ISSN: 2754-6683

Journal of Marketing & Supply Chain Management

SCIENTIFIC Research and Community

Review Article

Open Access

Why should Firms Especially smaller Firms Focus on IAM (Identity & Access Management), Zero Trust Instead of Investing in Wide Array of Complex Tools and Security Solutions

Pranith Shetty

Information Security & Risk Lead, Cisco, New Jersey, USA

ABSTRACT

Every firm big or small, regardless of the industry, operating capital, size, geographical coverage, aims at improving its cybersecurity and risk posture. These firms build on that strategy by investing in cybersecurity defense tools and processes. The cybersecurity defense industry is filled with various companies providing security tools that span across the information security domains like access management, physical controls, encryption etc. The choices are endless and it is challenging to decide especially if you are a smaller firm with limited budget to spend. Bigger firms can explore choices and eventually go ahead with a tool and implementation model , can revert back changes if they don't like the results, however, that's not the case for smaller firms, the choice has to be rational, beneficial in the long run and not expensive. Of all the information security domains, Access management is the most important domain and the one to secure first for any firm, it offers defense in depth.

This articles dives into details about concepts like Access management, difference between Access management and Access control, Identity and access management, Zero trust which is an advanced and matured framework on similar lines. It also explains why it makes sense for smaller companies with limited budget to opt for these choices, rationale, benefits.

***Corresponding author**

Pranith Shetty, Information Security & Risk Lead, Cisco, New Jersey, USA.

Received: December 08, 2023; **Accepted:** December 15, 2023; **Published:** December 22, 2023

Keywords: Identity & Access Management, Information Security, Cybersecurity, Zero trust, Access Management, Access Control, Risk management

Introduction

Cybersecurity landscape keeps on evolving continuously, especially when there is a significant shift in the form of pandemic [1]. This gave rise to a new form of work culture with employees working from home, thus resulting in an increase in attack surface. The endpoints now no longer reside in offices but also extend to home networks, personal devices, cellphones etc. There has also been a steady rise in the adoption of third-party vendors to gain competitive edge in the market, save time and resources. May be the firms are pivoting a strategy, there could be varied reasons.

With the increase in the attack surface, there could be wide variety of cyber threats that could include Malware, APTs (Advanced Persistent Threats), Social engineering attacks such as phishing scams, Ransomware attacks, Zero-day vulnerabilities and other such attacks.

Rationale for Study

To tackle with these challenges and the threat landscape, firms have a wide array of tools and techniques to choose from. The decision to opt for a certain tool or technique is very challenging, Since it's not just the selection that the firm needs to be mindful of, but the cascading list of steps that follow in the form of current state assessments, target state, implementation, maintenance and service costs, and if the tool is based on a subscription model that is an additional cost to consider and hits the cost center wallet. The adoption of a certain tool or process can get expensive really quick. This is just one tool put into perspective, if the firms are opting for several tools from different firms, the cost is only going to increase and multiply. With tools and processes leveraged from different companies, firms might have to think about complexity and compatibility.

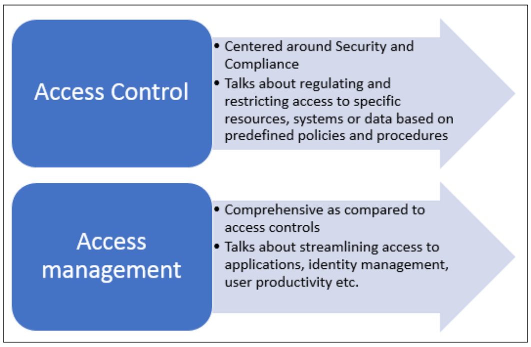
The adoption of an IAM and Zero trust process provides a very strong basic set of controls that smaller firms can digest in terms of spend. It provides a stable operating environment, prior to firms expanding and branching out. Even if the org grows in size or for bigger firms looking into zero trust and IAM techniques are very much worth it in case the spend is not in place for an innovative concept like the SSE or suites. Banking on Zero trust-based approach is going to be palatable especially for smaller firms in terms of budget spend, looking to expand later.

