Security Network Auditing: Can Zero-Trust Be Achieved?

Carl Garrett

Security Network Auditing: Can Zero-Trust Be Achieved?

GIAC (GSNA) Gold Certification

Author: Carl Garrett, cgarrett42@gmail.com
Advisor: *Dr. Johannes Ullrich*

Accepted: *2020-08-09*

Abstract

Since 2010, government and business organizations have begun to adopt the Zero-Trust framework. Although the concept is a decade old, organizations are still in the infant stages of its implementation. Given that tablets and mobile phones have become an intricate part of business aids, all organizations will eventually integrate Zero-Trust into their environments. Many third-party vendors market Zero-Trust tools; though, they only provide one or two pieces to achieve "true" Zero-Trust.

Designing a security auditing Zero-Trust framework, professionals must use a layered approach to defense-in-depth. They must also understand the principle of Least Common Mechanism because complicated information technology systems are challenging to control. In traditional perimeter networks, users must authenticate to an entire organizational network, where perimeter-less Zero-Trust networks are segmented; thus, users can log on a Zero-Trust network by accessing a single-segment at a time. This technology eliminates the need for virtual private networks (VPN), thus, providing faster access.

Additionally, most organizations state they audit their systems. However, this project focuses on auditing Zero-Trust devices, applications, data, and network traffic, not continuous logging. When implementing the Zero-Trust framework, organizations will learn how to plan and audit for adequate security.

1. Introducing Zero-Trusts

Google experienced a security breach by China in 2009; thus, Google overhauled its network the following year. The security incident was detrimental; therefore, Google tasked its engineers to develop a stealthy solution. They called their initiative BeyondCorp and, once fully developed, deployed their engineered solution beginning in 2010 (Osborn et al., 2016). The goal of BeyondCorp was to improve the security posture of the entire company. At about the same time, John Kindervag of Forrester Research coined the term "Zero-Trust." Kindervag studied and created Zero-Trust for similar reasons Google designed BeyondCorp (Moscaritolo, 2011). For both philosophies, security incidents were big problems because adversaries had already breached the internal networks in many organizations. Although Google's BeyondCorp and Kindervag's Zero-Trust formed in the year 2010 timeframe, the term, BeyondCorp, is rarely used. Zero-Trust remains the preferred globally recognized term.

1.1. What is Zero-Trust?

Zero-Trust, simply stated, is a philosophy. It doesn't come from hardware or software, although these components are required to manage the network posture. It instructs security practitioners never to trust, always validate (Gilman & Barth 2017). The Zero-Trust framework has five trust regions: users, devices, applications, data, and network traffic (Bardowell & Lyles, 2020). For Zero-Trust, IT systems do not place inherited trust in any of the five trust regions; though, verification for all five trust regions is a requirement. In other words, the IT systems must verify the device, its state, and the connected user before being allowed access to the network resource (Moscaritolo, 2011). Furthermore, access to one network resource does not mean access will be granted to other resources. For Zero-Trust, all networks, internal and external, are deemed unfriendly.

1.2. Why is Zero-Trust Important?

Zero-Trust is a buzzword and a distinct marketing term. Just-In-Time Verified Trust is a more substantial definition. However, this research will utilize the name Zero-Trust for this study. This technology is, thus, crucial for many reasons. First,

organizations implementing Zero-Trust collapse adversarial attack surfaces. For example, a user logs into an application connected to a data storage server. The user authenticates through an Identity and Access Management (IAM) system and performs work activity then logs out. Upon logout, all IT services to the application and storage server shut down, and the attack surface closes. Even in a hostile network, lateral network traffic ceases, causing the adversary to become frustrated.

Second, the Zero-Trust philosophy is essential when migrating to cloud-based environments. With most organizations, the internal network perimeter has expanded into the cloud; consequently, the security perimeter has disappeared as end-users have become dependent on cloud services like Microsoft O365. The majority of organizations have moved or will move a portion of their IT services to a cloud-based platform by 2021 (Shah, 2018). Therefore, a Zero-Trust implementation is vital for organizations to safeguard their data and applications, especially if they embrace the seven-layered security model with the Zero-Trust framework.

Last, the Zero-Trust framework lays the foundation for a faster, more robust security posture. Zero-Trust can replace traditional VPN access. For example, in a conventional network, a device and user must authenticate to the VPN before they are allowed access to applications and data on enterprise networks. For Zero-Trust, users and devices authenticate to the web apps and data without inheriting any other access rights to other IT resources. This direct access method is faster because the users will not authenticate to inherited services, only the specific IT system.

1.3. Problem with Zero-Trust

Due to its comprehensive approach to IT security, there are several issues with Zero-Trust that organizations must define before implementing the technology. Those issues include different classes of users, devices, applications, and data storage. For users, organizations will have on-site users, remote users, contractors, customers, vendors, and other third-party organizations requiring specific access. Then, organizations will have to look at laptops and tablets for compliance. For most organizations, device control will be challenging as organizations can only control employee's equipment, not external customer equipment.

Applications and data storage can become complicated too. Legacy application revisions are needed to include multi-factor authentication. Plus, changes in data storage authorizations are essential to match least privilege, not inherited permissions given on traditional networks. Absolute Zero-Trust for most organizations isn't achievable due to complex administrative duties; however, most organizations should begin to implement some form of it.

