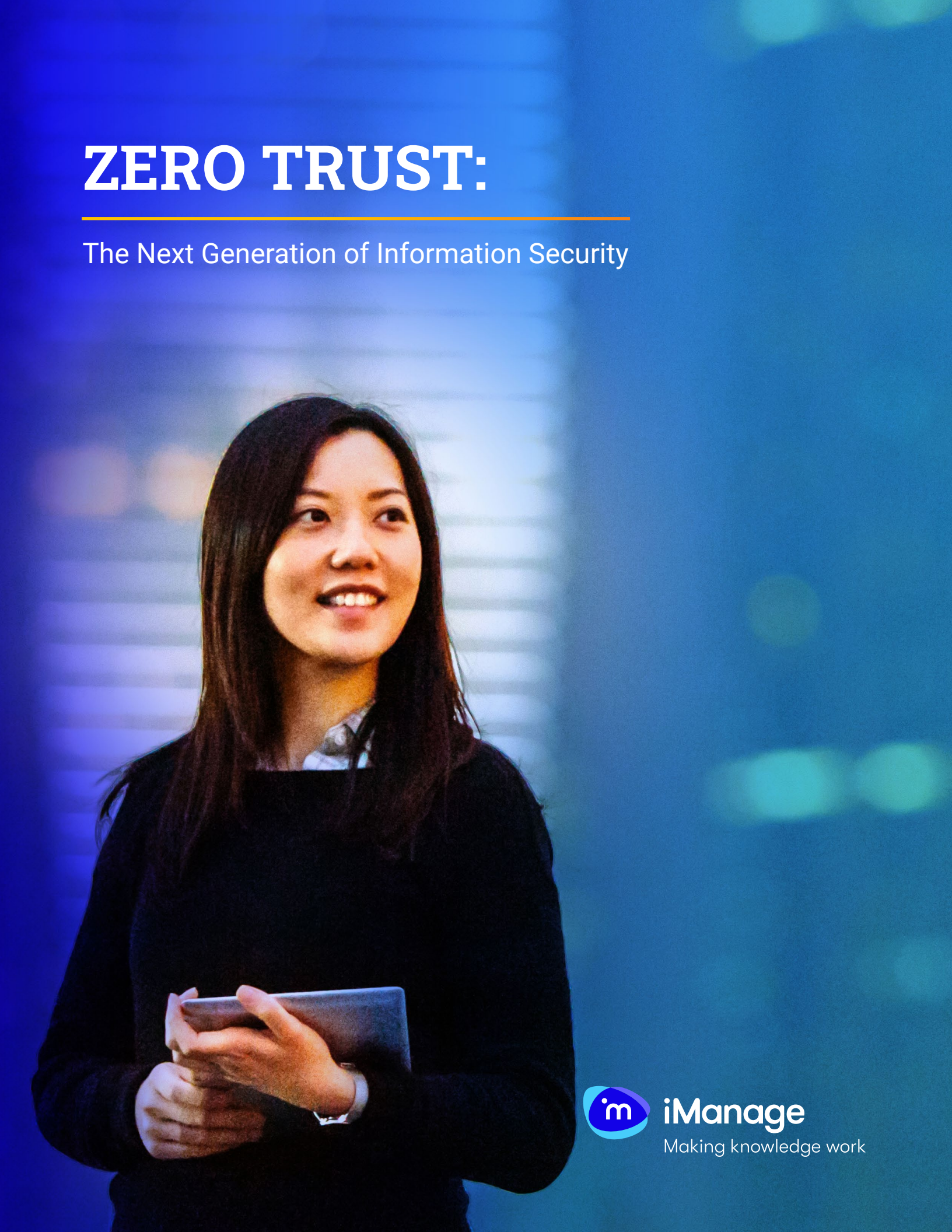
ZERO TRUST:

The Next Generation of Information Security



iManage

Making knowledge work

CONTENTS

© Copyright 2021 iManage

HOW ZERO TRUST DELIVERS BETTER SECURITY

As the landscape of security threats changes and grows, it becomes clear that the potential for data loss poses an existential threat to professional services firms. Trust is the cornerstone of any professional services firm's business, and any loss of confidence jeopardizes their relationship with customers. The rapidly evolving nature of threats requires these enterprises to adopt a more comprehensive approach to information security.

