Zero Trust Containers Architecture for Safeguarding of Sensitive Data

By: Adrian Magno

INTRODUCTION TO ZERO TRUST

In today's digital landscape, **sensitive data** is at constant risk. The **Zero Trust** model ensures that no one, whether inside or outside the organization, is trusted by default. This slide introduces the concept and its importance in **data security**.

- With the surge in cloud-native architectures and microservices, containers have emerged as a dominant method for deploying applications, offering significant benefits in scalability and portability.
- However, these advantages also bring unique security challenges, particularly in safeguarding sensitive data.
- Traditional security models, which rely heavily on perimeter-based defenses, prove insufficient in today's distributed and dynamic environments.

UNDERSTANDING ZERO TRUST

The **Zero Trust** framework operates on the principle of 'never trust, always verify'. This means that every access request is thoroughly **authenticated** and **authorized**, regardless of the user's location. It is essential for protecting sensitive data in modern environments.

- Zero Trust represents a paradigm shift in security, where every interaction—whether internal or external—is deemed untrustworthy.
- At the core of this model is the principle of “never trust, always verify,” which mandates rigorous identity verification, continuous monitoring, and minimized trust zones.
- This approach is particularly relevant in containerized architectures, where applications may operate in untrusted or hybrid cloud environments.

PROBLEM STATEMENT

What is the problem:

- Organizations adopting cloud-native architectures and microservices are facing security threats related to sensitive data in containers.
- Traditional perimeter-based security models are inadequate for the complexities of dynamic and distributed environments.

Potential solution:

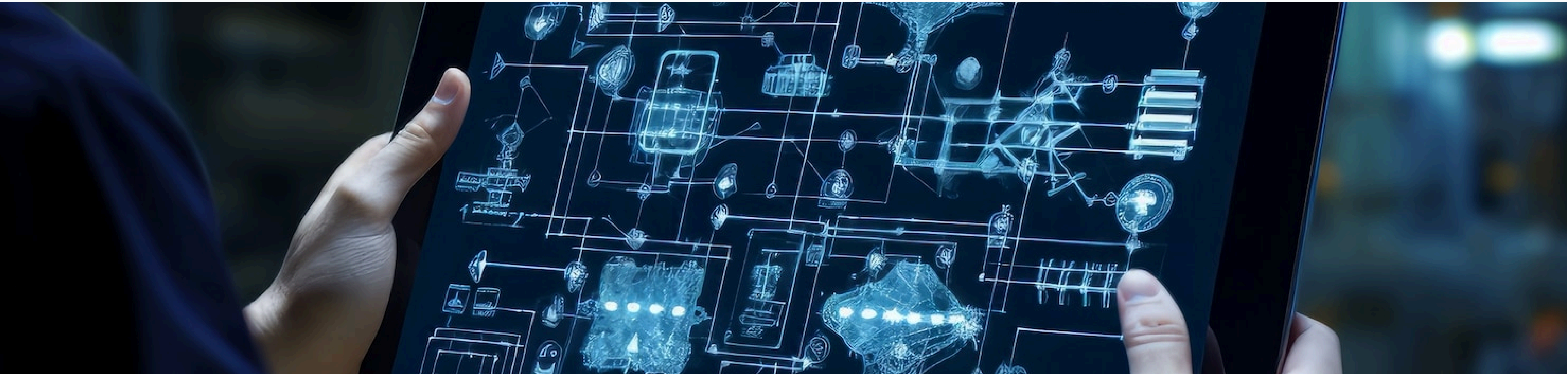
- A shift towards a Zero Trust security model, treating every interaction as untrustworthy.
- Implementation of rigorous identity verification and continuous monitoring is essential.

Research focus:

- Exploration of methodologies for integrating Zero Trust principles within containerized architectures.
- Evaluation of the effectiveness of these methodologies in safeguarding sensitive data.
- Presentation of empirical findings to guide organizations in enhancing their security posture.

LITERATURE REVIEW: EVOLUTION OF ZERO TRUST ARCHITECTURE

- The concept of Zero Trust architecturehas rapidly evolved, especially incontainerized environments.
- Containerstransform application development, deployment, and management.
- Inherent complexity of containers introduces newdata security challenges.
- Traditional security modelsare ill-suited: Rely on perimeter-based defense strategies.Become obsolete in dynamic, distributed systems.
- Zero Trustassumes that no entity is trusted by default, making it suitable for container security.
- Importance ofcontinuous verification,stringent access control, andreal-time monitoringis emphasized.



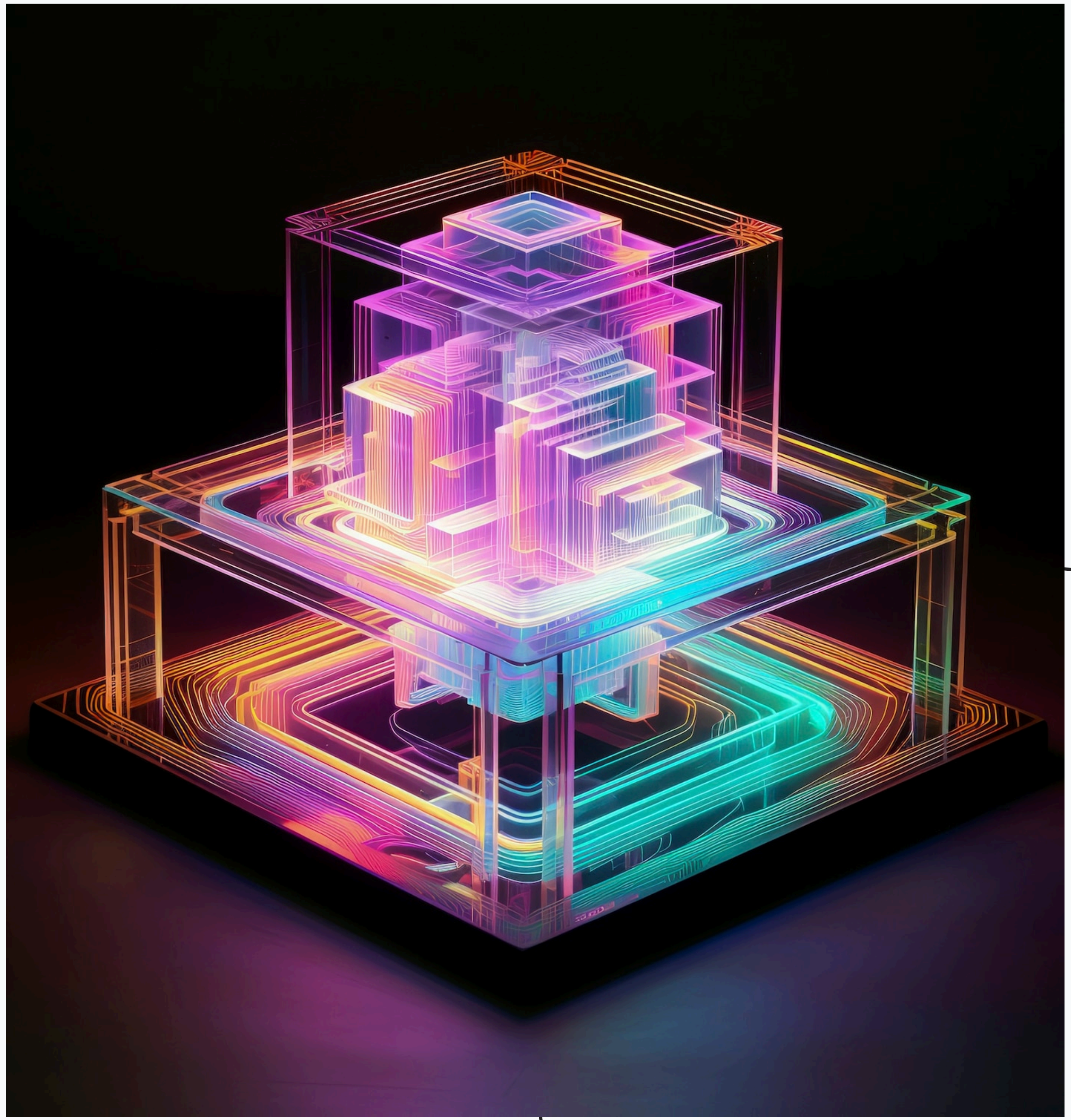
MICROSEGMENTATION IN ZERO TRUST

Critical area of focus: micro-segmentation.