1.4. Achieving Zero-Trust

Achieving Zero-Trust will be different for the various types of organizations. For example, a manufacturing organization will most likely have additional Zero-Trust requirements compared to a banking organization; or, an engineering organization will undoubtedly have different requirements than a financial organization. For established entities, Zero-Trust is more challenging to achieve due to legacy users, applications, hardware servers, and data storage. Hybrid environments, on-premise, combined with cloud-based IT systems, make it even tougher to attain complete Zero-Trust. Unfortunately, no one size approach suits every business and government unit; however, new organizations can immediately embrace the Zero-Trust framework. When planning Zero-Trust, simple open designed IT systems are easier to manage (Saltzer & Schroeder, 1975).

2. Trusting the Zero-Trust Process - Methodology

The testing environment for this research uses a self-built lab with a Microsoft Azure cloud server infrastructure and two local virtual machines. The researcher chose this model for its ease and duplication; though, an on-premise or other cloud solution like Amazon Web Services is adequate as well. To audit a Zero-Trust model for compliance, an understanding of the IT system's five pillars and access control technology is crucial. See Figure 1: Access Control Engine below.

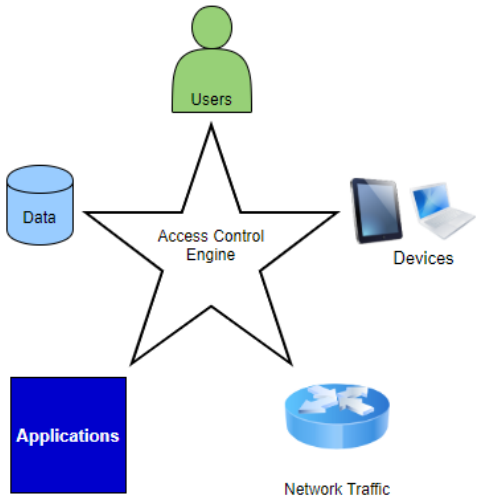

Figure 1: Access Control Engine

For this research, the expectation is to deny all access to all five trust pillars by default; then, allow access as needed. The researcher will also use examples of micro-segmentation to demonstrate a critical foundational principle of the Zero-Trust framework. Micro-segmentation creates logical network segments between controlled traffic from web apps to databases. This technique design is granular and prevents adversarial lateral movement from propagating, especially for web applications. Next, the researcher builds net-flow transports, which allows network traffic only through the needed ports. Then, for testing, the researcher completes several different mock scenarios.

3. Zero-Trust Devices and Users Authentication

For valid Zero-Trust, IT Auditors must verify with IT Administrators that all devices on the Zero-Trust segmentation are recognized and validated. The auditor must also know the processes to prove the devices are valid. There are are two primary device groups: bring your own device (BYOD) and organization devices. Organizations will provision their own devices through active directory; however, for BYOD, an endpoint management solution like Microsoft Enterprise Mobility and Security, MobileIron, or other platforms are necessary. Endpoint management solutions probe the device's hardware features to determine if a device meets the required hardware security

standards. Plus, Zero-Trust requires an endpoint management solution for external customer-facing devices.

User trust in the Zero-Trust security realm is continuously changing. Password-based user authentication is still widely used. However, single password-based authentication does not meet Zero-Trust conditions. Therefore, as a part of a Zero-Trust approach, organizations should make use of more enhanced user authentication practices. Multi-factor authentication is an ideal solution. Plus, for the very best multi-factor authentication, a smart card, USB token, certificates, and biometrics should be used. For most customer-based web applications, username/password and one-time-passcode will be adequate for multi-factor.

3.1. Case Study 1: Device and User Authentication

3.1.1. Test 1: Device Validity

In this simple mock scenario, the researcher created a Microsoft Azure lab with Azure Active Directory and Microsoft Endpoint Management (MEM). Then, the researcher registers the Windows10 virtual machines to Microsoft Intune, which is part of the MEM solution. See Figure 2: Device Enrollment below. In this test, the researcher replicated the registration process to validate the enrolled devices.

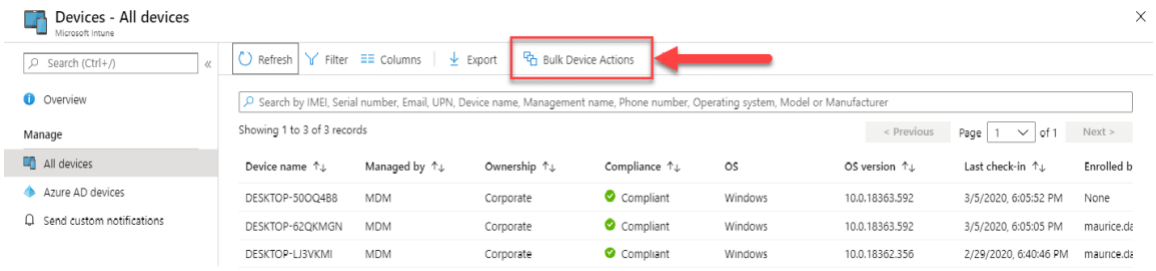

Figure 2: Device Enrollment

3.1.2. Test 2: User Authentication

In this test, the researcher created an Azure Web App, deployed application code, and enabled multi-factor authentication using Azure Active Directory. First, for establishing the Web App, the researcher logged into the Azure portal and created a resource app service called zerotrustlab2. For this to work correctly, a programmer uploads into the Azure cloud the program code. Then, Azure figures out the resources it

needs to run the system code. Therefore, if the web application needs a virtual machine, then Azure deploys one. Then, to implement the web application, the researcher added an external repository source code from GitHub with a file transport protocol (FTP) connection. After that, the researcher performed a validation test with the new URL.

