Paperclip

White Paper

Zero Trust Architecture & Paperclip SAFE®

Where do I begin…

Zero Trust Architecture (ZTA) is a cybersecurity framework that can improve your security posture by replacing perimeter security as we know it. We need ZTA today because threat actors have defeated perimeter security and have demonstrated their free will inside the infrastructure. ZTA offers a superior alternative, based on the core tenet of ***"never trust, always verify."*** Paperclip SAFE® enables effective implementation of a ZTA through its process-based micro-segmentation secure storage system. With its ability to enforce granular segmentation, SAFE supports the realization of ZTA initiatives.

Some Background

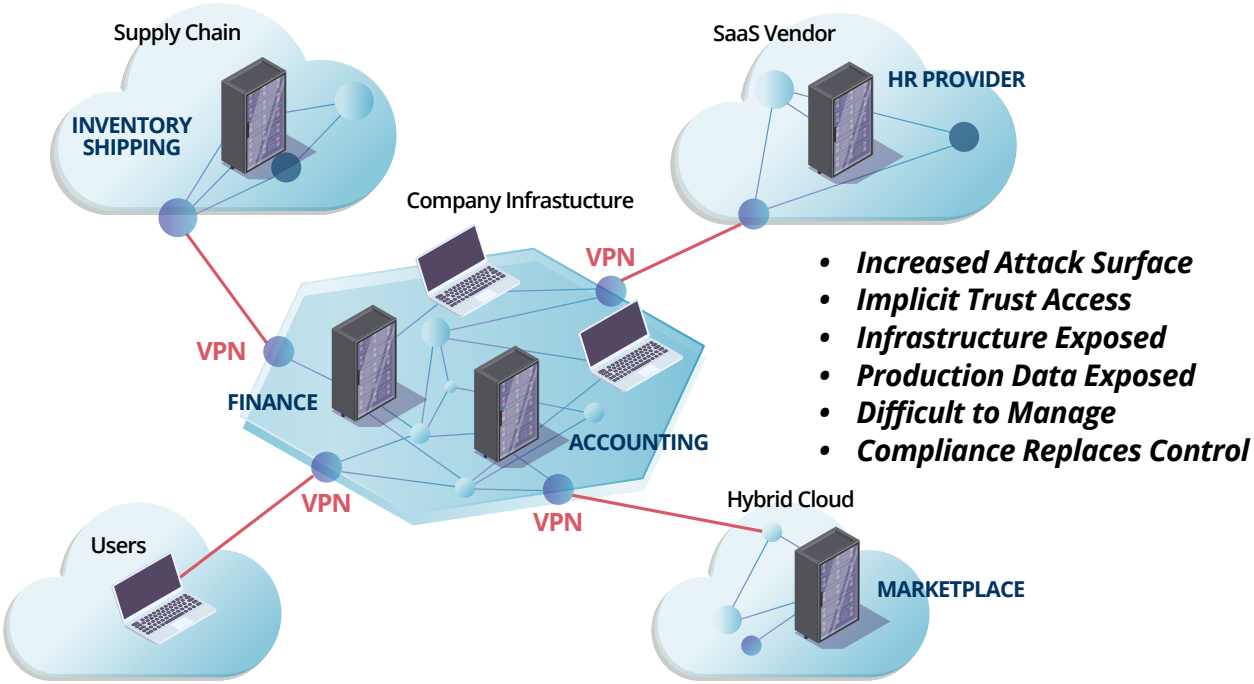
Traditional perimeter security has become obsolete simply because we have vacated the perimeter. Work from home, cloud SaaS vendors, electronic commerce and electronic content have been major factors for working outside the perimeter. To keep everyone secure, IT and security organizations have spent the last decade focused on hardening the perimeter with innovative, complex solutions such as VPNs for home workers, secure communications with the supply chain, multifactor authentication (MFA) and encryption. Yet, these efforts have not yielded the desired results.