- Divides container environments into smaller, isolated zones.Limits lateral movement of attackers within the system.

Research by Smith et al. (2022):

- If one part is compromised, the attack cannot easily spread.
- Minimizes exposure of sensitive data and restricts potential damage.
- Reduces the attack surface, creating a more secure environment.
- Enables granular security policies tailored to specific containers or microservices.



IDENTITY-BASED ACCESS CONTROL AND ENCRYPTION

- Integration of identity-based access control in container environments:
- Vital for hybrid or multi-cloud setups.
- Multi-factor authentication (MFA) recommended: Verifies access attempts based on multiple criteria (device identity, user credentials, behavioral patterns).
- Importance of encryption in containerized environments:
- Encrypt data both at rest and in transit
- Jones et al. (2021) discuss complexities in distributed systems.
- Challenges of key management for encryption.
- Adoption of robust key management systems for containers is essential.
- Use of Transport Layer Security (TLS) protocols for data in transit.

METHOD 1: MICROSEGMENTATION FOR CONTAINERS

- **Article**: Efficacy of Micro-Segmentation Assesment Report (2022)
- **Focus**: Exploring how microsegmentation controls can threat lateral movement within a network and increase the time and effort for attackers
- **Methodlogy**: It simulated attack scenarios in a 100-workload environment with varying levels of segmentation applied
- **Results**: Increased attack time by 300%-950% across use cases, a 44% reduction in visible services and progressively higher attack effort with more workloads

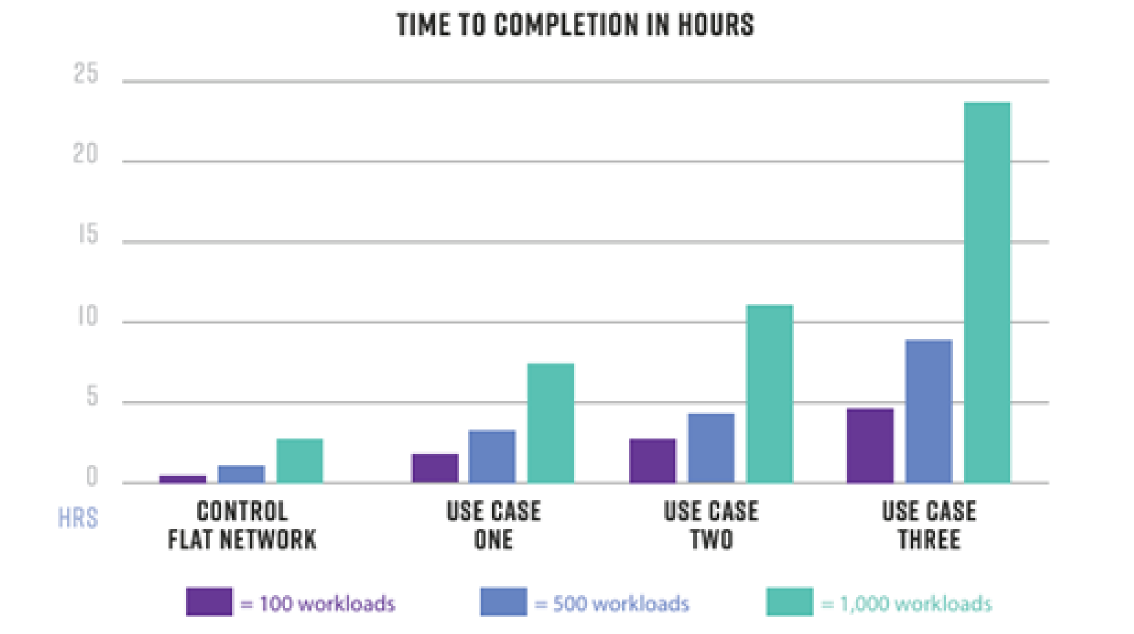
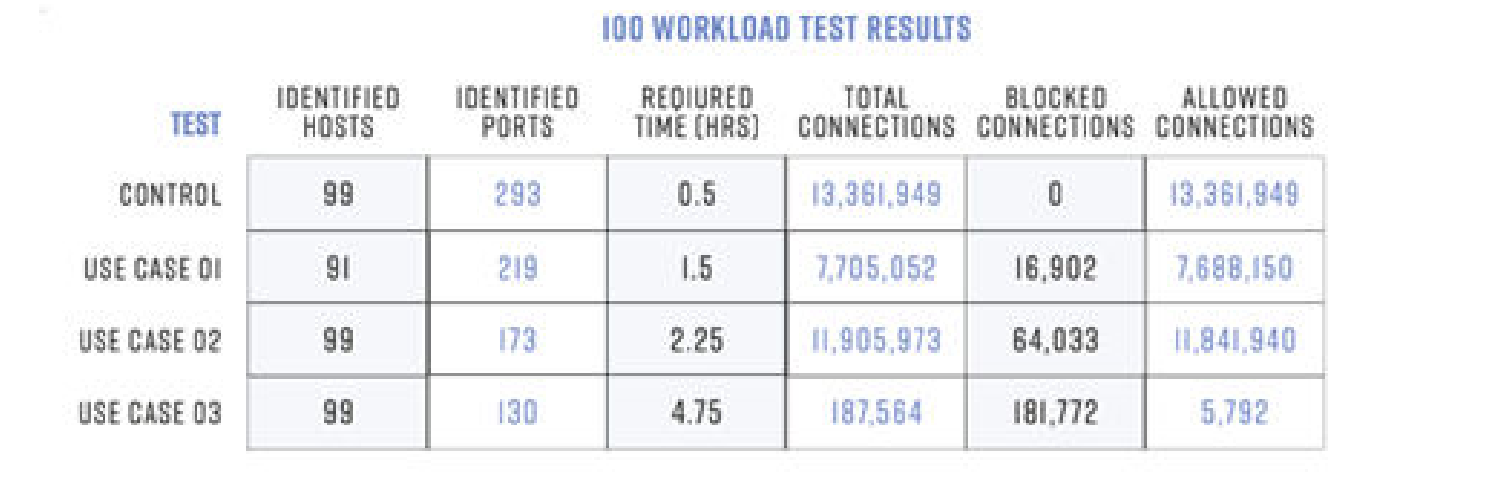


FIGURE I - RESULTS AND EXTRAPOLATIONS BASED ON TEST OUTCOMES



100 WORKLOAD TEST RESULTS

TEST	IDENTIFIED HOSTS	IDENTIFIED PORTS	REQUIRED TIME (HRS)	TOTAL CONNECTIONS	BLOCKED CONNECTIONS	ALLOWED CONNECTIONS
CONTROL	99	293	0.5	13,361,949	0	13,361,949
USE CASE 01	91	219	1.5	7,705,052	16,902	7,688,150
USE CASE 02	99	173	2.25	11,905,973	64,033	11,841,940
USE CASE 03	99	130	4.75	187,564	181,772	5,792

FIGURE 3 - RESULTS OF TESTING 100 WORKLOAD ENVIRONMENTS

METHOD 2: OPTIMIZING IDENTITY-BASED ACCESS CONTROL

- **Article**: Quantifying Permissiveness of Acces Control Policies (2022)
- **Focus**: Quantifying policy permissiveness and using constraint transformation to improve the efficiency and security of access control policies in cloud-based environments
- **Methodlogy**: Permissiveness quantification using a logarithmic scale and constraint transformation heuristics to simplify complex policy rules and improve evaluation speed.
- **Results**: Significant reduction in policy permissiveness with type constraints applied, improving security. For example, in AWS S3, permissiveness reduced from log2(AM) = 2,494.85 to log2(AM) = 1,499.67. Constraint transformation reduced evaluation time in AWS EC2 from 880.18 seconds to 33.41 seconds, drastically improving performance.