Finally, the researcher enabled multi-factor authentication in Azure Active Directory. Azure Active Directory supports a simple method to create user credentials and controls the levels of access for those users. Then, the researcher configured the user account for multi-factor authentication in Azure Active Directory. To work correctly, a deployed application uses Azure Active Directory to prompt for validation before gaining access to the website. If the app opens after proper multi-factor authentication, Zero-Trust access is validated. See Figure 3: Multi-factor Authentication below.

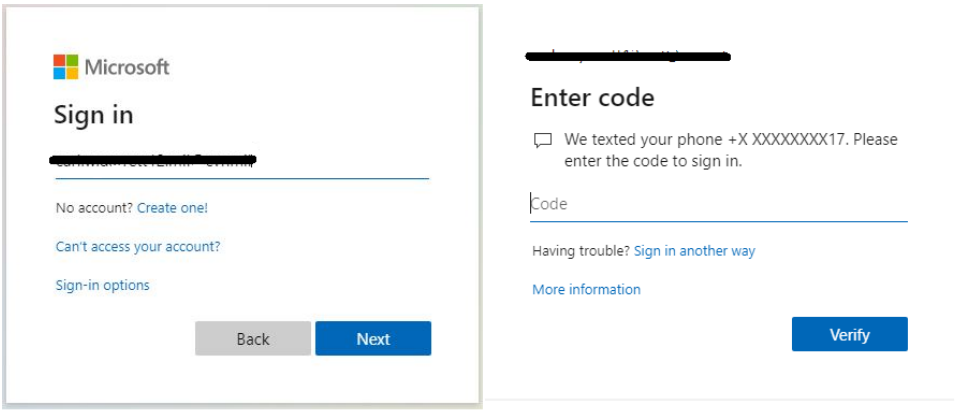

Figure 3: Multi-factor Authentication

3.2. Device/Users Findings and Auditing

In Test 1, it is essential to realize that devices that are allowed access to apps and data must have identities in an access control management system like Microsoft Endpoint Management. Even though this was a simple scenario, without device control, Zero-Trust does not exist. The researcher confirmed unregistered devices could not access the IT system.

For successful IT audits, auditors must confirm there is an adequately configured endpoint management system. Auditors must verify that devices cannot reach IT systems that aren't registered. Plus, devices must also have least privilege. In other words, a laptop

registered on an endpoint management system may have more or less access than a tablet or other IoT device.

In Test 2, the researcher had trouble initially setting up multi-factor authentication, which clarifies that single-factor authentication is the default. However, single-factor authentication credentials do not meet Zero-Trust benchmarks due to widespread credential stealing. After creating the ZeroTrustLab2 web app, a provisioned app in the "All applications" blade of Azure Active Directory appears. Then, the researcher enabled multi-factor authentication on the users and assigned the web app to each user to authenticate.

During testing, the researcher configured four separate user accounts. Two accounts had multi-factor authentication enabled, and two had single-factor authentication. Both types of user accounts were allowed into the web app. The only difference was that a one-time-passcode was texted to the researcher for the multi-factor authentication accounts to complete the logon. Looking into this further, the researcher needed to upgrade Azure Active Directory for the web app to require only multi-factor authentication. After the upgrade of Azure Active Directory, the web app denied single-factor authentication user accounts. See Figure 4: Access Denied below.

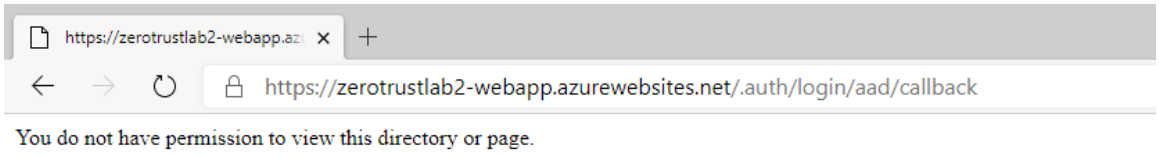

Figure 4: Access Denied

If the researcher is auditing for multi-factor authentication compliance, user accounts must have multi-factor authentication configured, and web apps must require multi-factor authentication. It would have been simpler for the researcher to create groups and assign users; though, this was not available in the free version of Azure Active Directory. Still, the concept of least privilege was prevalent as just enough access was given to the users who required the app.

4. Zero-Trust Application Auditing

For web apps, the compute and application components usually function as a single unit. It's also important to understand that applications are typically interfaces to databases like SQL. Micro-segmented Zero-Trust encompasses an application that writes data to an authorized database via encrypted network net-flows. Putting these components together provides trusted cybersecurity.

4.1. Case Study 2: Web Application Testing

4.1.1. Test 1: Application Segmentation

In Case Study1, Test 2, the researcher took the built web app and provisioned it for multi-factor authentication with Azure Active Directory. Yet, to provision the web app, App Service Authentication must be selected to "On" and set to "Log in with Azure Active Directory." Also, the researcher could have used authentication services from Facebook, Twitter, or Google; however, organizations should not rely on other platforms to authenticate. To lock down the web app to multi-factor authentication and device compliance, the researcher configured conditional access in Azure Active Directory. See Figure 5: Conditional Access below. The researcher then tested for access.