The concept of trust needs to permeate through all layers of a security architecture to ensure that previously assumed gatekeepers of access were not compromised by modern and sophisticated attack vectors. Many enterprises still rely on trust as a central component of their security posture at a single-entry point, for example, trust in the system administrator. Yet to guard effectively against today's threats, the nature of security defences must also evolve. Modern security needs to start with a major change in mindset around trust.

iManage has adopted this challenge as fundamental to its approach to service delivery. We have developed a robust security portfolio, built on the philosophy that security needs to be comprehensive, pervasive, and unobtrusive to the user. Our goal is to help our customers stay ahead of fast-moving security needs by adopting the best available strategies and technologies. Zero Trust is a next-generation security framework that ensures the highest level of protection for your critical data assets.

This white paper is designed to introduce the concept of Zero Trust and how iManage is implementing it across our platform.

© Copyright 2021 iManage

What is Zero Trust?

The Zero Trust security framework challenges the idea of trust in any form: trust of networks, trust between host and applications, even trust of super users or administrators. As Zero Trust experts Evan Gelman and Doug Barth explain in their book, a Zero Trust network always conforms to the five foundational principles below:

- "The network is always assumed to be hostile.
- External and internal threats exist on the network at all times.
- Network locality is not sufficient for deciding trust in a network.
- Every device, user, and network flow is authenticated and authorized.
- Policies must be dynamic and calculated from as many sources of data as possible." [1]

Successfully implementing a Zero Trust blueprint requires automation, strong authentication and minimal access privileges, limited to only what is necessary to accomplish the task at hand. It also requires rigorous vulnerability analysis of all software, and constant monitoring of the network for any anomalies.

The bottom line: in a complex and constantly evolving cyber threat environment, the best way to secure a network is to assume absolutely no level of trust. In an environment designed according to the Zero Trust model, no one person or account should be able to solely execute a change to the system that can affect the security of the system.

iManage Zero Trust Architecture

The Zero Trust principles at iManage touch all aspects of our business, from storage, to networking, servers, software development, and even product management. iManage continues to make a substantial investment in complying with all major security and privacy standards. However, our commitment to Zero Trust goes beyond the currently established standards. (Note: The American National Institute of Standards and Technology has just published a draft *Zero Trust standard: NIST 800-207* announced September 23, 2019). Zero Trust is an evolutionary concept, requiring an ongoing, iterative effort to review and respond to a dynamic security environment.

How iManage Zero Trust Works in Practice

The following infographic provides a practical view of how a typical exploit might take place in a traditional environment, and how Zero Trust stops the attack.

[1] Gilman, Evan & Bart, Doug (2017). *Zero Trust Networks: Building Secure Systems in Untrusted Networks.* Sebastopol, CA. O'Reilly Media, Inc. (Kindle location 139)

© Copyright 2021 iManage

iManage

iManage Cloud Zero Trust

Traditional vs. Zero Trust: Same Story, Two Different Outcomes

SCENARIO 1

Traditional
Security Breach

SCENARIO 2

Zero Trust
Attempted Security Breach

Dan* emails a "video" to Bob**

- Video included a Zero-day executable.
- Zero-day infects Bob's primary device.

Bob views video

- Zero-day infects Bob's device, but the device never has any connectivity to production.

Attack is stopped here.

- Bob uses his machine to administer a server environment.
- His credentials are recorded over several days.

Bob's machine gets infected with malware

- Given the situation above, this is unlikely to happen in a Zero-Trust network. Assume, however, that Bob's machine attempts to request a change that impacts the security of the production network, but the change is denied because a peer rejected the change after review.

Attack is stopped here.

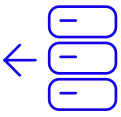
- Many of the servers he connects to have outbound SSL connectivity.
- Malware moves to app server.

Bob connects to cloud app server

- Given the situations above, this is unlikely to happen in a Zero-Trust network. Assume, however, that there is malware on a server on the production network. Even so, it is unable to scan or gain credentials in the environment.

