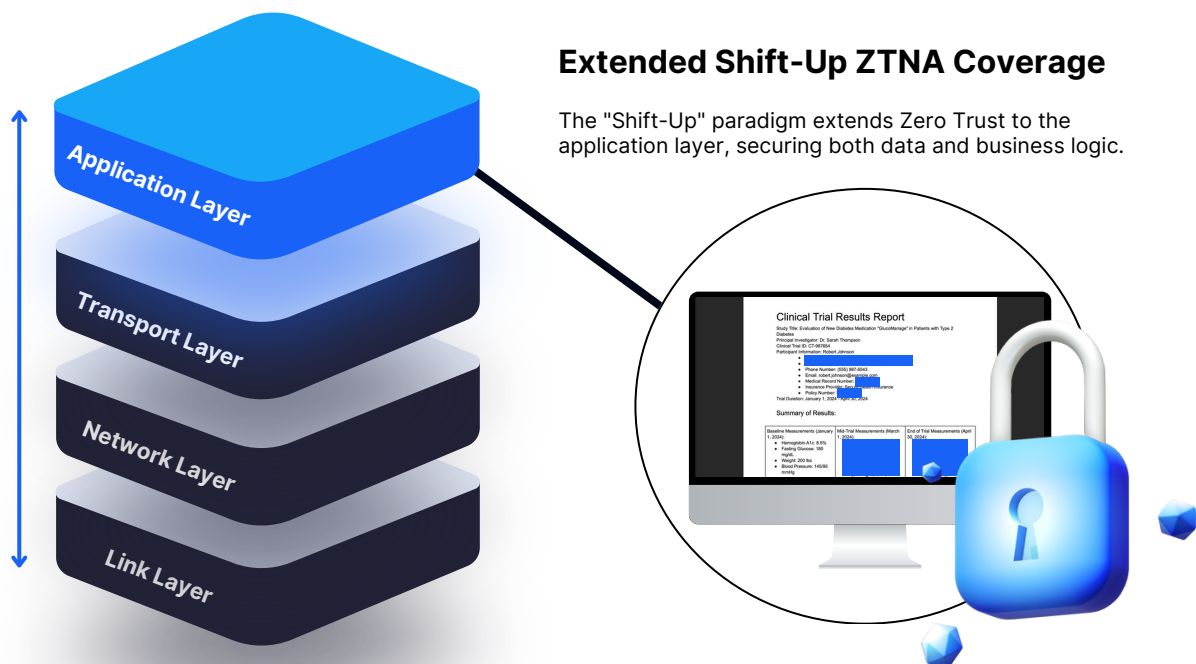
## A New Paradigm in Zero Trust

One way to protect from elusive threats such as those mentioned above is to extend the ZTNA principles, otherwise focused on the network and infrastructure, to the application data itself, especially sensitive portions of such data. This new paradigm is what we refer to as “Shift-Up” ZTNA.

To understand this new approach of shifting ZTNA principles up to reside inside the application layer in the TCP/IP stack, it is important to first understand where traditional ZTNA operates in the stack.

The TCP/IP stack forms the very foundation of the internet and networking. It provides a set of rules and procedures for how data is packaged, transmitted, and received over networks like the internet.





Traditionally, ZTNA security is mostly concerned with the lower layers—particularly the network and transport layers. It focuses on securing the connections and transmissions between devices and networks. Although some core functions, such as network segmentation, can be applied at both the network and application layers, ZTNA implementations often only provide coarse, packet-level access control even at the application layer. They lack fine-grained controls at the sub-app, service, or data level. This limitation creates exploitable gaps, as illustrated in the above scenarios.

To bridge these gaps, our suggested "Shift-Up" paradigm extends the reach of ZT principles into the application layer, particularly to the data and business logic inside the application. It ensures that ZTNA's security mechanisms go beyond securing application connections to directly engage with the data and resources most valuable to organizations.

# What is Shift-Up Zero Trust?

## Granular Access Controls

### Unparalleled precision.

Define who can access what, down to individual fields, objects, and/or pages in documents if necessary.

## Advanced Policy Management

### Tailored permissions.

Create granular policies to authorize users to access specific data and app functions.