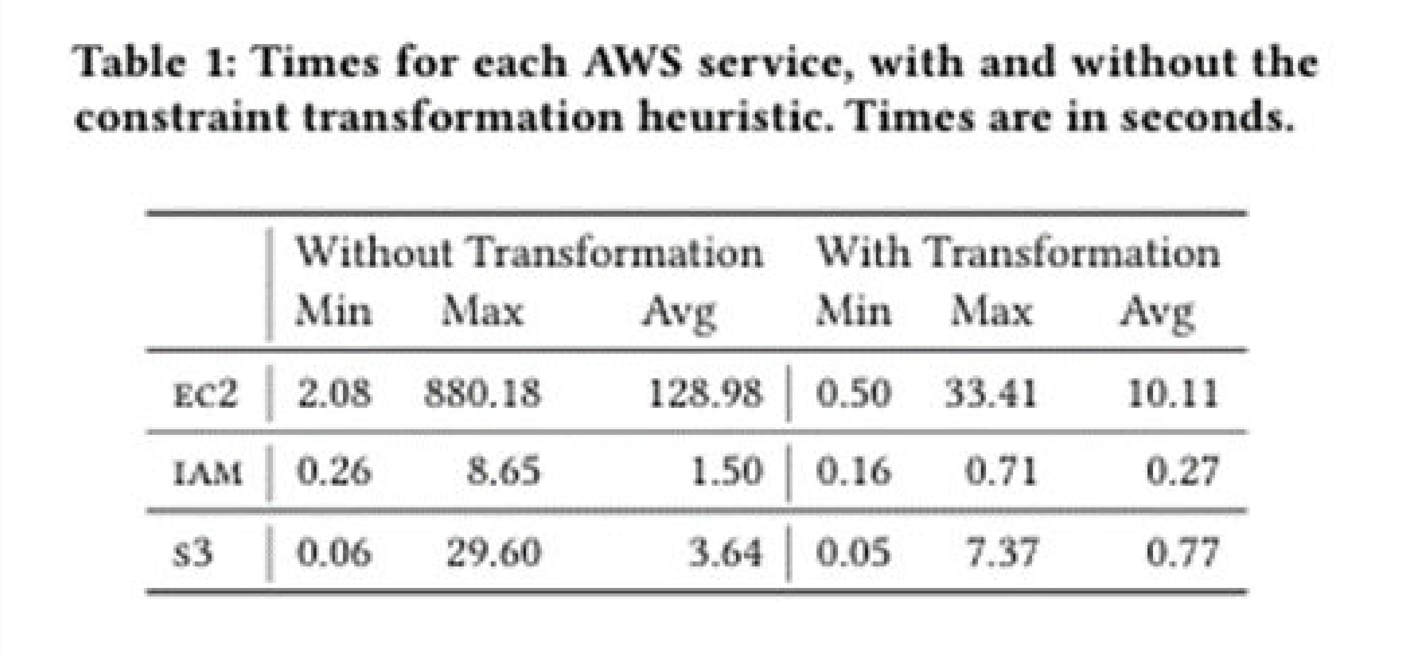


Table 1: Times for each AWS service, with and without the constraint transformation heuristic. Times are in seconds.

	Without Transformation			With Transformation		
	Min	Max	Avg	Min	Max	Avg
EC2	2.08	880.18	128.98	0.50	33.41	10.11
IAM	0.26	8.65	1.50	0.16	0.71	0.27
S3	0.06	29.60	3.64	0.05	7.37	0.77

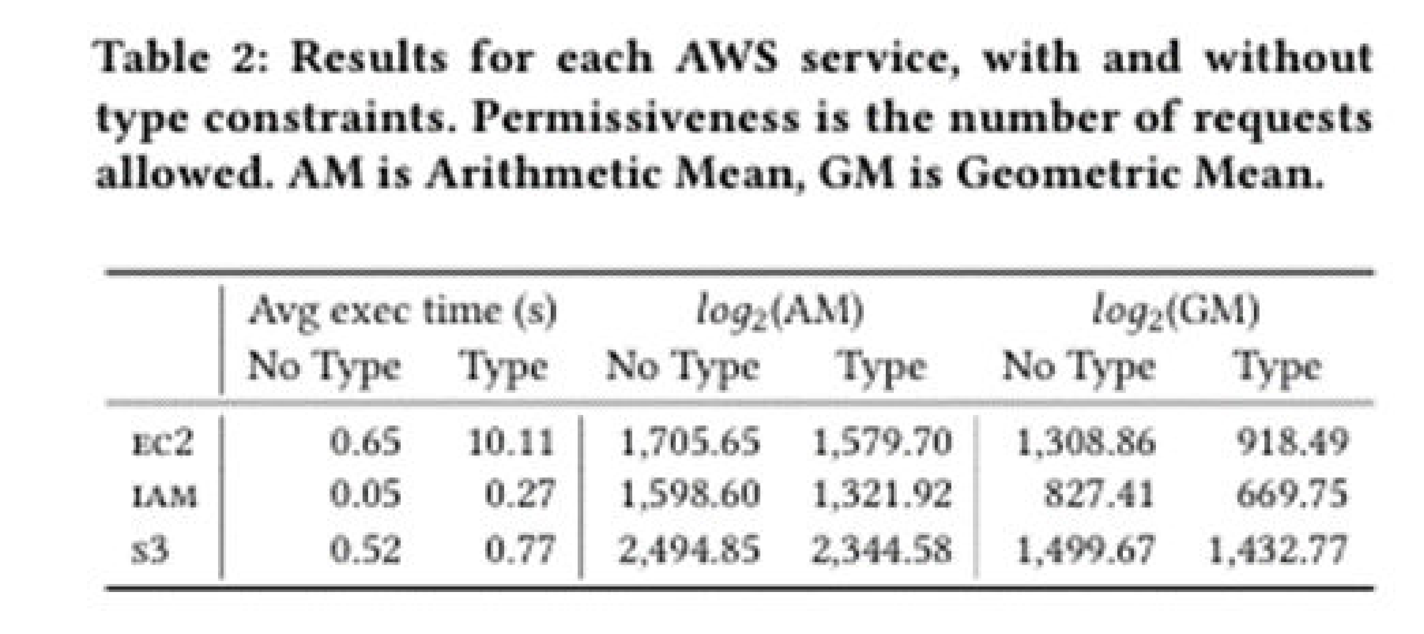


Table 2: Results for each AWS service, with and without type constraints. Permissiveness is the number of requests allowed. AM is Arithmetic Mean, GM is Geometric Mean.