Attack is stopped here.

- The attacker uses shell to scan network, find a server for a vulnerability, and gain access to customer data.

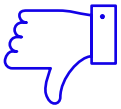


A reverse shell is setup on an app server

- Given the situations above, this is unlikely to happen in a Zero-Trust network. Assume, however, that an attacker has collected data that he wants to send outside. Since no system has internet connectivity, he cannot exfiltrate data.

Attack is stopped here.

- Attacker finds a SFTP server with a well known "ops" ID and uses ID to exfiltrate data.
- **Data breach has occurred.**



Malware on app server connects to malicious file repository

- **Data is Safe.**

* Dan = highly trusted (phished email)
** Bob = system administrator

© Copyright 2021 iManage

BUILDING A ZERO TRUST ARCHITECTURE

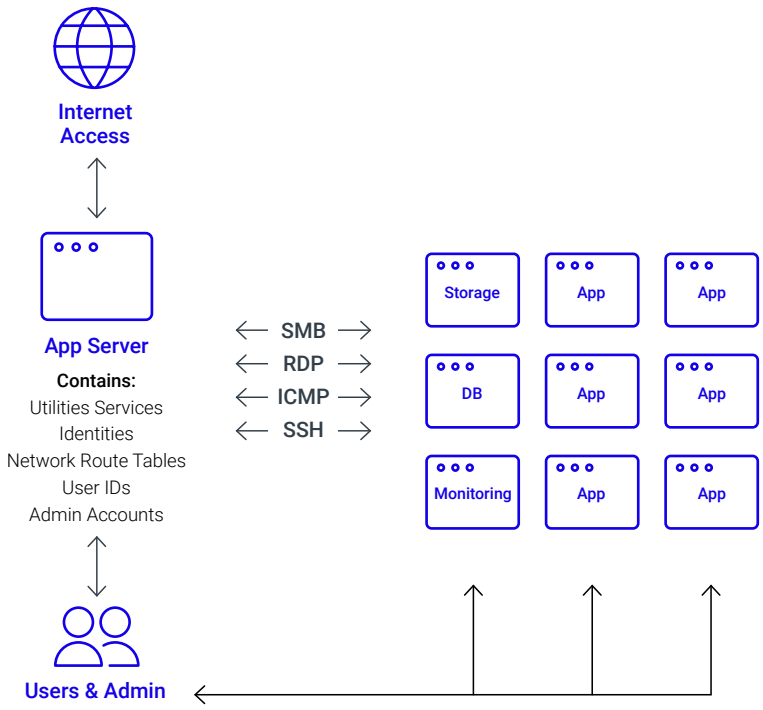
Traditional Environment, Standard Security Model and Zero-Trust Security Model

Building a Zero Trust Architecture

Traditional Environment

In a traditional flat network, defenses are built around the perimeter of a network to prevent attacks from the internet. A small business owner might build such a network because this kind of architecture is easy to manage, is cost-effective, and an organic way to grow a small network.