## Shift-Up Zero Trust



## Fine-Grained Encryption

### Protect what matters most.

Apply encryption selectively to specific data elements within documents, databases, and containers.

## Data-Centric Security

### Protection beyond the perimeter.

Ensure data is protected at rest, in use, and in transit regardless of user, device, or location. Selectively decrypt in-memory only and trace usage activities.

# How Shift-Up ZT Fills ZTNA's Security Gaps

## SCENARIO 1 Compromised SaaS Application

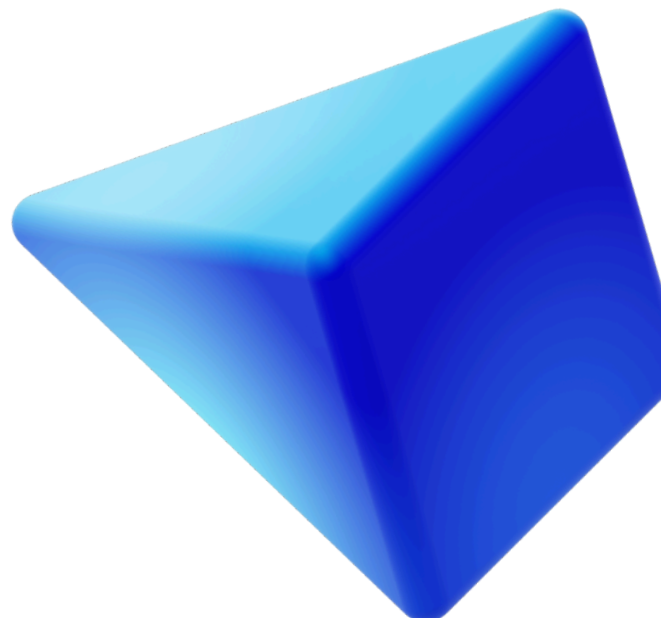
Shift-Up ZT advocates for protecting sensitive information in documents before uploading them to third-party cloud storage or SaaS applications (especially if such applications do not need to process sensitive data). Protection via encryption renders sensitive data unreadable by unauthorized entities. Even if the SaaS application gets compromised, attackers will not obtain the sensitive data.

## SCENARIO 3 Insider Threats

Shift-Up ZT's selective use of encryption can limit access to specific sensitive portions of the data, which means that authorized insiders do not always view all protected information in folders they may have access to. Additionally, because sensitive data is decrypted only for legitimate users on an as-needed basis (e.g. when a document is opened for viewing), exfiltration becomes a much more arduous task.

## SCENARIO 2 Ransomware-infected BYOD Devices

Shift-Up ZT imposes granular, policy-based cryptographic access control for the sensitive documents and even fields/objects *inside* documents. Selectively encrypted content remains intact and protected even if stored on compromised devices. This ensures that ransomware cannot decrypt or read the sensitive data stored on disk, nor can it manipulate or exploit it after exfiltration.





## The Shift-Up Advantage

Shift-Up ZT builds upon the strengths of ZTNA by adding flexible and tunable data-centric security measures. It enables realization of a stronger data security posture and provides more comprehensive protection, that travels with the data and documents as they move around. Specifically, Shift-Up ZT offers:



### Reduced Attack Surface

By encrypting data and documents, Shift-Up ZT minimizes the impact of malware or compromised systems as attackers cannot access protected sensitive information.



### Enhanced Data Protection

Data encryption throughout its lifecycle (at rest, in transit, and in use) ensures its confidentiality even after data leaves the enterprise or network.



### Secure-by-Design Applications

Embedding Shift-Up ZT features directly within applications and data storage systems right from the initial phases of the software development life cycle (SDLC) can ensure intrinsically secure applications.