	Avg exec time (s)		log_2(AM)		log_2(GM)	
	No Type	Type	No Type	Type	No Type	Type
EC2	0.65	10.11	1,705.65	1,579.70	1,308.86	918.49
IAM	0.05	0.27	1,598.60	1,321.92	827.41	669.75
S3	0.52	0.77	2,494.85	2,344.58	1,499.67	1,432.77

METHOD 3: CONTINUOUS AUTHENTICATION IN ZTCS

- **Article**: Security, Privacy, and Usability in Continuous Authentication: A survey (2021)
- **Focus**: Utilizing continuous authentication throughout sessions using physiological, behavioral, and context-aware biometric data to ensure ongoing user verification.
- **Methodlogy**: Physiological biometrics like facial recognition, behavioral biometrics such as keystroke dynamics, and context-aware authentication utilizing factors like IP addresses and GPS location..
- **Results**: Facial recognition systems achieved accuracy rates between 64-97%, keystroke systems up to 97% accuracy, and context-aware systems with 85% accuracy and a 0.03% error rate. Continuous monitoring ensures real-time reauthentication based on changing user behavior and environmental conditions.

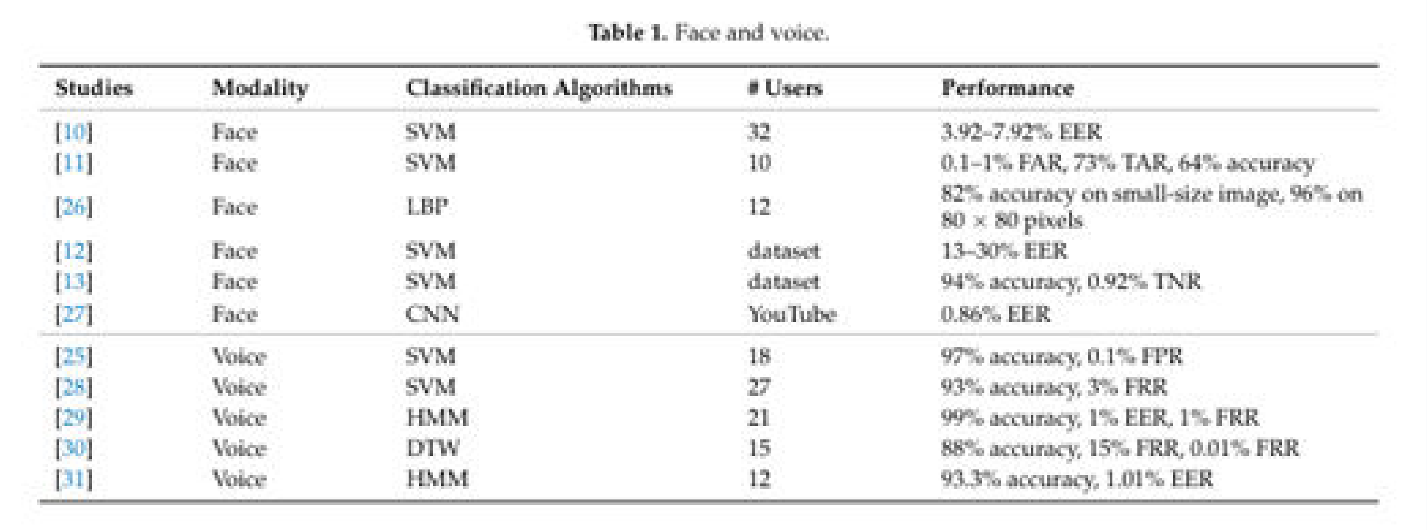


Table 1. Face and voice.

Studies	Modality	Classification Algorithms	# Users	Performance
[10]	Face	SVM	32	3.92–7.92% EER
[11]	Face	SVM	10	0.1–1% FAR, 73% TAR, 64% accuracy
[26]	Face	LBP	12	82% accuracy on small-size image, 96% on 80 × 80 pixels
[12]	Face	SVM	dataset	13–30% EER
[13]	Face	SVM	dataset	94% accuracy, 0.92% TNR
[27]	Face	CNN	YouTube	0.86% EER
[25]	Voice	SVM	18	97% accuracy, 0.1% FPR
[28]	Voice	SVM	27	93% accuracy, 3% FRR
[29]	Voice	HMM	21	99% accuracy, 1% EER, 1% FRR
[30]	Voice	DTW	15	88% accuracy, 15% FRR, 0.01% FRR
[31]	Voice	HMM	12	93.3% accuracy, 1.01% EER

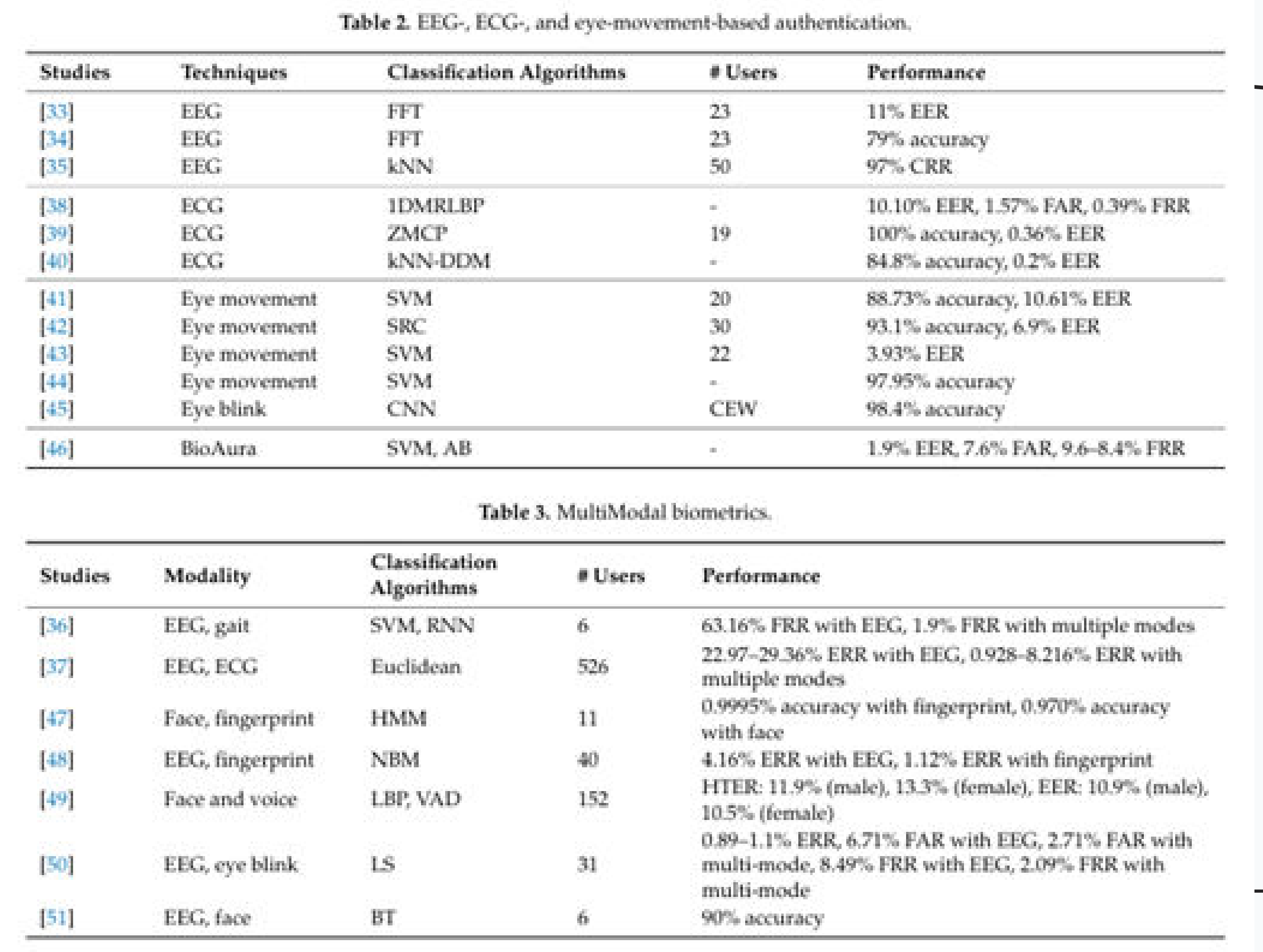


Table 2. EEG-, ECG-, and eye-movement-based authentication.