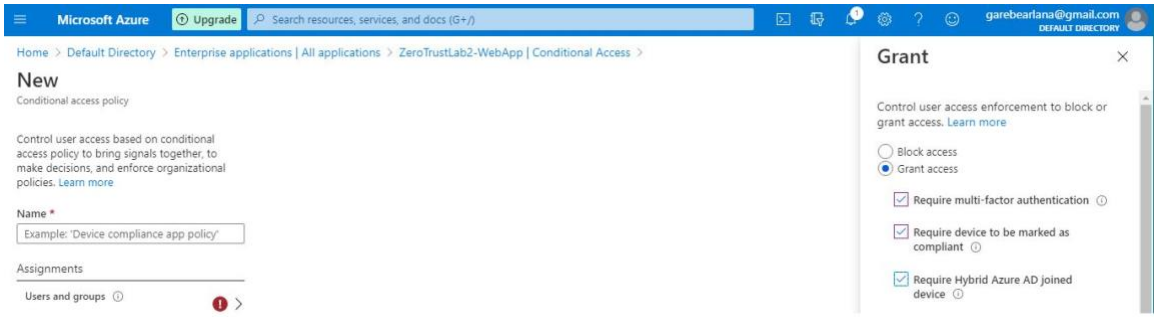

Figure 5: Conditional Access

4.1.2. Test 2: Enabling TLS Between Client and Server

In this test, the researcher configured the IIS web server with https to require client certificates before accepting web app access. This technology worked when the web app refused a connection when the client did not get issued certificates. On the other hand, the web app granted access to the client that received certificates.

4.2. Application Findings and Auditing

For Case Study 2, the researcher confirmed that proper conditional access on the web app using least privilege are keys to successful Zero-Trust compliance. Furthermore, the researcher tested connectivity with a certificate and achieved positive results. If the user was issued a certificate, the web app opens. Without a certificate, the web app denies access. The researcher also confirmed that legacy web apps would be a concern without authentication and certificates. An external IT Auditor should not have access to an organization's network and surf to an open web app without authentication and certificates. If the website opens, the micro-segment is not Zero-Trust compliant. Many organizations will depend on third-party apps to grant access to legacy web apps to bridge the gap until they can micro-segment all their IT systems. However, third-party apps complicate organizations due to added IT administrative responsibilities.

Checking for compliance, an external IT auditor must get a listing of all web applications and attempt to login. If the auditor can get into any web apps without credentials, the auditor must determine security risk. Auditors must evaluate customer-facing web apps as to the procedures to enroll and verify authenticity. Also, auditors must verify certificates issued to users with proper credentials for privileged access. If the web app writes data to a database, the auditor must evaluate that users and devices authenticate using multi-factor. Auditors must access internal web apps too. For all internal web apps with sensitive records, the organizational policy should require multi-factor authentication. Then, since third-party identity and access management applications involve complex configurations, IT Auditors should verify authentication with legacy web apps.

5. Zero-Trust Data Storage and Network Auditing

The researcher kept data storage and networking together for the case study because they correlate and are keys to effective Zero-Trust compliance. For data storage, IT systems must be able to encrypt data-at-rest, and, for networking, IT systems should encrypt data-in-motion. Micro-segmenting data-at-rest and data-in-motion require programmers to write code with data validation using reliable net-flows. The only way to

check for Zero-Trust compliance is to label data, such as sensitive, classified, or unclassified, and know where and how the data travels on the network.

5.1. Case Study 3: Storage Data and Network Flows

5.1.1. Test 1: Disk Encryption

For Test 1, the researcher took the Window Server 2016 virtual machine and added storage to the disk volume. The researcher created an Azure key vault and implemented encryption to the virtual disk. For confirmation, the researcher logged into the Windows 2016 server, navigated the disk volume, and verified encryption on the storage drive.

5.1.2. Test 2: SQL Data Encryption

In Test 2, the researcher configured an Azure SQL database and used the existing 2016 Windows Server with SQL Server Management Studio. Using Azure's deterministic encryption, the researcher configured the sample database. From SQL Server Management Studio, the researcher logged into the test sample to set the database with "Enable Always" encrypted. Personally identifiable information (PII) data then filled the database tables with phone numbers, email addresses, and password hashes. Then, the researcher encrypted only the phone numbers on the sample database. To verify data encryption, the researcher attempted to access the data from a query search.

5.1.3. Test 3: Data-In-Motion Encryption

Using Azure storage, the researcher used a JPEG image that is only available through secure TLS 1.2 encryption. The researcher experimented with network traffic flows and access by developing an encrypted network highway between the web app and storage vault. This network highway was a bi-directional path; and, it did not have access or other exits along the route. For this to work correctly, the researcher required traffic flow through https only. Then, only the web app had access to the JPEG files by building a shared access signature, which granted access only to the storage vault from the web app itself. A successful rendered web app confirmed micro-segmentation, and data encryption operated as it should.

5.2. Data Storage/Network Findings and Auditing

For the provisioned 2016 Windows Server virtual machine, the researcher confirmed that Azure created drive encryption during the initial setup. However, by adding additional storage capacity at a later time, IT Admins must configure the new storage volume for encryption because it is not enabled by default. This situation can leave organizations vulnerable. Auditors must confirm with top leadership whether or not formatted disk volumes have stout encryption. See Figure 6: Disk Encryption below.