### Granular Access Control

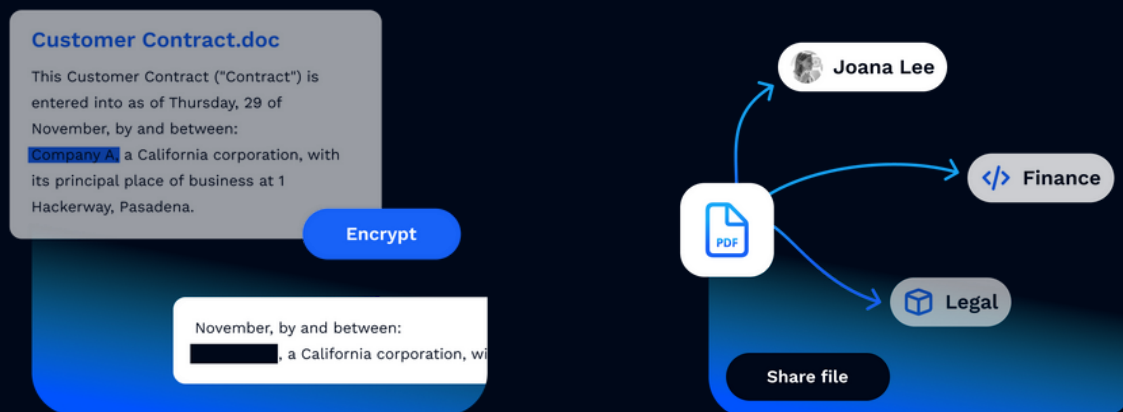
It allows for more precise control over what users can do with data, limiting insider threats and accidental data leaks.





# Understanding Shift-Up ZT’s Fine-grained Cryptographically Enforced Access Control

Fine-grained cryptographically enforced access control is at the heart of the “Shift-Up” paradigm. In simple terms, it is the idea to selectively utilize encryption within the application layer to reinstate fine-grained access control. Fine-grained control refers to the capability to apply these policies at a very detailed level—down to individual data fields inside files and documents, or even specific elements within an application.



## 01. Data-Centric Security

By embedding security and access control mechanisms at the sensitive data or object level, security becomes intrinsic to the data. The protection mechanism now travels with the data across networks and devices, extending the perimeter to data rather than the pathways it traverses.

## 02. Scalability

Cryptographic solutions can be scaled easily across large and diverse environments, providing a consistent method for securing data across various platforms and applications.

## 03. Enhanced Privacy

Data encryption and the need for the proper cryptographic keys for access raises the barrier for unauthorized access.

## 03. Flexibility

Selectively using encryption and fine-grained controls allow organizations to tailor access rights to specific needs and roles of users.

# Data Classification: A Major Challenge in the Shift-Up Paradigm

One of the main challenges in implementing Shift-Up ZT is accurately classifying which data, or portions of data, need protection. It is one thing to identify sensitive data in structured storage or just a few documents; however, scaling manual classification to unstructured data spread across millions of files, documents, data containers, and databases is virtually impossible. It must be automated.

## AI and ML-powered Automation for Data Classification and Selective Encryption

Organizations must leverage automation to scale data classification and apply selective encryption and fine-grained access control across all unstructured corporate data. However, the accuracy of automated data classification depends on the quality of underlying algorithms and trained models, which indirectly depends on vast datasets used to train AI and ML algorithms and the sophistication of analytical capabilities driving the automation.

### Automation in classification

AI and ML-powered data classifiers can detect sensitive documents, like financial and legal documents, forms of intellectual property, as well as personal information, such as PII, credit card details, etc., held within the documents. Shift-Up ZT can leverage such data classifiers to autonomously identify and categorize sensitive information across large digital repositories.

### Automation in workflows

Integrating classification and encryption mechanisms directly into content generation and ingestion processes can boost efficiency and pave the way for incremental adoption. Automating these workflows can ensure that data is automatically classified and encrypted as soon as it is generated or ingested and remains protected throughout its lifecycle.



## Other Challenges



### Embedding Shift-Up ZT

Another major concern about the Shift-Up paradigm is embedding it in applications and workflows from the ground up. By adopting secure-by-design principles, such as enabling object-level encryption inside documents and files, and attribute-based, granular access controls in applications during the earlier design phases, organizations can seamlessly integrate Shift-Up ZT and ensure data security from the outset.