We now have an "extended perimeter." As depicted in the figure below, the extended perimeter has effectively expanded the attack surface and exposed our digital assets to increased levels of risk. Now, every endpoint connected to the perimeter is an evolving vulnerability. Phishing reigns supreme as the number one tactic (responsible for 90% of data breaches) to introduce malware and other attack tools that break perimeter defenses, all with the end goal of accessing your most valuable data.

Indeed, to date, MITRE, a nonprofit research laboratory, has documented 14 tactics and over 760 techniques that attackers have utilized to enter the perimeter. Once inside the perimeter, attackers exploit critical data for monetary gains by ransom, theft, destruction, and all of the above. In 2022, cybercrime cost companies and people around the globe $6 trillion. Experts predict this will increase to $10 trillion by the end of 2025. If cybercrime were a country, it would have produced the third largest GDP, ahead of Japan, Germany and the United Kingdom (StatisticTimes.com).

It was in this context that the ZTA initiative began back in 2010, led by the U.S Defense Information Systems Agency (DISA) and Department of Defense (DOD), with the Black Core Project. One of project's leaders, John Kindervag, emphasized that all network traffic is untrusted. Early in the discussion, data was the emphasis, but midway through the process identities became the driver because of mobile and cloud adoption. Today with the released consensus of ZTA frameworks, ZTA now has defined methods, requirements, goals and objectives designed to replace the perimeter as we know it today.

Extended Perimeter



How Zero Trust works

Verification is the key to operationalizing the idea of "never trust, always verify." By default, no user or device is ever trusted for access until it has been verified in a Zero Trust environment. A ZTA will verify all users, devices, workloads, networks, and data access—regardless of where, who, or to what resource. This might involve advanced device analytics or the use MFA. Once verified, the user is granted the absolute minimum access, limited to whatever data, application, or network segment he or she requires—and nothing else. ZTA connects users securely to the resources they need by a secure endpoint to endpoint encrypted tunnel.

ZTA creates perimeters around resources known as micro-segmentation. There is a gatekeeper called the Controller, which is responsible for all access and connections. The architecture hides the infrastructure by eliminating the ability of attackers to laterally move across the network.