Access Control vs Access Management and IAM

It's important to understand key terminologies involved in this process starting with Access controls vs management, Identity and access management.

Access control and Access management are very crucial components or concepts that can and should be leveraged by firms to safe guard their systems and data [2]. Both of these terms are sometimes used interchangeably and they play unique roles within your security architecture. For example: In a company's network, an access control policy would be more about restricting access to confidential data, entry denied to staff attempting to access.

Access management may involve a proper onboarding of staff involving creation of accounts, operational processes around modification of roles and an offboarding process around disabling accounts.



Access Control

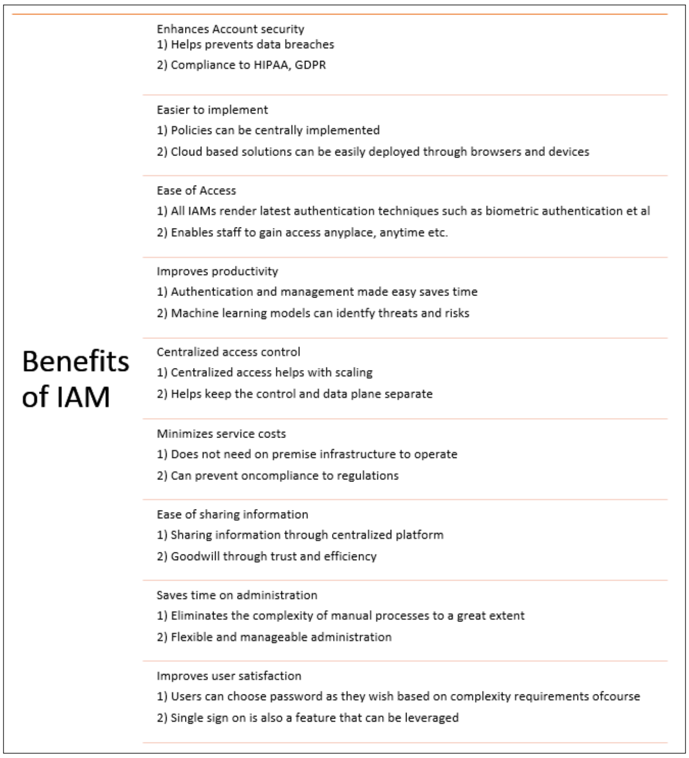
- Centered around Security and Compliance
- Talks about regulating and restricting access to specific resources, systems or data based on predefined policies and procedures

Access management

- Comprehensive as compared to access controls
- Talks about streamlining access to applications, identity management, user productivity etc.

Figure 1: Access Control vs Access Management

Identity and Access management is a fundamental and critical cybersecurity capability, Identity and Access management is a domain in cybersecurity that helps an organization with roles, access controls, rights, privileges etc. [3, 4]. This adds a defense of depth component to the existing network infrastructure. There are many IAM tools in the industry that can be leveraged for this domain and secure the environment.



Benefits of IAM

Enhances Account security
1) Helps prevents data breaches
2) Compliance to HIPAA, GDPR

Easier to implement
1) Policies can be centrally implemented
2) Cloud based solutions can be easily deployed through browsers and devices

Ease of Access
1) All IAMs render latest authentication techniques such as biometric authentication et al
2) Enables staff to gain access anyplace, anytime etc.

Improves productivity
1) Authentication and management made easy saves time
2) Machine learning models can identfy threats and risks

Centralized access control
1) Centralized access helps with scaling
2) Helps keep the control and data plane separate

Minimizes service costs
1) Does not need on premise infrastructure to operate
2) Can prevent oncompliance to regulations

Ease of sharing information
1) Sharing information through centralized platform
2) Goodwill through trust and efficiency

Saves time on administration
1) Eliminates the complexity of manual processes to a great extent
2) Flexible and manageable administration

Improves user satisfaction
1) Users can choose password as they wish based on complexity requirements ofcourse
2) Single sign on is also a feature that can be leveraged

Figure 2

Zero Trust

The core principle of Zero trust is "Never trust; Always verify", it basically means never assume trust, begin the process of trust in users and devices through continuous monitoring of each access attempt with custom security policies that protect every application [5].

Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per request access decisions in information systems and services in face of network viewed as compromised [6]. The goal is to prevent unauthorized access to data and services coupled with making access control requirement as granular as possible. It works on a basic premise that no user or device is to be implicitly trusted. It assumes that a breach has already occurred or will occur and user should not be granted access based on a single verification at the enterprise perimeter but instead the user, device should be continually verified. Zero trust shifts from a location centric model to an identity, context and data centric approach with fine grained security controls between users, systems, applications, data and assets that change over time.

Initial implementation of zero trust might seem expensive but it will enable a cost saving strategy that will pay firms in the near future, not considering the benefits that this approach offers. There is a maturity model with respect to Zero trust, as described below firms based on their strategy can step into various phases and try to mature it over the years, based on how they see fit [6].

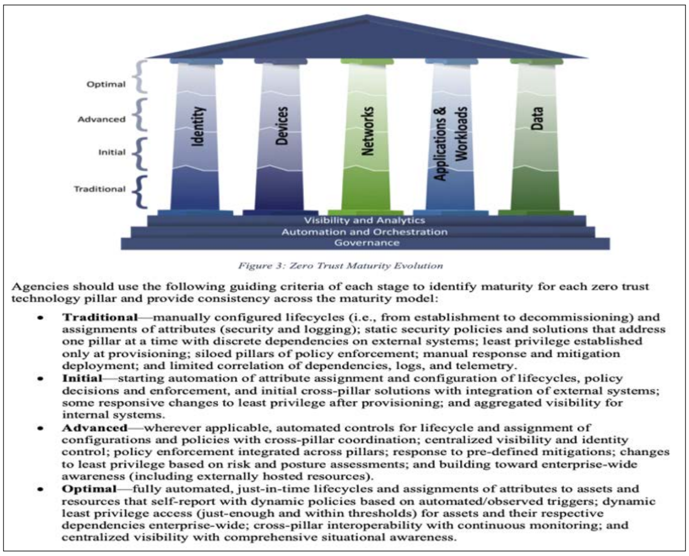

Optimal
Advanced
Initial
Traditional
Identity
Devices
Networks
Applications & Workloads
Data
Visibility and Analytics
Automation and Orchestration
Governance

Figure 3: Zero Trust Maturity Evolution

Agencies should use the following guiding criteria of each stage to identify maturity for each zero trust technology pillar and provide consistency across the maturity model:

- **Traditional**—manually configured lifecycles (i.e., from establishment to decommissioning) and assignments of attributes (security and logging); static security policies and solutions that address one pillar at a time with discrete dependencies on external systems; least privilege established only at provisioning; siloed pillars of policy enforcement; manual response and mitigation deployment; and limited correlation of dependencies, logs, and telemetry.
- **Initial**—starting automation of attribute assignment and configuration of lifecycles, policy decisions and enforcement, and initial cross-pillar solutions with integration of external systems; some responsive changes to least privilege after provisioning; and aggregated visibility for internal systems.
- **Advanced**—wherever applicable, automated controls for lifecycle and assignment of configurations and policies with cross-pillar coordination; centralized visibility and identity control; policy enforcement integrated across pillars; response to pre-defined mitigations; changes to least privilege based on risk and posture assessments; and building toward enterprise-wide awareness (including externally hosted resources).
- **Optimal**—fully automated, just-in-time lifecycles and assignments of attributes to assets and resources that self-report with dynamic policies based on automated/observed triggers; dynamic least privilege access (just-enough and within thresholds) for assets and their respective dependencies enterprise-wide; cross-pillar interoperability with continuous monitoring; and centralized visibility with comprehensive situational awareness.

