Zero Trust Architecture And Ransomware Mitigation

Ely Johnson

Introduction

- Ransomware is a major and growing cybersecurity threat
- Attacks cause significant financial and operational damage
- Modern environments (cloud, remote work) increase risk
- **Zero Trust Architecture (ZTA)**
  - No implicit trust
- **Focus:** How ZTA helps reduce ransomware impact

What is Ransomware?

- Malware that encrypts files for ransom
- Enters via phishing or vulnerabilities
- Spreads through lateral movement
- Causes major operational & financial damage

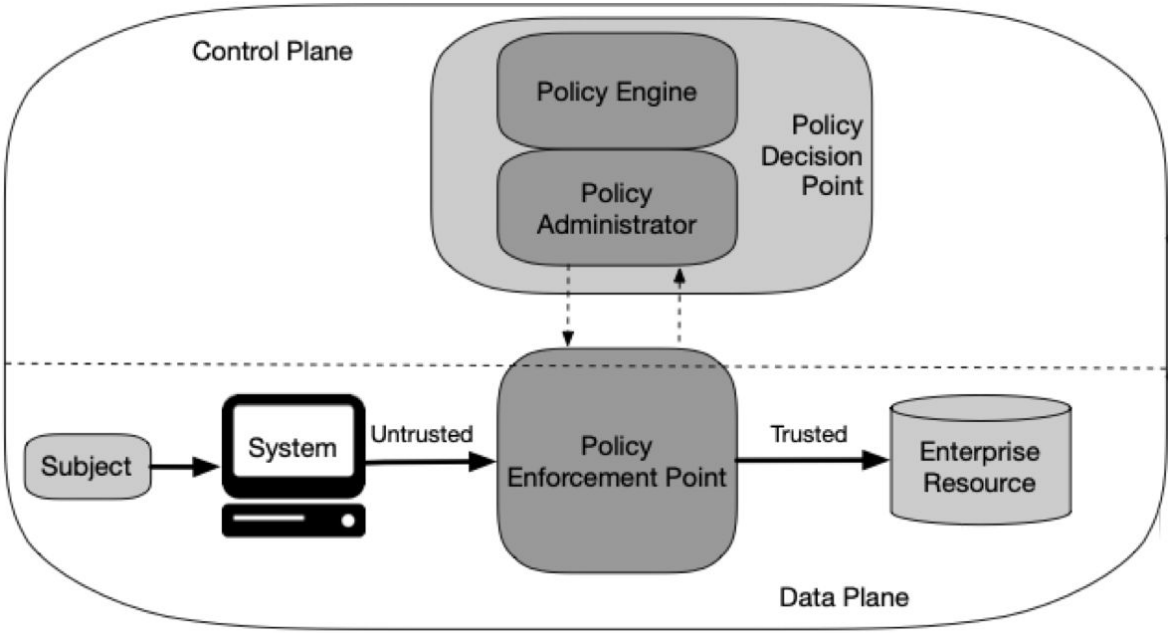
Traditional Security and Where It Falls Short

- Perimeter-based (“trust inside, block outside”)
- Assumes internal users are safe
- Limited visibility after access is granted
- Allows attackers to move laterally

What is Zero Trust Architecture (ZTA)?