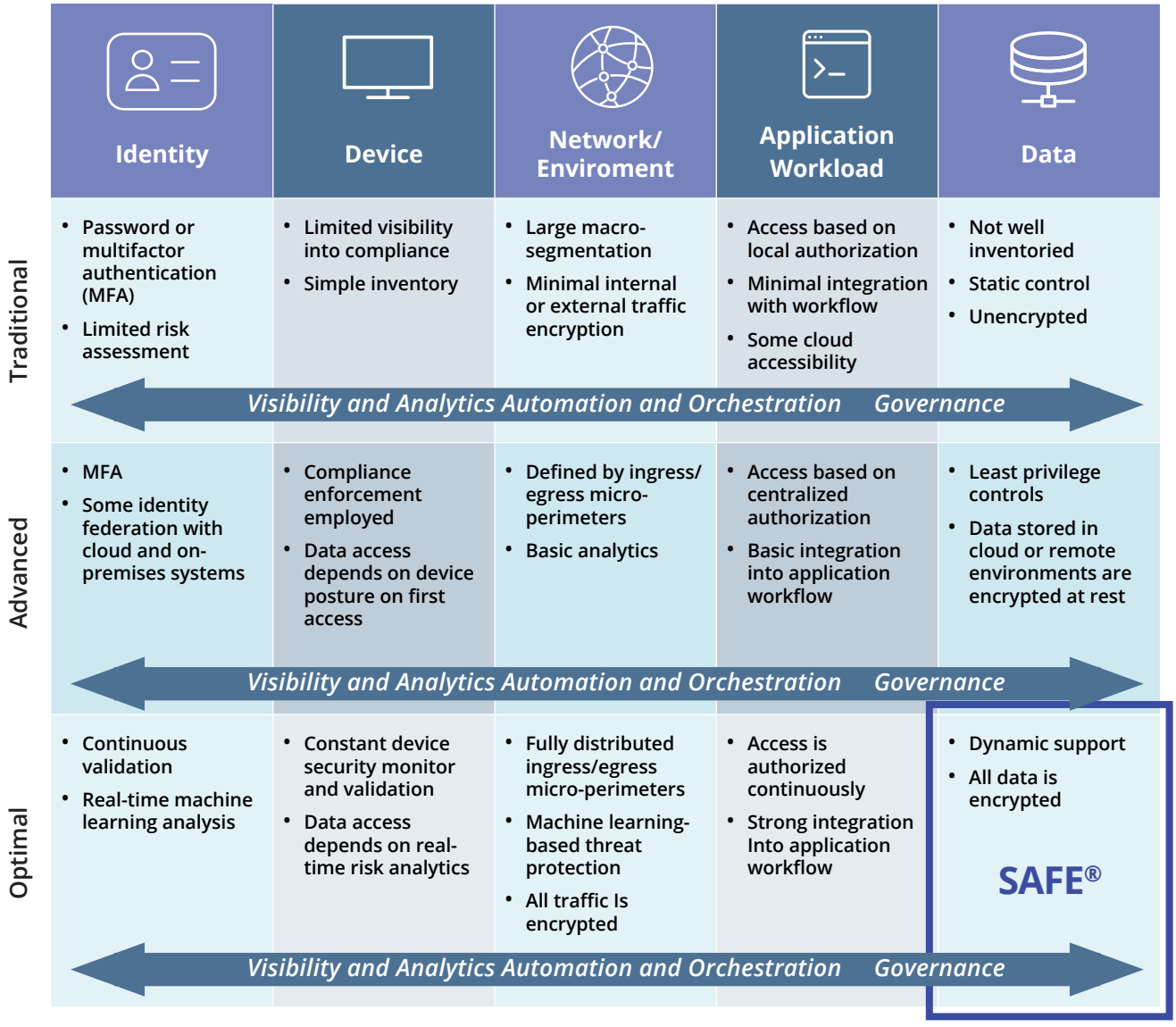
Another ZTA method is the separation of data and access into two planes whereby data flow only executes after access has been granted. By separating these two tasks, latency will be minimal as this process executes with every user hitting their enter key or clicking their mouse. Remember, all communications are untrusted and must be verified.

To understand the significance of these changes, consider how access works in today's traditional infrastructure. Users connecting to web app vendors for Human Resources (HR), Customer Relationship Management (CRM), purchasing (business transactions), analytics, compliance, security monitoring, etc., connect directly or through the company's virtual private network (VPN).

Many applications maintain their own access controls (e.g., login, password, MFA) for user access with different degrees of authentication and authorization. This architecture produces many vulnerabilities resulting in a significant attack surface. It also makes it quite difficult to enforce access controls and other security countermeasures.

ZTA introduces advanced posture wherein the basic implementation of ZTA components like Identity and Access Management (IAM) solutions are able to verify the user's identity and device. Then, Single Sign On (SSO) solutions grant access to secure application workloads. Data is accessed with minimal privileges required to process the workload or task. Data not in use remains encrypted (e.g., powered off devices, online archives, backup media).

Going further, optimal ZTA implementation introduces continuous oversight through automation and orchestration. Machine learning applied to users, devices, infrastructure, application workloads and data will be more responsive than people tasked with log reviews. In addition, data should always be encrypted and monitored for potential attacks, including encryption-in-use, at rest and in transit.