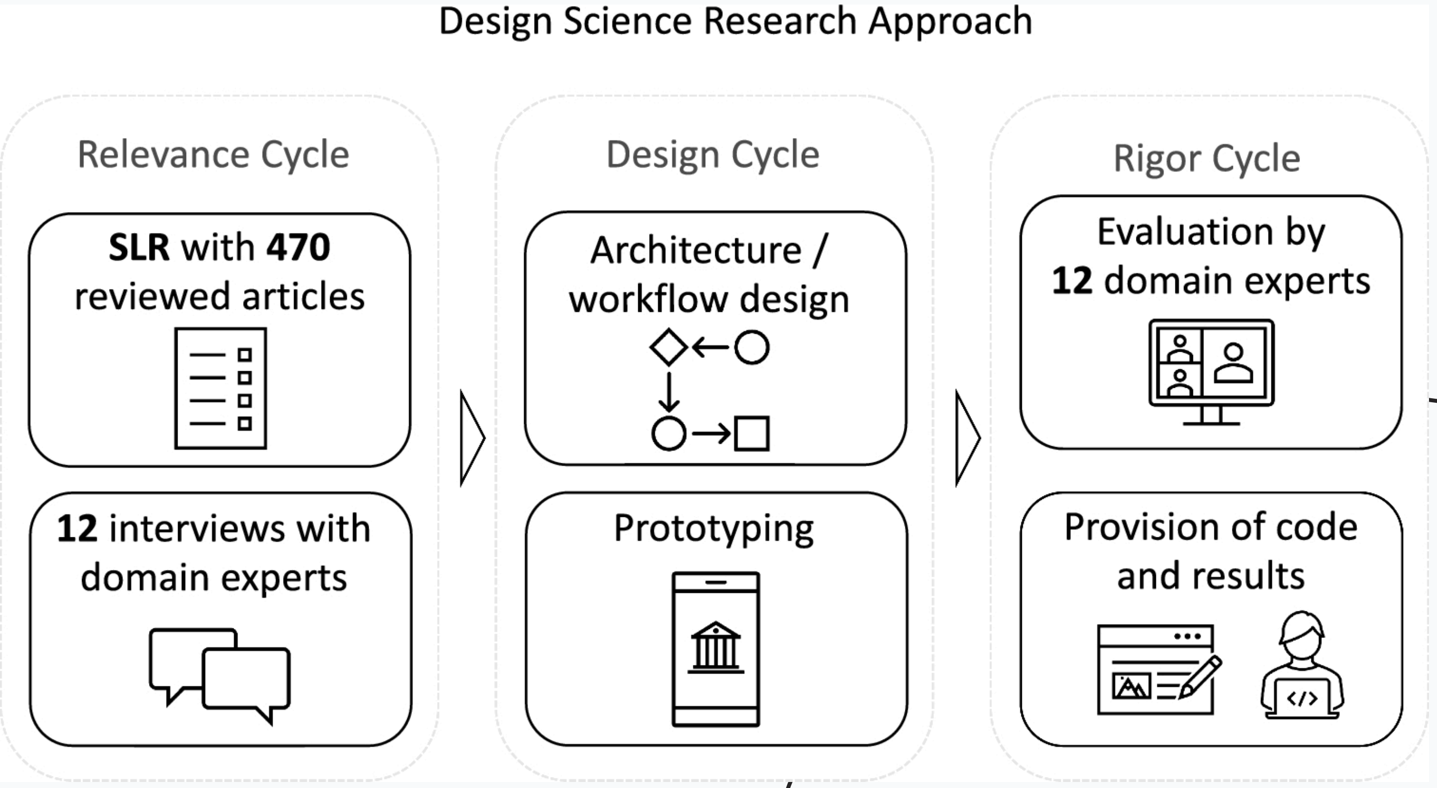
Studies	Techniques	Classification Algorithms	# Users	Performance
[33]	EEG	FFT	23	11% EER
[34]	EEG	FFT	23	79% accuracy
[35]	EEG	kNN	50	97% CRR
[38]	ECG	1DMRLBP	-	10.10% EER, 1.57% FAR, 0.39% FRR
[39]	ECG	ZMCP	19	100% accuracy, 0.36% EER
[40]	ECG	kNN-DDM	-	84.8% accuracy, 0.2% EER
[41]	Eye movement	SVM	20	88.73% accuracy, 10.61% EER
[42]	Eye movement	SRC	30	93.1% accuracy, 6.9% EER
[43]	Eye movement	SVM	22	3.93% EER
[44]	Eye movement	SVM	-	97.95% accuracy
[45]	Eye blink	CNN	CEW	98.4% accuracy
[46]	BioAura	SVM, AB	-	1.9% EER, 7.6% FAR, 9.6–8.4% FRR

Table 3. MultiModal biometrics.

Studies	Modality	Classification Algorithms	# Users	Performance
[36]	EEG, gait	SVM, RNN	6	63.16% FRR with EEG, 1.9% FRR with multiple modes
[37]	EEG, ECG	Euclidean	526	22.97–29.36% ERR with EEG, 0.928–8.216% ERR with multiple modes
[47]	Face, fingerprint	HMM	11	0.9995% accuracy with fingerprint, 0.970% accuracy with face
[48]	EEG, fingerprint	NBM	40	4.16% ERR with EEG, 1.12% ERR with fingerprint
[49]	Face and voice	LBP, VAD	152	HTER: 11.9% (male), 13.3% (female), EER: 10.9% (male), 10.5% (female)
[50]	EEG, eye blink	LS	31	0.89–1.1% ERR, 6.71% FAR with EEG, 2.71% FAR with multi-mode, 8.49% FRR with EEG, 2.09% FRR with multi-mode
[51]	EEG, face	BT	6	90% accuracy

METHOD 4: IMPLEMENTING ACCESS REVIEWS AND RECERTIFICATION

- **Article**: A Systematic Review of Identity and Access Management Requirements in Enterprises and Ponteital Contributions (2024)
- **Focus**: Systematically auditing and reviewing user access rights through regular recertification to minimize privilege creep and unauthorized access.
- **Methodlogy**: Regular audits, Role-Based Access Control (RBAC), and automation of access reviews to streamline the recertification process and reduce errors.
- **Results**: Organizations experienced a 30% decrease in unauthorized access incidents and a 25% decline in security incidents by using RBAC. Automation led to a 40% reduction in the time spent on access reviews, while thorough documentation reduced non-compliance issues by 20%.