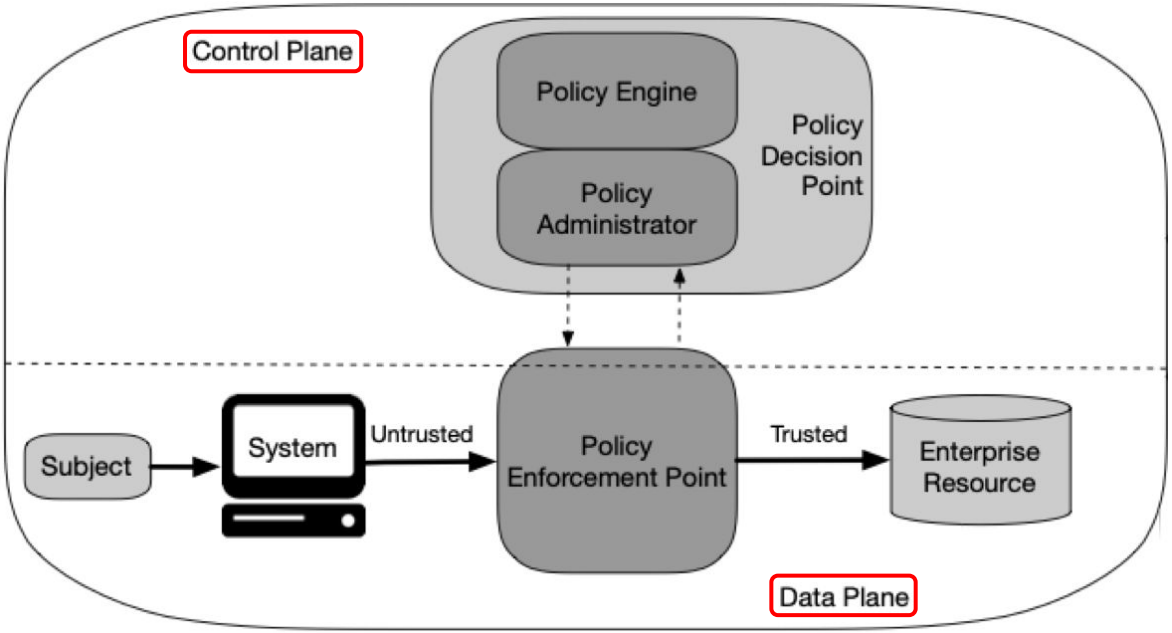
- Security model: **“Never trust, always verify”**
- No implicit trust (inside or outside network)
- Continuous authentication & authorization
- Access based on identity, device, and context

Core ZTA Logical Components



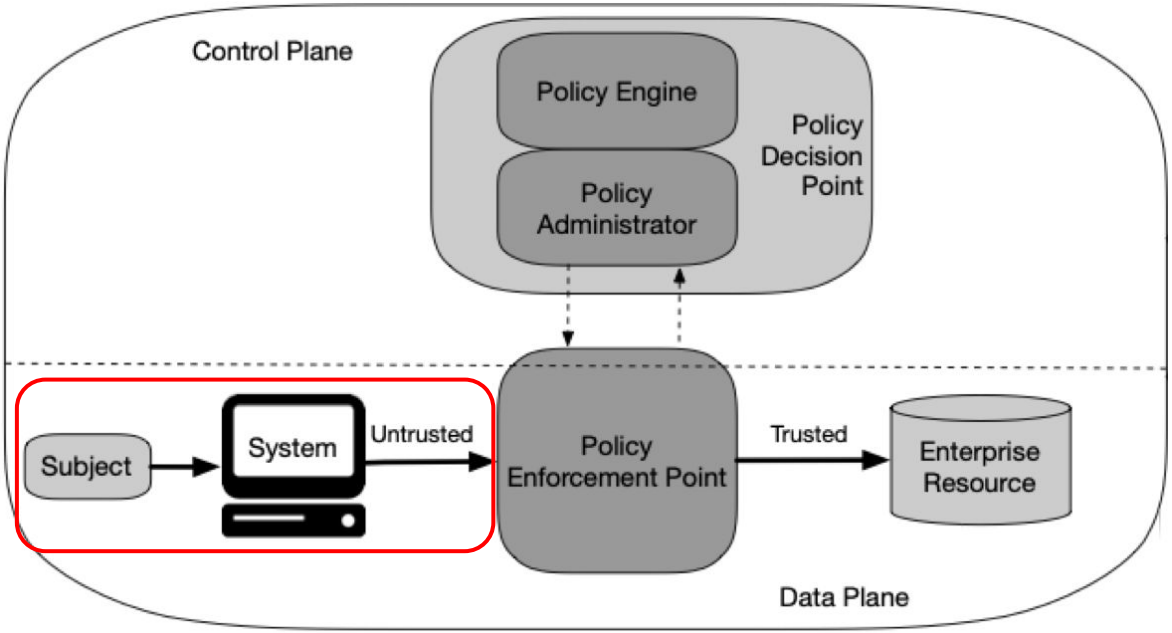
[6]