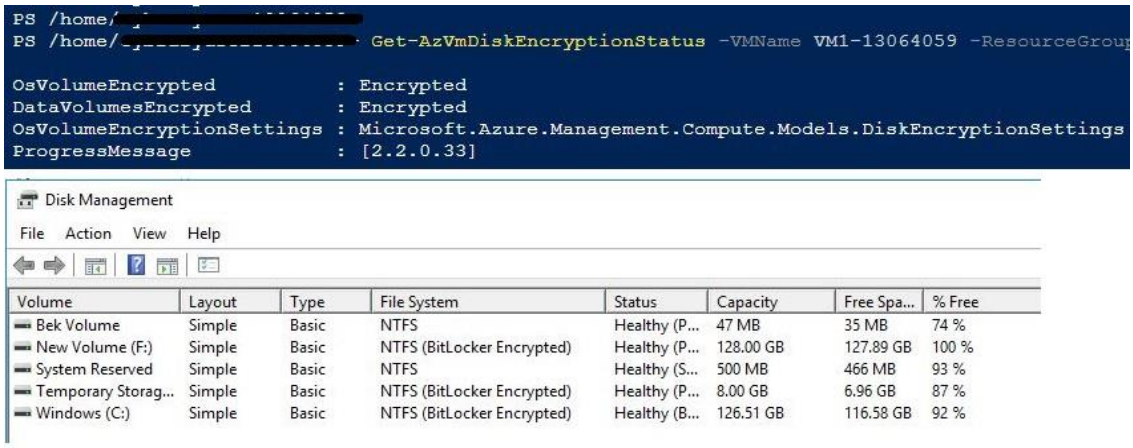

Figure 6: Disk Encryption

For Test 2, the researcher validated the deterministic encryption method in the Azure portal for SQL data. This encryption technique is faster than most encryption algorithms; though, most encryption standards are applicable. IT auditors must also validate encryption on the data itself, especially personally identifiable information (PII) data. The researcher configured encryption on the phone number table and confirmed it works. See Figure 7: Encrypted Data below. All PII should be encrypted. IT auditors must look at all PII in databases and determine access vulnerabilities.

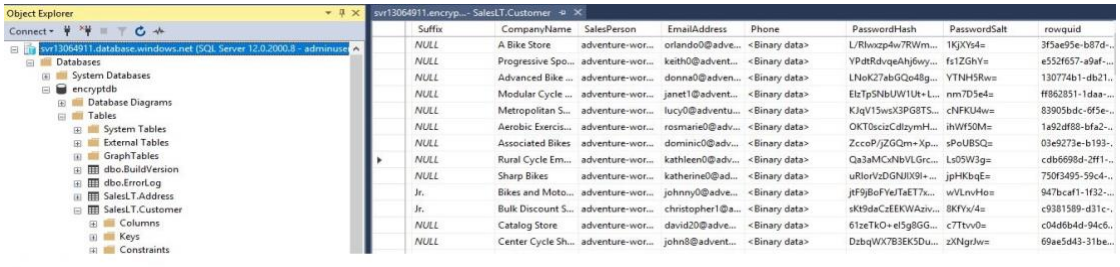

Figure 7: Encrypted Data

For Test 3, the researcher confirmed data-in-motion from the storage vault to the web app using secure https. See Figure 8: Enabled TLS 1.2 below. The researcher

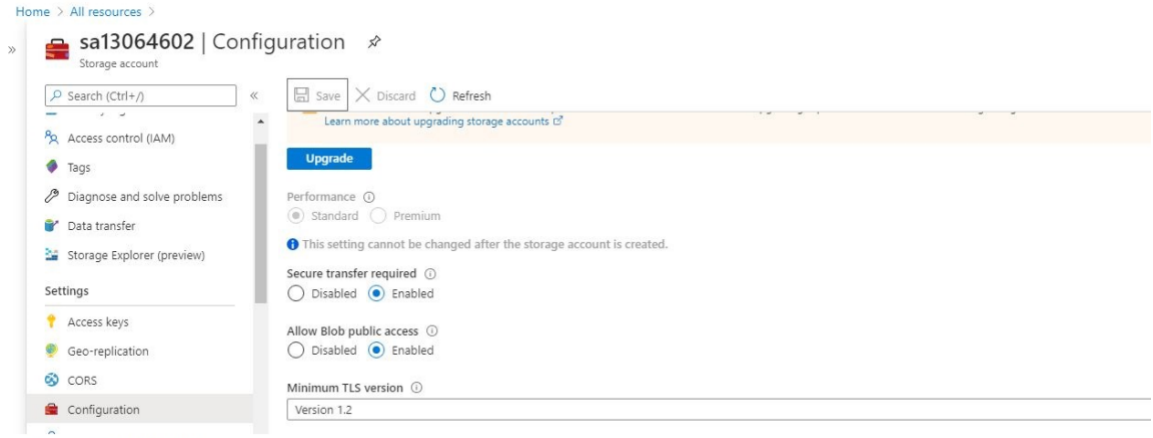

Figure 8: Enabled TLS 1.2

also verified the shared access signature connector, which grants access only from the storage vault to the web app. For this test to be a successful audit, the auditor must verify TLS 1.2 encryption for network traffic flows. Plus, the auditor must confirm that unsecured accounts cannot open web apps. See Figure 9: Unsecured Account below.

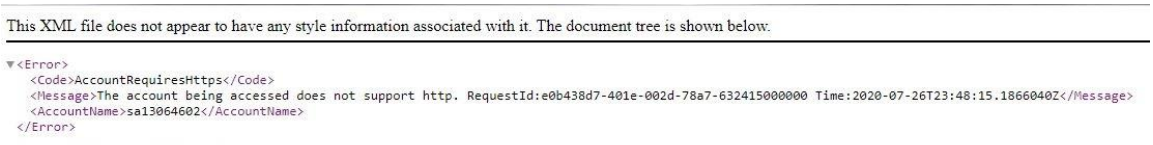

Figure 9: Unsecured Account

6. Designing Zero-Trust

Proper design of Zero-Trust IT systems is no small task; however, security processes should not make the IT resource more challenging to access (Saltzer & Schroeder, 1975). The researcher sat through a demo of an identity access management platform from a third-party provider. The sales engineer demonstrated how one could take all your different IT systems in all the various platforms and bundle them in one location on their software platform. The software platform bundle advertises itself as a Zero-Trust privilege access management system. Though a great product, the additional security connectors add new challenges by adding complex layers to the organization's IT systems.