Figure 3

Method

Let's dive a little bit into Zero trust access for user and device access to applications, basically taking care of endpoints regardless of where they are operating from [5].

1) Establish user Trust

Leverage phishing resistant MFS (Multifactor authentication) regardless of Staff or contractors, staff should have an MFA application installed either on their cell phone or portable device which should be provided by the organization.

2) Verify Device Trust

Apply device posture checks through something similar to a trusted endpoint policy

3) Enable Access to Applications.

Shrink the attack surface through organization's SSO to get to applications, more secure applications through a concept called

ZTNA (Zero trust network access) [7].

4) Enforce Contextual Access

Risk based authentication through location, time, device behavior etc.

5) Verify Trust Continuously

Continuously monitor access through WIFI profile, session timeouts etc.

The product used here was Duo which is a Cisco product and there are several use cases with implementation performed across different firms, most of them are smaller firms who don't have the budget spend to use other tools or broader portfolio of programs etc. This concept of Zero trust access provides them with the security that they need and reduce their overall risk posture.

There are a few other products that are very similar and offer similar functionality those could be used as well and if Zero trust gets a little expensive , firms can resort to IAM solutions that are comparatively cheaper than Zero trust products. IAM solutions won't offer risk posture profiles, contextual verification based on location etc. however they will provide basic protection using the tenets of access control and access management. These solutions also fit better in the context of having a smaller staff and operating locally as opposed to a multinational firm spread out across nations.

Conclusion

IT Security is very much about investing to prevent damage, there is no single magic tool that can solve all of cybersecurity concerns for any firm, however, identity and access management solutions, more so concepts like Zero trust can help take care of the basic security provisions and is an excellent part of the overall package, if the organizations are willing to spend extra and get more tooling and techniques that's on their liberty to access budget spend [8]. Purely investing in IAM and Zero trust solutions is a highly profitable investment with returns both in saving costs and from data breaches. It can reduce the overall operational spend especially for smaller firms who operate on a tighter budget and are at the mercy of investors for their fiscal needs. These firms need solutions and tools that save them time, effort, money and resource spend [9-11].

References

1. Chipeta C (2022) What is the Cyber Threat Landscape?. UpGuard, www.upguard.com Available: https://www.upguard.com/blog/cyber-threat-landscape.
2. Rohit Rao (2023) Access Control vs Access Management: An In-Depth Comparison. www.zluri.com Available: https://www.zluri.com/blog/access-control-vs-access-management/.
3. Robin Materese (2016) Identity & access management. NIST Available: https://www.nist.gov/identity-access-management.
4. Admin (2022) 9 Key Benefits of Identity and Access Management (IAM). vSecureLabs Available: https://vsecurelabs.co/benefits-of-identity-and-access-management/.
5. Cisco (2023) Zero Trust Security. Duo Security Available: https://duo.com/solutions/zero-trust-security.
6. (2023) Zero Trust Maturity Model. Available: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.
7. Cisco (2023) What Is Zero Trust Network Access?. Available: https://www.cisco.com/c/en/us/products/security/zero-trust-network-access.html.
8. (2023) 3 reasons why you should invest in Identity and Access Management. get.sivis.com Available: https://get.sivis.com/en/blog/3-reasons-why-you-should-invest-in-identity-and-access-management.
9. (2016) Why should your company invest in access control?. imageHOLDERS Available: https://www.imageholders.com/insights/why-should-your-company-invest-in-access-control/.
10. D Saso (2022) Access Management Can Save You Money. OneLogin Identity Management Blog Available: https://www.onelogin.com/blog/access-management-can-save-you-money.
11. NIST (2023) Risk Appetite - Glossary | CSRC. csrc.nist.gov Available: https://csrc.nist.gov/glossary/term/Risk_Appetite.