Figure 1: Traditional Environment



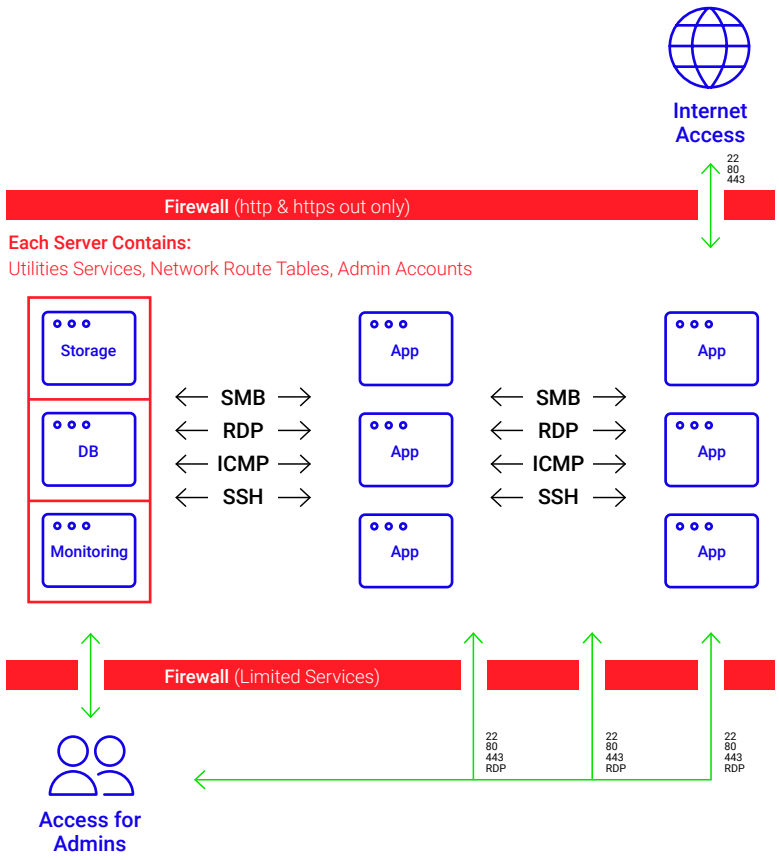
This approach has been largely discarded, because it presents multiple vulnerabilities resulting from built-in trust. For example, a rudimentary network trusts every device within its perimeter (Figure 1). This traditional environment includes servers that have access to each other over many basic protocols — ping, server message block (SMB), remote desktop control (RDP), internet control message protocol (ICMP), or secure shell (SSH) etc. There are also many administrators that have broad access to the bulk of the production systems and many utilities and resources that also have access to the environment. All these characteristics create a vast, unprotected surface of attack.

© Copyright 2021 iManage

Standard Security Model

Unfortunately, even today, most networks are only slightly more secure than the one described above. Let's call these networks standard environments. These are traditional environments where security has been bolted on after the environment was built. Figure 2 is a standard model, which was secured by firewalls and where network access was somewhat restricted. Users don't have direct access to the production network. Access to important resources, such as databases and storage, may be controlled better. Servers are isolated to a large production network.

Figure 2: Traditional Environment Secured



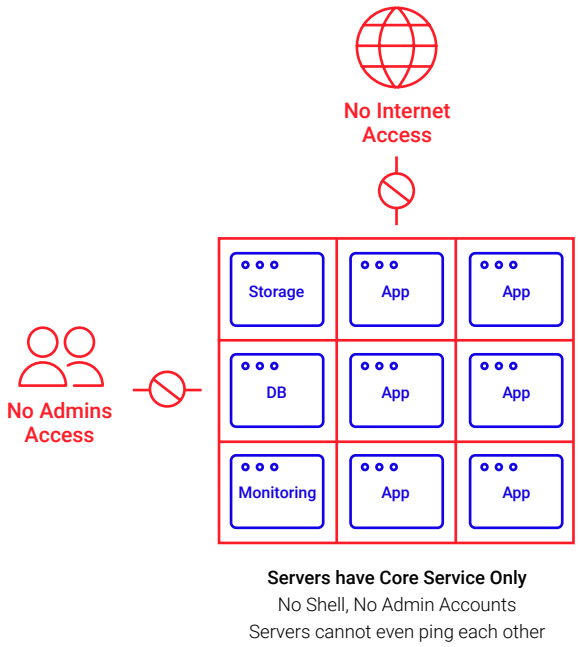
This kind of protection improves security and meets many, if not most, compliance standards. Yet it is still inherently flawed because it relies on trusting human beings, system accounts and network ranges. No matter how strict the monitoring, there is still a zone in the network that is trusted and where the system administrator has privileged access. All systems still have network access to each other. A surprising number of companies and cloud vendors still follow this model.

© Copyright 2021 iManage

Zero Trust Security Model

The growing sophistication of cyber attacks has caused leading security architects to reconsider the very basis of trust. Unlike the two examples above, in a Zero Trust model, no trust of any kind is assumed. Instead, the architecture requires that all connectivity must be explicitly authorized. In this way, a security architecture built on Zero Trust does not present any default paths between servers and the production network, the internet, or users (Figure 3).