Based on these case studies, organizations can simplify all their system if they do the following. First, all organizations should have device standards, including ones for mobile tablets and phones. Second, organizations should choose just one platform like Microsoft Azure, Google, AWS, or on-premise IT systems. Too many IT platforms increase complications. Third, micro-segment all networking, databases, and web applications into trusted segments. Last, encrypt all data-at-rest and data-in-motion. IT auditors must understand these conditions to simplify organizational systems.

6.1. Mature Versus New Organizations

Existing technology, along with different organizational requirements, determine the Zero-Trust implementation plan. Established networks have more traditional IT systems, with a perimeter firewall around the organization. For these networks, external devices and network traffic are untrusted while internal network traffic is trusted. On the other hand, Zero-Trust systems do not have perimeters. They are micro-segmented. Due to backing out of existing technology, mature organizations will find Zero-Trust implementation challenging. However, if an organization is new, it should pursue Zero-Trust architecture from the beginning.

6.1.1. Part 1: Designing for Micro-segmentation

When constructing Zero-Trust, large and small organizations should plan for future IT operations. Zero-Trust designing does not start with next-generation firewalls or identity access management third-party systems. Zero-Trust starts with micro-segmentation first. See Figure 10: Micro-segment below.

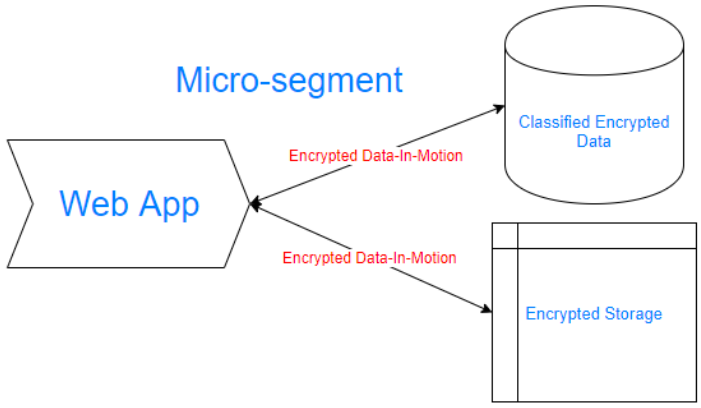

Figure 10: Micro-segment

For example, Mario is a project manager for Foam, Inc. that has adopted Zero-Trust architecture. The finance department would like Mario's team to develop a web app to track credit terms for all their business to business (B2B) customers based on an algorithm with the following conditions:

- How many years has the customer conducted business with Foam, Inc?
- What amount of sales dollars per year does the customer do with Foam, Inc?
- What is the amount of Foam, Inc. accounts receivables from the customer?

Also, within the web app, the finance department will view B2B contacts, phone numbers, email addresses, B2B customer birthdays, plus many files.

For Mario to be successful, he must first provision an encrypted database and file storage. At the same time, the developer designs the application according to the needs of the finance department. Mario then works with an IT admin to configure the web app to communicate with the database and file storage. Last, Mario establishes a virtual network and provisions networking on a cloud-based or on-premise platform using TLS 1.2 encryption. This sequence of events creates a micro-segmentation for this web app.

All organizations can have successful micro-segment implementations if they create plans and maintain control of their web apps. Azure, Google, and AWS cloud providers publish Zero-Trust architecture plan designs to follow. Furthermore, IT auditors should examine every micro-segment for data protection. Organizational data is the most critical element to safeguard. Application and Network layers should act as a protection mechanism to structural data. See Figure 11: Protection below.

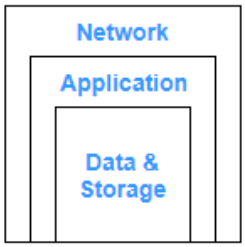

Figure 11: Protection

6.1.2. Part 2: Designing Identity Access

Identity and Access Management (IAM) is the other component of Zero-Trust architecture. The role of IAM is to grant access to web apps based on predefined privileges. Most users and devices are external customers; however, many web apps programmed today are for internal organizational users. For IAM systems to work, one must configure the access management engine. The engine processes the request to allow authenticated users and devices through the gateway to the micro-segments. See Figure 12: Identity & Access below.

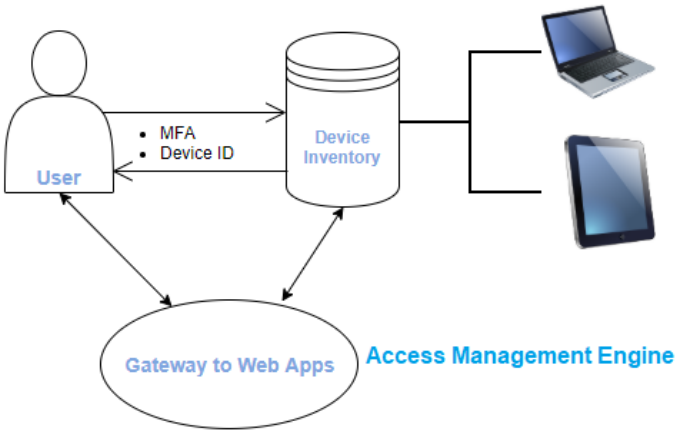

Figure 12: Identity & Access

Although this sketch is a basic prototype, most IAM systems function similarly to this architectural design. When configuring an IAM, use these conditions:

- Enable multi-factor authentication
- Enable single sign-on
- Migrate devices and users to one database and centralize
- If using mobile devices, use cloud-based identity management
- Enable self-services like registering devices and password resets
- Assign access to authorized web apps according to least privilege best practices
- Lockdown internal identities based on standard devices

For IT auditors, assessing is simple! Auditors should evaluate for best practices based on the above conditions. When configured correctly, IAM adds layers of protection of our most valuable assets, data, and storage. See Figure 13: Layered Protection below.