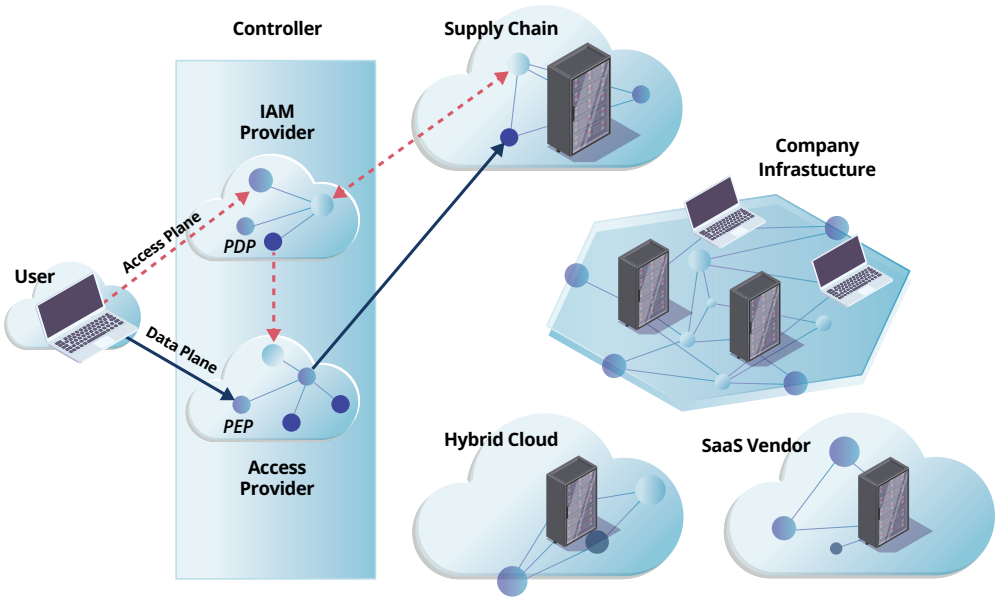


Cybersecurity and infrastructure Security Agency, Cybersecurity Division, June 2021

One of the constructs of ZTA is that most endpoints will have an agent installed. This agent will document the trusted endpoint and address for users and devices when checking them against the IAM solution. Workloads will be defined by the "Need to Know" implemented by Roles (e.g., full access to HR with limited work hours access to finance) and Privileges (e.g., HR access can create, read, update, and delete with finance access can read and update). In this model, IAM will monitor Roles while the Web Application will enforce the Privileges. ZTA moves user security out of the Web Application/Database to the IAM, where the Web Applications now participate in a Single Sign On (SSO) access model (e.g., SAML, OpenID, OAuth) from the IAM.

Zero Trust Architecture

Drop All Firewall only opens a connection when authorized by the controller.



1. **Users & Device authentication at IAM**
2. **IAM authorizes connection to Access Provider**
3. **Access Provider connects User to Resource**

- **Connections are encrypted tunnels isolating the other resources from view**
- **Monitoring of Users' activity with near real-time alerts**
- **Perimeter in now virtual, its connection based on IP/port based**

ZTA approaches the design of the infrastructure from the inside out versus outside in, which is the norm in today's perimeter security models. ZTA networks are micro-segmented around resources hiding behind firewalls, gateways, and proxy servers. ZTA data relies on encryption, automated machine learning monitoring and orchestrated responses.

It's worth considering ZTA if you want to get better at protecting your business from interruption due to lack of access to key operational data. Maintaining status quo perimeter security has proven that it just can't stop the breach. At best, it's partially effective. The continued rise in data theft events and costs dictate that a better approach must be implemented. Securing the infrastructure with perimeter security needs to evolve from the access-then-authentication model to ZTA's authentication-before-access model.

ZTA helps reduce the risk of data breaches that can potentially expose user identities, personal identifiable information (PII), intellectual property, financial accounts and other sensitive data. ZTA does this by offering a viable defense when utilizing Encryption-in-Use in addition to Encryption-at-Rest and Encryption-in-Transit. The architecture helps limit the impact of attacks through segmentation. ZTA can also reduce the costs of remediating a data breach or other serious security incident.

What are the critical assets to be protected?

Workloads that process data for an end result should be the highest priority for ZTA. Sensitive data is another critical digital asset that will benefit from ZTA's stronger protections. This might include data, that if exposed, would reveal personal identities, nonpublic information, financial access, intellectual property and medical information. Similarly, it's essential to protect data that will cause harm to individuals, organizations, and companies if made public. It's really all about the data—and the internet is 100% data.

What are the opportunity costs of not adopting ZTA?

By not adopting ZTA, you expose your organization to opportunity costs that include the potentially astronomical expense of handling a major data breach—coupled with the loss of reputation and business that come with such an event. You may get turned down for cyber insurance, which will further increase the cost of responding to a cyberattack. Your ability to comply with regulations may also be affected, which can result in fines and other liabilities.