Figure 3: Zero Trust Model



As there is no implicit trust, computer hosts have no connection to any other host, even if they are on the same network, part of the same subnet, and assigned to perform the same tasks (see Figure 3). The same is true for the database servers. The network does not have a path to the internet. There is not even a pre-existing network path for any human actors. There's no implied access to any point of the network.

© Copyright 2021 iManage

OTHER CRITICAL ELEMENTS OF iMANAGE ZERO TRUST

Other Critical Elements of iManage Zero Trust

Customer Managed Encryption Keys

Another essential element of the iManage Zero Trust model is encryption. A typical environment is one where the vendor hosts the data securely and provides a base level of encryption at a volume level. iManage offers an additional layer of encryption at the file level. The customer has the option of maintaining the master keys for their data, including the ability to revoke them. In this model the client maintains full control over the data, independent of the vendor.

Zero Touch Updates

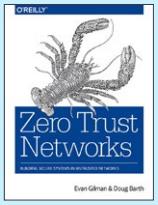
Another layer of protection in a Zero Trust model is the automation of software changes, which minimizes the possibility of human error or interference. A Zero Trust environment should be "touchless," meaning that the human ability to intervene is removed. There should be no human access to any of the infrastructure components; no ability to shell, SSH, or "remote in" into the compute layer. All system components, from digitally signed host images to digitally signed application microservices are fully automated and deployed automatically after quality assurance and staging review.

Can Zero Trust be Added to a Traditional Environment?

It is very difficult to layer Zero Trust concepts onto an existing network. The fundamental features of a Zero Trust implementation require careful planning and automation that do not lend themselves to a traditional flat network. To understand how complex retrofitting is, consider the challenges below, which are just a few among the many known obstacles.

Network Segmentation

When a flat network is built and grows in an organic way, systems and applications are added without tracking data flows, server groups, or network ranges. All systems in this production network sit in a zone of internal trust and free connectivity. Moving to a Zero Trust architecture would require investigating and resolving connections across all servers in the network. In a medium-size environment, this could mean thousands of access reviews. In a Zero Trust environment built from the ground up, connectivity does not exist in the first place, so such network segmentation problems do not exist.



> Rather than being something which is layered on top, considered only after some value has been built, security must be fundamentally infused with the operation of the system itself.
>
> **Evan Gilman & Doug Barth**

© Copyright 2021 iManage

Policies Management

Once the network has been segmented and secured, it becomes necessary to maintain the established network isolation. This involves managing hundreds of very complex policies, which typically requires an automated policy management mechanism. Maintaining a system with thousands of complex policies is not practical or cost-effective and increases the potential for errors.

Encryption

Implementing encryption for all data at rest and in transit for any system requires managing hundreds, if not thousands, of secrets, such as private certificates, database credentials, and application credentials. Managing this in a manual fashion exposes these secrets to human beings and less secure systems. Encrypting, storing, and managing this sensitive data across all these systems would involve thousands of hours of development and configuration time.

iManage Zero Trust

Zero Trust architecture is quickly gaining recognition as the best-of-breed security model for the most technically sophisticated and security-conscious global enterprises. As the landscape of security threats continues to grow and evolve, it is essential for every customer-focused business to adopt the best available security strategies. iManage is unique in our commitment to a Zero Trust architecture and to delivering the most secure platform and products to customers.

For more information about how we support Zero Trust across our platform solutions, go to imanage.com.

About iManage™

iManage is the company dedicated to Making Knowledge Work™. Its intelligent, cloud-enabled, secure knowledge work platform enables organizations to uncover and activate the knowledge that exists inside their business content and communications. Advanced Artificial Intelligence and powerful document and email management create connections across data, systems, and people while leveraging the context of organizational content to fuel deep insights, informed business decisions, and collaboration. Underpinned by best of breed security, sophisticated workflows and governance approaches, iManage has earned its place as the industry standard through continually innovating to solve the most complex professional challenges and enabling better business outcomes for over one million professionals across 65+ countries. Visit www.imanage.com to learn more.

© Copyright 2021 iManage