Design Science Research Approach

Relevance Cycle

SLR with **470** reviewed articles

12 interviews with domain experts

Design Cycle

Architecture / workflow design

Prototyping

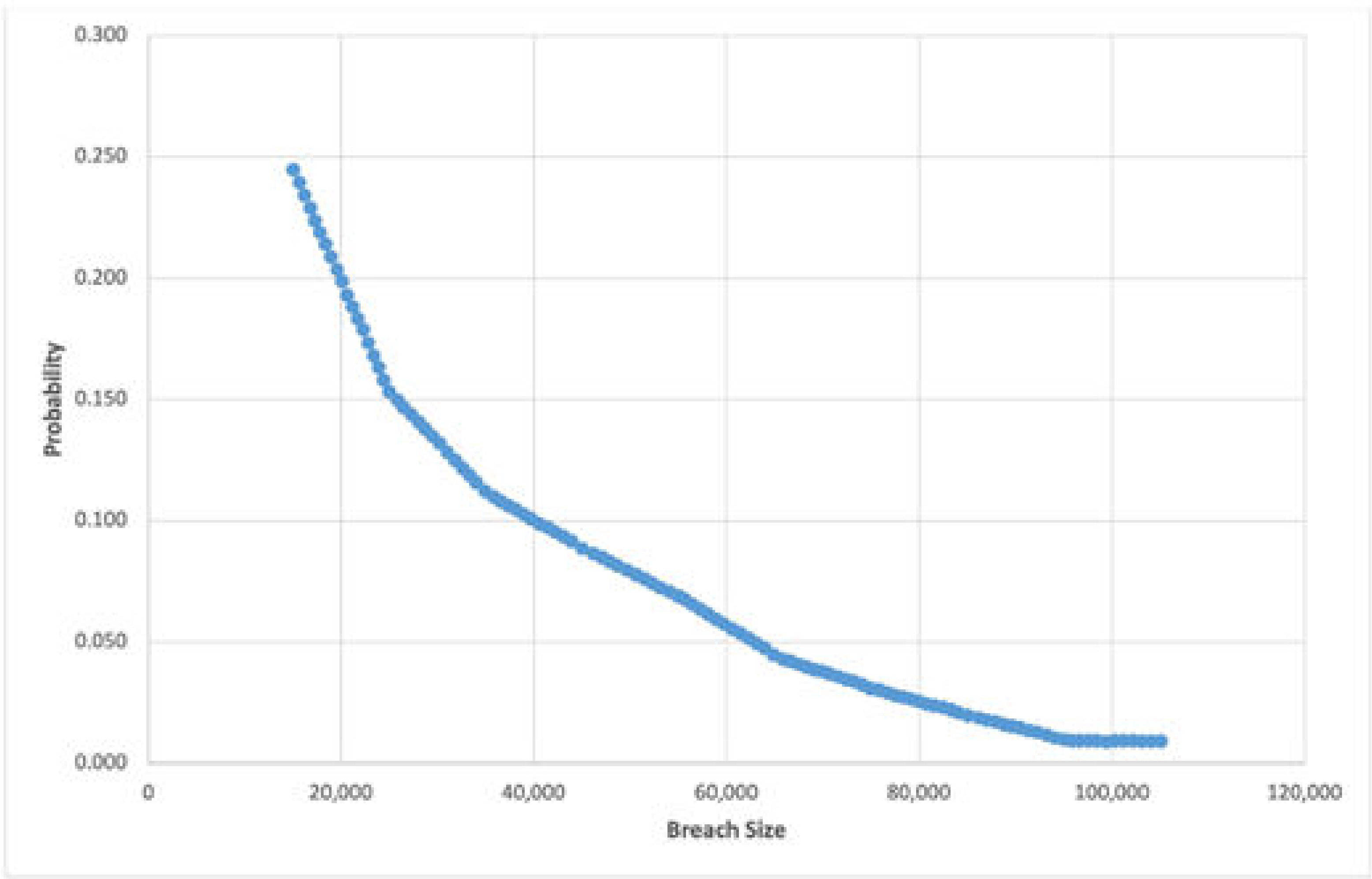
Rigor Cycle

Evaluation by **12** domain experts

Provision of code and results

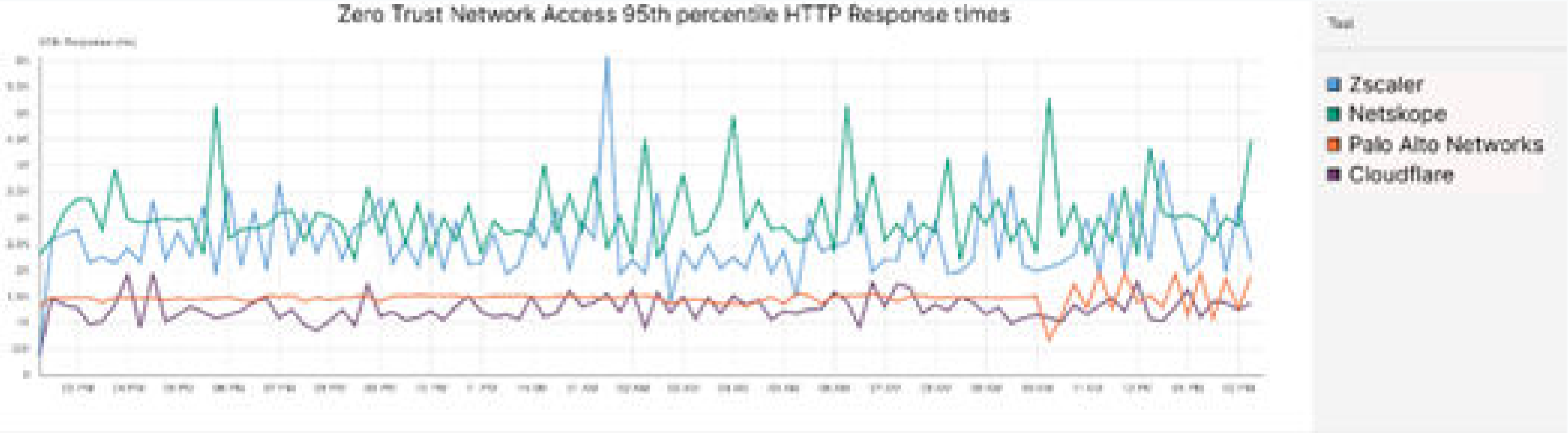
METHOD 5: DATA ENCRYPTION AND TOKENIZATION