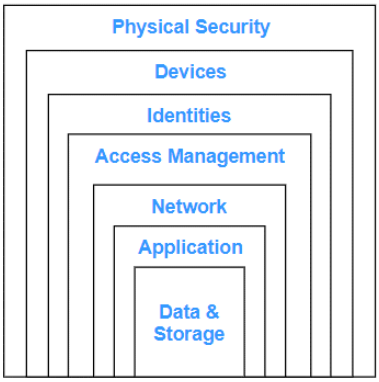

Figure 13: Layered Protection

6.2. The Finished Product

Zero-Trust Architecture has only two high-level components: the micro-segment and the IAM system. When these two-components work in harmony, IT security is more robust without the use of third-party devices like dedicated web-access firewalls and virtual private networks. Additionally, this research focuses on IT security auditing. Understanding the Zero-Trust design with layered protection is the difference between good and great IT auditors. For robust security, users and devices authenticate with the access management engine, opening the gateway to micro-segmentation web applications.

7. Migrating to Zero-Trust

When migrating from a traditional network to a Zero-Trust system, the essential item for organizations to consider is the platform. There are many different cloud vendors to consider, including an on-premise solution. Creating a plan on a single platform is essential when migrating. The blueprint will look different based on the organization's needs. For example, XYZ Widget Factory, with fifty locations and thirty-five thousand workers world-wide, will have unique migration plans versus an engineering company with one locale and thirty-five employees.

All organizations, regardless of size, should micro-segment all future developed web applications. Large organizations should migrate smaller groups of legacy web apps into micro-segmentation. Then, use rolling deployments to implement them. Small organizations should consider one major implementation after the legacy web apps have been micro-segmented. Next, all organizations should employ an IAM solution, apply the micro-segmented connector to the web apps, and migrate to it. Whether large or small, organizations can complete this task quickly. Last, organizations should monitor Zero-Trust technology for data exfiltration.

For Zero-Trust, other items must take place during the migration journey. Organizations must educate and train their user population. Since the Covid-19 pandemic, only thirty-eight percent of the workforce go to their workplace every day (Bekker, 2020). Therefore, workers have overused virtual private networks (VPN) and virtual desktop interfaces (VDI) from remote locations. Zero-Trust Architecture solves these issues by eliminating the need for those technologies. Finally, when considering a platform like Azure or an on-premise solution, determine future operations and best value. Nearly all organizations have some form of cloud-based applications due to the rising numbers of tablets and mobile phones used for business. Plus, cloud-based platforms like Azure make it simple to transfer web-based applications. Cloud computing migration is more straightforward to quickly provision servers, data storage, and web hosting.

8. Assessing and Auditing Zero-Trust

Once an organization begins to migrate to Zero-Trust, IT security, IT admins, and IT auditors should review proper Zero-Trust guidelines. Since auditing is the process of reviewing and verifying the operation, assessing should also take place to identify the Zero-Trust weaknesses. Once Zero-Trust vulnerabilities are identified, remediate immediately.

8.1. Zero-Trust Auditing List

When auditing for Zero-Trust, different organizations will have various solutions based on the type of hardware, software, and other IT services. Internal IT auditors must understand the types of IT systems in their organization to build an auditing checklist; however, external auditors will develop a generic list before proceeding with an audit. In either case, when creating a list, use the philosophy of the seven-layer protection model. Physical security, devices, and identities can gain access to micro-segmented networks, applications, and data only through an access management system. See Figure 13: Layered Protection above.

Below is a list of everyday items to check for Zero-Trust compliance. This list is by no means complete; still, it acts as a starting point for auditors.

Zero Trust Auditing	Checklist
Physical Security	1. Is your physical equipment locked with double security, i.e., door, fence, cabinet, etc.? 2. Do IoT devices have "Find My Device" applied?
Devices	1. Is an endpoint management system deployed? 2. Are device standards configured for all endpoints, tablets, and mobile devices? 3. Are limits placed on the number of devices users or customers can register? 4. Do organizations provision their own devices? 5. Can registered devices can reach IT systems? 6. Do registered devices have least privilege? 7. Can unregistered devices reach IT systems? 8. Are all devices encrypted and passcode protected?
Users	1. Is multi-factor authentication enabled for all users? 2. For larger organizations, are groups formed for administrative ease? 3. Are users allowed access to services and applications they don't need? 4. Is privilege access configured?
Applications	1. Are all web apps micro-segmented? 2. Do all web apps require multi-factor authentication? 3. Is single-sign-on implemented? 4. Do all customer-facing web apps require enrollment and registration? 5. Is a third-party IAM solution used?