### Performance Concerns

Encryption and digital signatures at the application level can introduce significant computational and spatial overhead, especially when applied to various objects within documents. This overhead can negatively impact the application's responsiveness and throughput. However, the performance impact can be minimized by carefully using the appropriate cryptographic primitives for each task. For example, efficient symmetric encryption algorithms encrypt the actual (bulk) data while only the symmetric key is encrypted via expensive public-key schemes.



### Key Management

Key management systems (KMS) and fine-grained access control can become a significant challenge as cryptographic access control scales across an organization's digital assets. Shift-Up ZT requires scalable and robust key management systems and policies. Integrating with existing identity providers (IDPs) and third-party KMS, and initially implementing Role-Based Access Control (RBAC) while allowing for migration to Attribute-Based Access Control (ABAC), can offer a realistic deployment path. This approach helps offload the burden of managing these complexities and ensures higher resilience and security through the provider's dedicated expertise.

## "Shift-Up" with Confidential

Confidential provides a data-centric security solution that can be embedded into organizational workflows to automatically safeguard sensitive information throughout its lifecycle. Confidential's AI-based, data-centric approach inherently enhances ZTNA implementations through:

### ★ **Selective Encryption**

Encrypt entire documents or specific sections or objects in them.

### ★ **Fine-Grained Access Control**

Tailor what is visible to different individuals or groups.

### ★ **Lifelong Protection**

Security and access control follow data throughout its lifecycle.

### ★ **Post-Quantum Cryptography**

Seamlessly upgradable to NIST's future-proof post-quantum algorithms.

### ★ **Intelligent Monitoring**

Advanced AI models quickly learn and recognize anomalous behavior patterns, improving accuracy and accelerating response as time goes on.

### ★ **Adaptive Trust**

Automatically adapt policies to revoke access as needed, based on real-time situational awareness.

### ★ **Automated Protection**

Automatically scan and detect sensitive information across any volume of unstructured data sets in both local and cloud environments.

### ★ **Data-Blind SaaS**

Confidential never accesses or stores your data, your data never leaves your infrastructure.

### ★ **Improved Traceability**

Detailed activity logs to track document access, even as it leaves your infrastructure.

### ★ **Seamless SaaS Integration**

Embed within cloud and SaaS applications, like email and Office tools, to provide users with real-time actionable insights and single-click security implementation when needed.

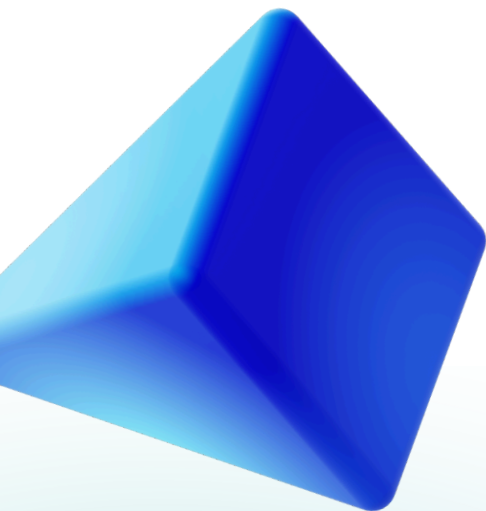


## Who we are

Confidential is at the forefront of data-centric security solutions, offering automatic and intuitive protection that safeguards unstructured sensitive data at every stage of its lifecycle - from creation through sharing and into storage. As the pioneer in data-blind technology for high-stakes sectors, Confidential protects content within documents, enabling secure sharing, collaboration, signing, and utilization in the AI era. Confidential's underlying patented technology was developed by SRI for DARPA, used across 170+ organizations in 34 countries, and awarded the Cyber Solution of the Year for 2023 by PwC Luxembourg.

## What we do


At Confidential, your trust is our most valuable currency. We are committed to upholding the highest standards of data protection, ensuring that your information remains confidential and secure, always. Our flexible, adaptive approach ensures that your data remains secure against both current and emerging threats. Join us in our journey towards a more secure digital future.



# Get in touch.

 [confidential.io](https://confidential.io)

 [linkedin.com/company/confidential-inc/](https://linkedin.com/company/confidential-inc/)

 [hello@confidential.io](mailto:hello@confidential.io)