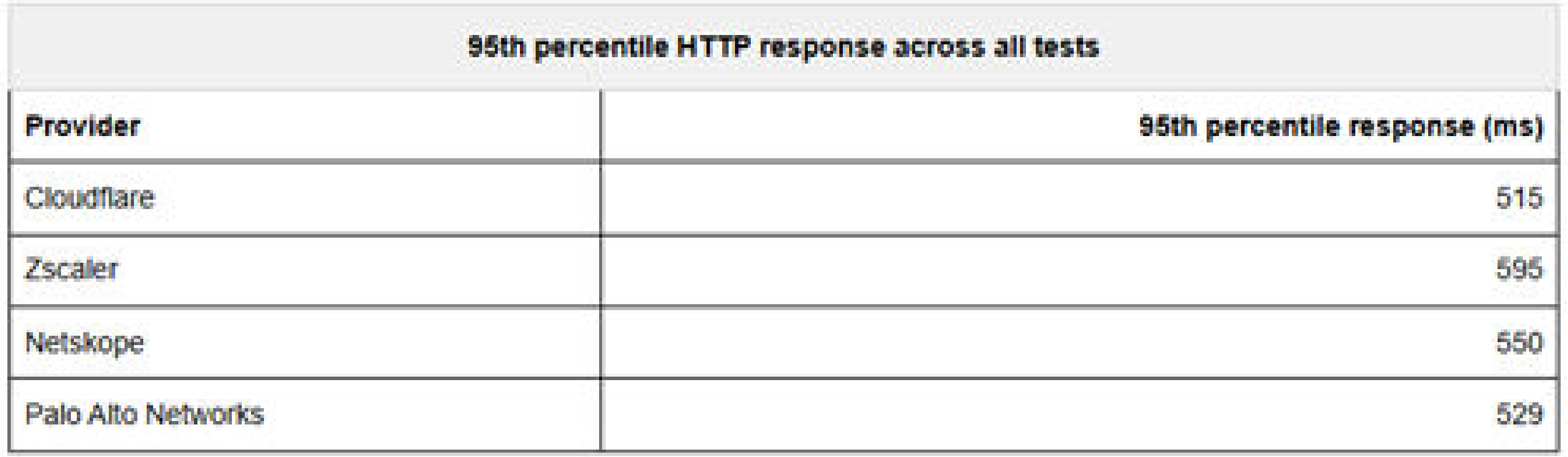
- **Article**: Quantitative Assesment of Cybersecurity Risks for Mitigating Data Breaches (2021)
- **Focus:** Using encryption to convert sensitive data into unreadable formats and tokenization to replace sensitive data with nonsensitive tokens, enhancing security and maintaining operational efficiency..
- **Methodlogy**: Encryption and tokenization techniques are employed to protect sensitive data, combined with quantitative assessments of breach costs and compliance with regulations like PCI DSS and GDPR.
- **Results**: Companies implementing encryption can reduce breach costs by 47%, as per Ponemon Institute data. Tokenization allows organizations to perform data analytics while maintaining compliance and protecting sensitive information, reducing the risk of frequent, smaller data breaches.



METHOD 6: PERFORMANCE OPTIMIZATION THROUGH SWB AND ZTNA

- **Article**: Addressing Security Challenges in Cloud-Native Architectures (2023)
- **Focus:** Improving security and performance by utilizing SWGs and ZTNA, ensuring fast, secure access to web resources without compromising user experience.
- **Methodlogy**: Performance tests comparing Cloudflare, Zscaler, and Netskope for SWG and ZTNA speeds, focusing on HTTP response times and threat minimization.
- **Results**: Cloudflare was 46% faster in ZTNA and 64% faster in Remote Browser Isolation compared to competitors. SWG tests showed a 95th percentile HTTP response time of 515 ms for Cloudflare, significantly faster than competitors. Organizations reported a 40% reduction in attack surface and a 60% decrease in data leakage incidents.





95th percentile HTTP response across all tests	
Provider	**95th percentile response (ms)**
Cloudflare	515
Zscaler	595
Netskope	550
Palo Alto Networks	529

METHOD 7: ADVANCED ENDPOINT DETECTION AND RESPONSE SYSTEMS

- **Article**: An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors (2021)
- **Focus:** Assessing the capabilities of EDR systems in detecting APTs through comprehensive telemetry and behavioral analytics.
- **Methodlogy**: Simulated APT attacks to evaluate the effectiveness of multiple EDR systems, analyzing real-time telemetry from various endpoints..
- **Results**: More than 50% of attacks were successful, revealing significant blind spots in existing EDR solutions. EDR efficacy depends on robust configuration and skilled SOC teams. Research also highlights vulnerabilities in EDR telemetry, emphasizing the need for continuous evaluation and adjustment to emerging threats.

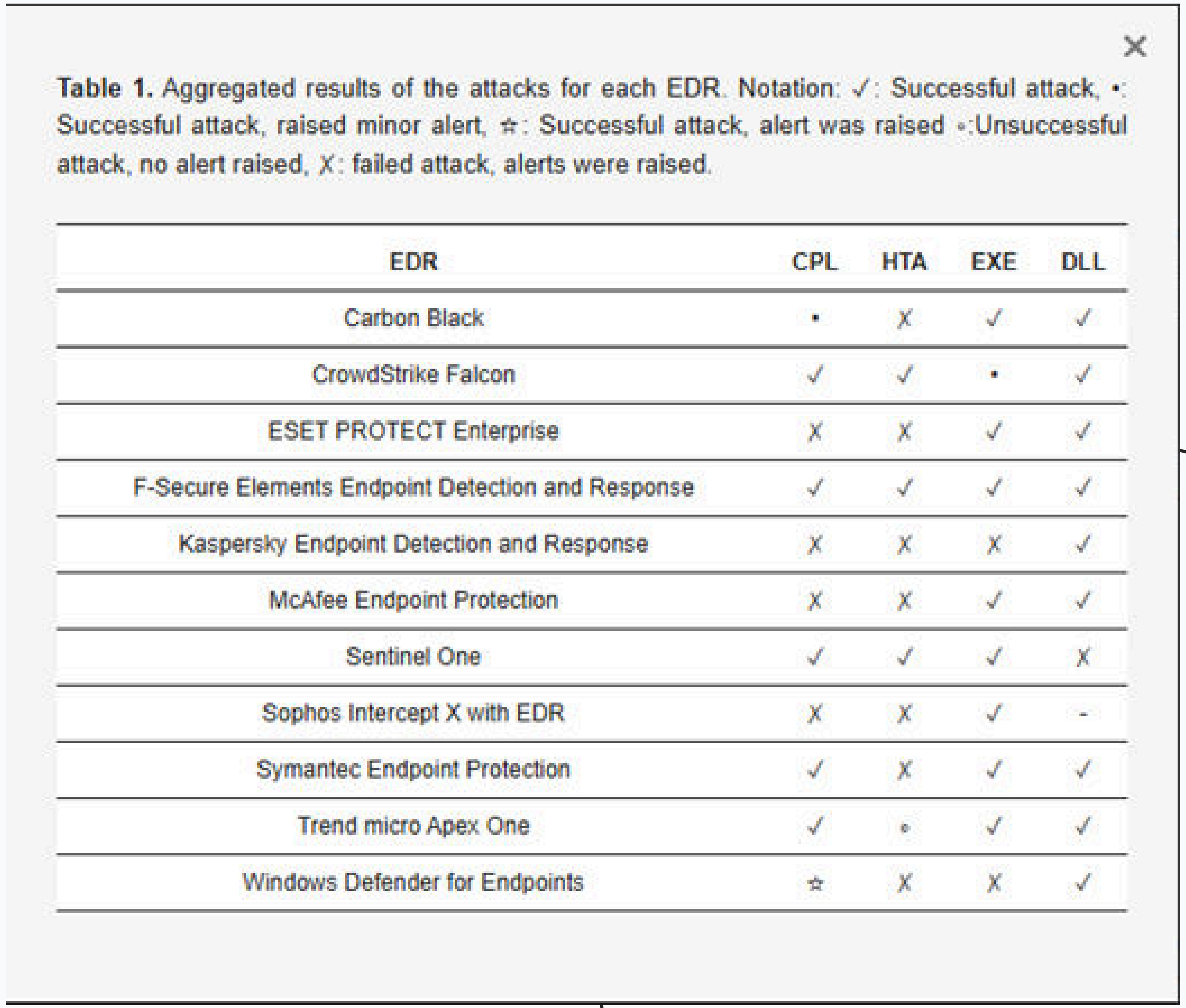


Table 1. Aggregated results of the attacks for each EDR. Notation: ✓: Successful attack, •: Successful attack, raised minor alert, ☆: Successful attack, alert was raised ∘:Unsuccessful attack, no alert raised, ✗: failed attack, alerts were raised.