	6. Are applications listed in your Identity and Access Management (IAM) system like Azure Active Directory?
Data and Networking	1. Is all data-at-rest encrypted? 2. Is all data-in-motion encrypted? 3. Have all dataflows been identified and tunneled from the web app to the database? 4. Have personal and business data been segmented?
Interview Sample	1. Are IT policies updated? 2. Do users understand AUP? 3. Do organizational managers understand the dangers of excess privilege access for their direct reports? 4. Do developers/programmers write secure code? 5. Do database admins understand dataflows?

8.2. Policies, Processes, and Procedures

When auditing, auditors should look at the current policies, processes, and procedures to determine if they comply with the Zero-Trust framework. All users should sign an acceptable use policy (AUP) and should understand it. Furthermore, users should understand what is not appropriate and know the consequences if violations occur. IT admins must develop procedures for business managers in determining access for their direct reports.

For developers and database admins, an understanding of the Zero-Trust process is essential for developing web apps. No longer can developers rely on IT security for implementing layered trust. Developers and database admins must understand dataflows and validation input. These processes are essential for achieving micro-segmentation. Moreover, organizations should require peer code review to verify it meets the Zero-Trust framework.

When auditing, auditors should interview a sample of end-users, database admins, and developers. If the interviewees don't understand the policies, processes, and procedures, users will figure out ways to circumvent security standards instead of using proper methods to request privileged access. Auditors should never underestimate the value of internal interviews.

9. Conclusion

Many organizations believe they operate using Zero-Trust principles. However, organizations that have bought into the concept of Zero-Trust are performing some functions of Zero-Trust. Most organizations cannot perform all tasks of Zero-Trust yet, as each organization is different and must devise its specific Zero-Trust benchmarks.

For an ultimately successful Zero-Trust organization, all networks will be segmented, all data will be categorized and protected, all devices isolated and authenticated, and all identities will have implemented the principle of least privilege. Still, due to the high level of granularity for Zero-Trust implementations, the study revealed many ways the Zero-Trust operations will fail. Organizations immediately lose device controls when they allow BYOD. Accessing the same data from different applications violates the Zero-Trust micro-segmented framework. Other Zero-Trust failures include open, unencrypted data, excess privilege access, and unknown dataflows. Furthermore, organizational IT staffing will carry heavy workloads converting legacy web applications to meet Zero-Trust requirements. Securing an organization's IT systems using this philosophy isn't easy; however, it is necessary due to the number of devices and users working remotely.

The Zero-Trust framework can be exasperatingly complicated, especially for established organizations. IT auditors will have their work cut out for them for many years to come due to organizations implementing this philosophy. Auditors will spend more time identifying the gaps in Zero-Trust than actually auditing for Zero-Trust compliance. However, the most critical object in auditing is how to guard organizational data. Even though Zero-Trust is more complicated, it's worth the investment.

References

Bardowell, M., & Lyles, M. (2020). Zero Trust Networks Study Guide. Retrieved July 13, 2020, from https://assets.ctfassets.net/kvf8rpi09wgk/6pX3i1UavAuqkz7FlZFirV/d9b0861878a1d2bae3c610acc9e2829d/Zero_Trust_Networks_Study_Guide__1_.pdf

Bekker, G. (2020, April 13). A Practical Approach to Replacing VPNs with Zero Trust Access. Retrieved August 01, 2020, from https://blog.banyansecurity.io/blog/a-practical-approach-to-replacing-vpns-with-zero-trust-access

Gilman, E., & Barth, D. (2017). *Zero trust networks: Building secure systems in untrusted networks*. Sebastopol, CA: O'Reilly Media.

McKay, P. (2020, March 02). How to find the right zero trust strategy. Retrieved June 24, 2020, from https://www.computerweekly.com/feature/How-to-find-the-right-zero-trust-strategy

Moscaritolo, A. (2011, June 01). Eliminating trust: The zero-trust model. Retrieved June 28, 2020, from https://www.scmagazine.com/home/security-news/features/eliminating-trust-the-zero-trust-model/

Osborn, B., McWilliams, J., Beyer, B., & Saltonstall, M. (2016, March). BeyondCorp Design to Deployment at Google SECURITY. Retrieved July 1, 2020, from https://research.google.com/pubs/archive/44860.pdf

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (Special Publication ed., 800-207, pp. 1-58) (United States, U.S. Department of Commerce, National Institute of Standards and Technology). Gaithersburg, MD: NIST.

Saltzer, J., & Schroeder, M. (1975, April 17). The Protection of Information in Computer Systems. Retrieved June 4, 2020, from https://www.cs.virginia.edu/~evans/cs551/saltzer/

Shah, T. (2018, December 13). How Zero Trust Organizations Secure the Cloud. Retrieved July 14, 2020, from https://www.secureworldexpo.com/industry-news/zero-trust-orgs-secure-cloud

Teitler, K. (2019, January 11). What Auditors Must Know About Zero Trust Networking. Retrieved June 11, 2020, from https://internalaudit360.com/what-internal-auditors-must-know-about-zero-trust-networking/

Last Updated: October 26th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Sydney 2020	**Sydney, AU**	**Nov 02, 2020 - Nov 14, 2020**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**Nov 09, 2020 - Nov 14, 2020**	**Live Event**
APAC ICS Summit & Training 2020	**Singapore, SG**	**Nov 13, 2020 - Nov 28, 2020**	**Live Event**
SANS Community CTF	**,**	**Nov 19, 2020 - Nov 20, 2020**	**Self Paced**
SANS Local: Oslo November 2020	**Oslo, NO**	**Nov 23, 2020 - Nov 28, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**