How urgent is ZTA adoption?

That depends on how much business you engage in that has federal, state, or local government oversight. Certain US federal agencies are required to implement Zero Trust, by executive order, in the next two years. If you're in the financial, insurance, or medical industries, new compliance controls will start to appear in 2023 and many of them mandate Zero Trust.

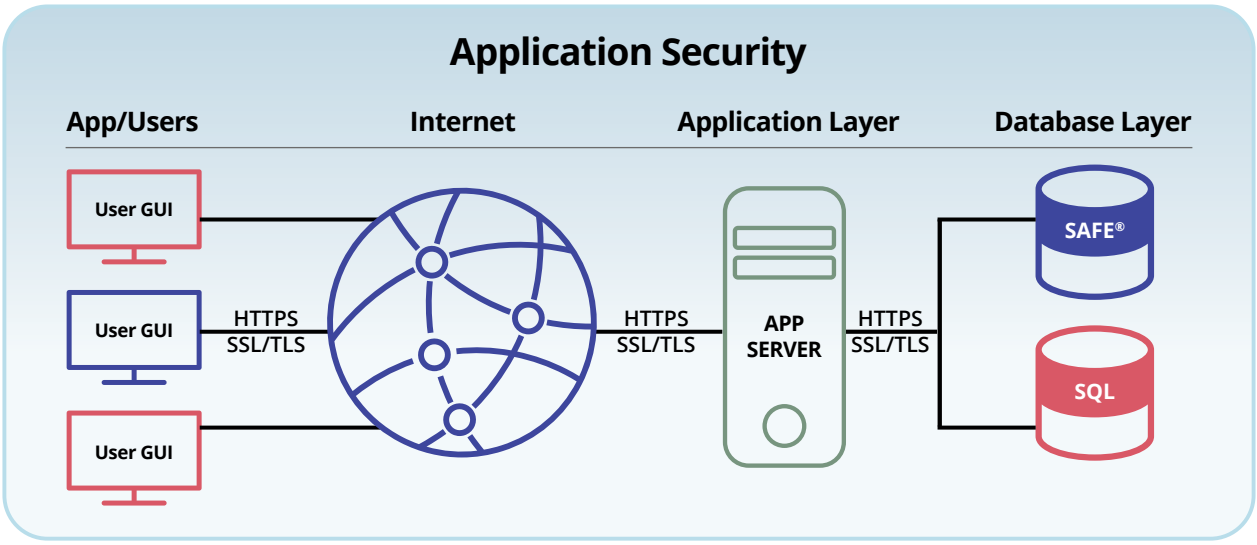
Organizations with greenfield projects and cloud infrastructures are prime candidates for ZTA because most new projects are being developed as containers which are then presented as micro-services to leverage cloud scaling. Micro-services use APIs to connect web applications or other processes. This approach aligns well with ZTA because micro-services function as resources that can be managed and monitored by the access controller.

Where does a company start with ZTA?

ZTA flips the perimeter security model by starting at the inside and working out. When you think inside, you're looking at the data layer. With ZTA, the most secure state is when the data layer always remains encrypted. ZTA's most optimal condition described within its fifth pillar of security is whereby the data always remains encrypted, and its environment is actively monitored. To make this work, you must encrypt data in use, not just at rest and in transit. You must enable applications to securely process plaintext data with an encryption-in-use solution.

Paperclip SAFE® and ZTA

Paperclip SAFE® is a foundational building block for a ZTA implementation. Functioning as a process-based micro-segmentation secure storage system, SAFE enables the kind of granular segmentation that is the essence of ZTA. The segmentation operates at the process or service level and only allows communications on specific network paths, protocols, and ports. This is a further realization of the ZTA idea. Process-based segmentation is more secure than traditional three tier-based segmentation.