EDR	CPL	HTA	EXE	DLL
Carbon Black	•	✗	✓	✓
CrowdStrike Falcon	✓	✓	•	✓
ESET PROTECT Enterprise	✗	✗	✓	✓
F-Secure Elements Endpoint Detection and Response	✓	✓	✓	✓
Kaspersky Endpoint Detection and Response	✗	✗	✗	✓
McAfee Endpoint Protection	✗	✗	✓	✓
Sentinel One	✓	✓	✓	✗
Sophos Intercept X with EDR	✗	✗	✓	-
Symantec Endpoint Protection	✓	✗	✓	✓
Trend micro Apex One	✓	∘	✓	✓
Windows Defender for Endpoints	☆	✗	✗	✓

RECOMMENDATION OF THE MOST EFFECTIVE METHODOLOGY

- **Method 5**: Data Encryption and Tokenization
- **Strong Data Protection**: Encryption keeps sensitive data unreadable, even if accessed by unauthorized parties. Tokenization further enhances security by substituting sensitive data with nonsensitive tokens.
- **Compliance with Regulations**: Helps meet GDPR, PCI DSS, and other regulatory standards, ensuring sensitive data is protected in compliance with legal requirements.
- **Cost and Risk Reduction**: Research shows a 47% reduction in breach costs for companies that use encryption, minimizing financial risks associated with potential data breaches.
- **Alignment with Zero Trust Principles**: Supports the Zero Trust model by protecting data regardless of user or service access, ensuring no implicit trust is given, even inside the network.
- **Versatility**: Effective in safeguarding both data at rest and in transit, ensuring data remains secure throughout its lifecycle in cloud-native and containerized environments.

CONCLUSION

- **Zero Trust Architecture (ZT)** is a critical framework for enhancing security in modern, containerized environments by eliminating implicit trust and enforcing strict access controls.
- By integrating methodologies like **Data Encryption, Tokenization, Continuous Authentication,** and **Micro-segmentation**, ZT ensures that sensitive data and systems are protected from both internal and external threats.
- Combining **Secure Web Gateways (SWGs), Zero Trust Network Access (ZTNA),** and **Advanced Endpoint Detection and Response (EDR)** systems optimizes both security and performance, ensuring that security measures do not compromise operational efficiency**.**
- Ultimately, Zero Trust is not just a **security measure** but a **transformative approach** to handling modern cyber threats, enabling organizations to proactively defend their systems while maintaining **agility** and **compliance** in an increasingly complex digital landscape.

REFERENCES

[1] Algarni, Abdullah M., Vijey Thayananthan, and Yashwant

K. Malaiya. 2021. "Quantitative Assessment of Cybersecurity Risks for

Mitigating Data Breaches in Business Systems" Applied Sciences 11,

no. 8: 3678. https://doi.org/10.3390/app11083678[2] Appel, J. (2021). Continuous Access Evaluation in Zero

Trust Architectures. Retrieved from https://jeffreyappel.nl/fast-response-with-azure-ad-continuous-access-evaluation-cae-and-conditional-access/[3] Baig, Ahmed Fraz, and Sigurd Eskeland. 2021.

"Security, Privacy, and Usability in Continuous Authentication: A

Survey" Sensors 21, no. 17: 5967.

https://doi.org/10.3390/s21175967[4] Baldwin, J.

(2023). Securing Cloud-Native Applications: The Role of Zero Trust.

Cybersecurity Journal, 4(1), 25-37. https://doi.org/10.1007/s42400-021-00092-8[5] Bishop Fox. (2023). Efficacy of Micro-Segmentation

Assessment Report. Retrieved from https://cdn.prod.website-files.com/63e25fb5e66132e6387676dc/641b70263ad4cb1b0568f2ae_Efficacy-of-Micro-Segmentation-Assessment-Report.pdf[6] Cai, F., Zhu, N., He, J., et al. (2019). Survey

access control models and technologies for cloud computing. Cluster

Computing, 22(Suppl 3), 6111–6122. https://doi.org/10.1007/s10586-018-1850-7[7] Cheng, L., & Zhang, Y. (2023). Addressing Security

Challenges in Cloud-Native Architectures. Journal of Cloud Computing, 12(2),

145-162. https://doi.org/10.1007/s13677-022-00318-9[8] Cloudflare. (2023). Spotlight on Zero Trust: We're

fastest and here's the proof. Retrieved from https://blog.cloudflare.com/spotlight-on-zero-trust/[9] Das, S., Kumar, R., & Patel, V. (2023). Zero Trust

Security in Containerized Environments: Best Practices and Implementation

Strategies. Information Security Journal, 32(3), 210-225. https://doi.org/10.1080/19393555.2023.2185437[10] Eiers, W., O'Mahony, E., Sankaran, G., Prince, B., Li,

A., & Bultan, T. (2022). Quantifying Permissiveness of Access Control

Policies. In Proceedings of the 44th International Conference on Software

Engineering (ICSE). Retrieved from https://vlab.cs.ucsb.edu/papers/ICSE2022_access_control.pdf[11] Glöckler, J., Sedlmeir, J., Frank, M. et al. A

Systematic Review of Identity and Access Management Requirements in Enterprises

and Potential Contributions of Self-Sovereign Identity. Bus Inf Syst

REFERENCES

[1] Illumio. (n.d.). Preventing Lateral Movement of
Threats with Micro-Segmentation. Retrieved from https://www.tigera.io/blog/deep-dive/preventing-lateral-movement-of-threats-with-microsegmentation/[2] Jones, M., & Smith, L. (2021). Data Encryption and
Tokenization. Applied Sciences, 11(8), 3678. https://www.mdpi.com/2076-3417/11/8/3678#B2-applsci-11-03678[3] Karantzas, G., & Patsakis, C. (2021). An Empirical
Assessment of Endpoint Detection and Response Systems against Advanced
Persistent Threats Attack Vectors. Journal of Cybersecurity and Privacy, 1(3),
387-421. https://doi.org/10.3390/jcp1030021[4] Kumar, A., & Patel, R. (2022). Advanced Endpoint
Detection and Response Systems against Advanced Persistent Threats Attack
Vectors. Journal of Cybersecurity and Privacy, 1(3), 387-421. https://doi.org/10.3390/jcp1030021[5] Kumar, A., & Patel, R. (2022). Continuous
Authentication in Zero Trust Environments. International Journal of
Information Security, 21(4), 369-386. https://doi.org/10.1007/s10207-022-00631-y[6] Martinez, A., Smith, J., & Johnson, L. (2022).
Enforcing Policy as Code in Containerized Environments. Springer. https://link.springer.com/article/10.1007/s12599-023-00830-x[7] Palo Alto Networks. (n.d.). What is microsegmentation?
Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-microsegmentation#benefits[8] Rose, S., Borchert, O., & Mitchell, S. (2020).
Zero Trust Architecture. NIST Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207[9] Trend Micro. (n.d.). ZTNA vs VPN: Secure Remote Work.
Retrieved from https://www.trendmicro.com/en_in/research/22/h/ztna-vs-vpn-secure-remote-work.html[10] Trend Micro. (n.d.). Secure Web Gateway (SWG) security
and SASE. Retrieved from https://www.trendmicro.com/en_us/ciso/22/j/secure-web-gateway-swg-security-sase-part-3.html[11] VPN Alert. (2021). Encryption statistics. Retrieved
from https://vpnalert.com/resources/encryption-statistics/[12] Zhou, Y., & Lin, Q. (2023). Optimizing
Identity-Based Access Control Through Constraint Transformation and
Permissiveness Analysis. Journal of Cybersecurity and Privacy, 1(2), 21.
https://doi.org/10.3390/jcp1020021