SAFE protects critical information in the data layer, ensuring privacy with complex encryption and monitoring. SAFE provides the real-time ability to process data while it remains fully encrypted, only revealing the minimal plaintext data necessary for the application layer to process. Such encryption of the data layer during processing greatly reduces the attack surface. Encrypting the data in use will protect the privacy of its contents if it is breached and exfiltrated. Given that most breach regulations extend safe harbor if the data stolen remains encrypted, SAFE thus greatly reduces the business impact of a breach.

The monitoring of data, also part of ZTA's fifth pillar, provides a defense against ransomware attacks and the malicious code designed specifically to ransom the data. Monitoring data includes systems that can detect environmental (e.g., platform, OS, database, users and devices) change and data usage relationships via machine learning, automated responses and orchestration with other security resources.

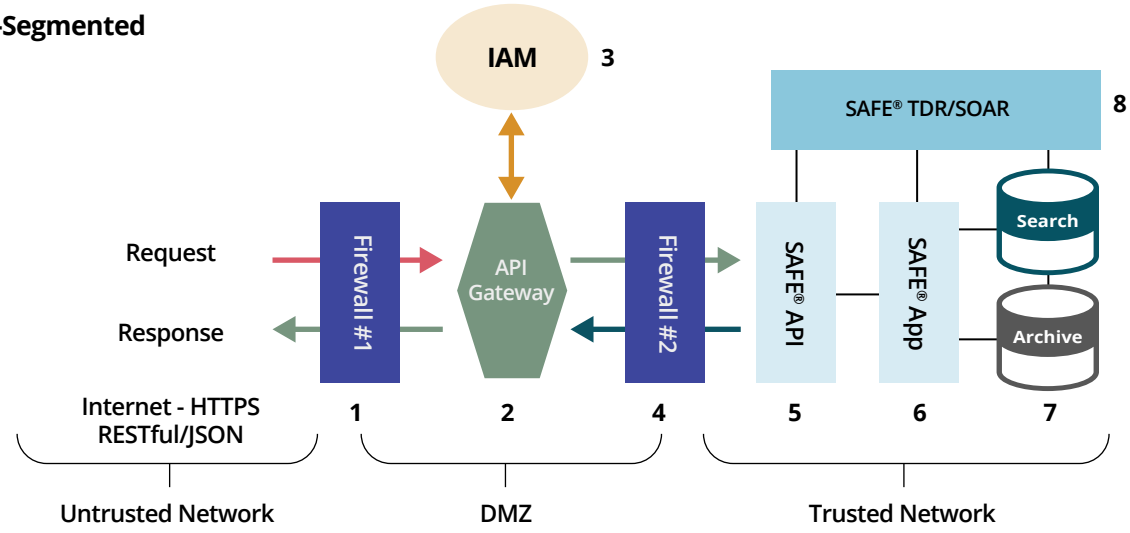
SAFE is designed for secure data storage on premises or in the cloud. SAFE plays an effective role in securing your data today inside the perimeter and integrates with any ZTA implementation.

SAFE as depicted in the below diagram is a micro-service. The SAFE system comprises the SAFE API, the SAFE application, two MS SQL databases and the SAFE threat detection and response (Items-5,6,7,8). These components are positioned behind firewall #2 resulting in micro segmentation. Access to the SAFE API is controlled by an API gateway (Item #2), in concert with the IAM controller for authentication and authorization.

Users via applications make requests to SAFE for any critical or sensitive data. A RESTful / JSON API request navigates firewall #1 to reach the API gateway. The API gateway communicates with the IAM to validate that the user and the application have current access based on their designated roles. The API gateway may then modify the request with additional information before releasing it to the SAFE API. SAFE will then execute the request and only decrypt the response data. This flow is repeated every time a request is processed. If the incoming request fails at the API gateway or at the SAFE API, that information is monitored by SAFE TDR and acted upon.

SAFE Microservice

Micro-Segmented



Zero Trust Architecture is the direction for better cybersecurity. As noted earlier, data was the initial emphasis of ZTA, and it remains the center of the conversation. Encryption-in-use is the future of necessary data security, and the Paperclip SAFE® solution is ready to deliver on this front.

You begin with Paperclip SAFE®

Paperclip Inc.
Mike Bridges, President

###