Control Plane and Data Plane



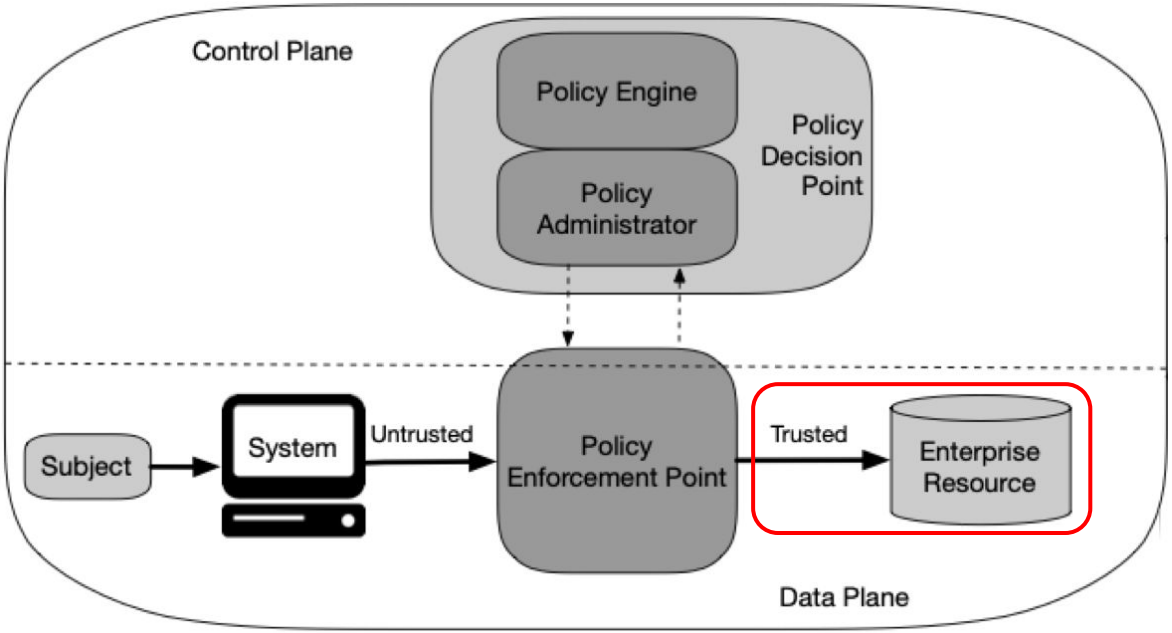
[6]

Subject/System



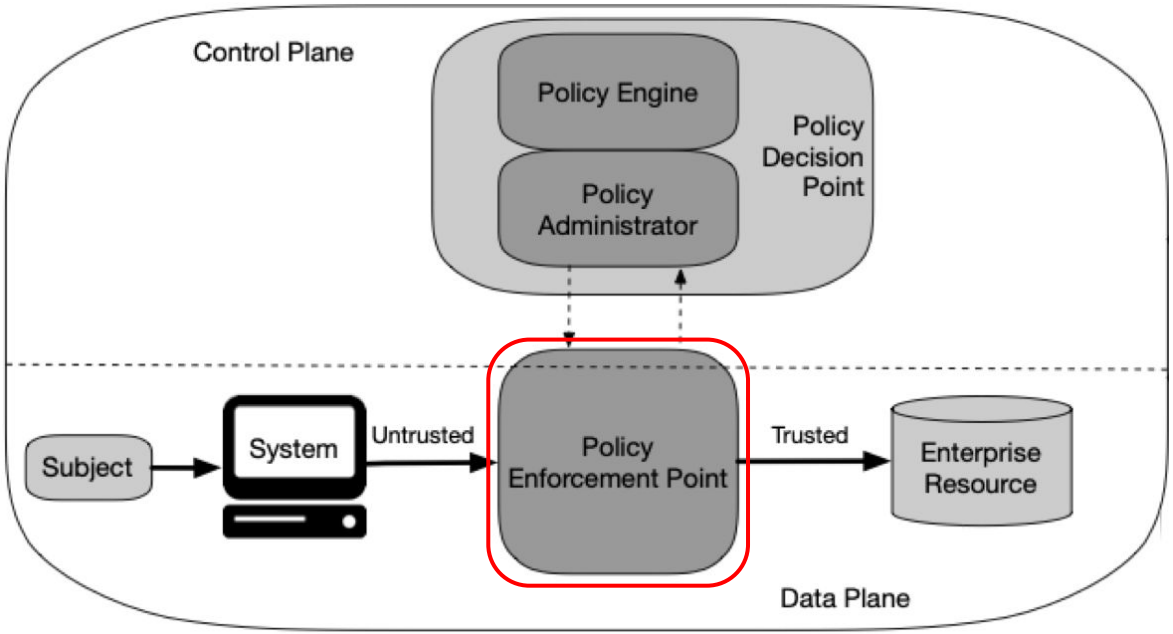
[6]

Enterprise Resource



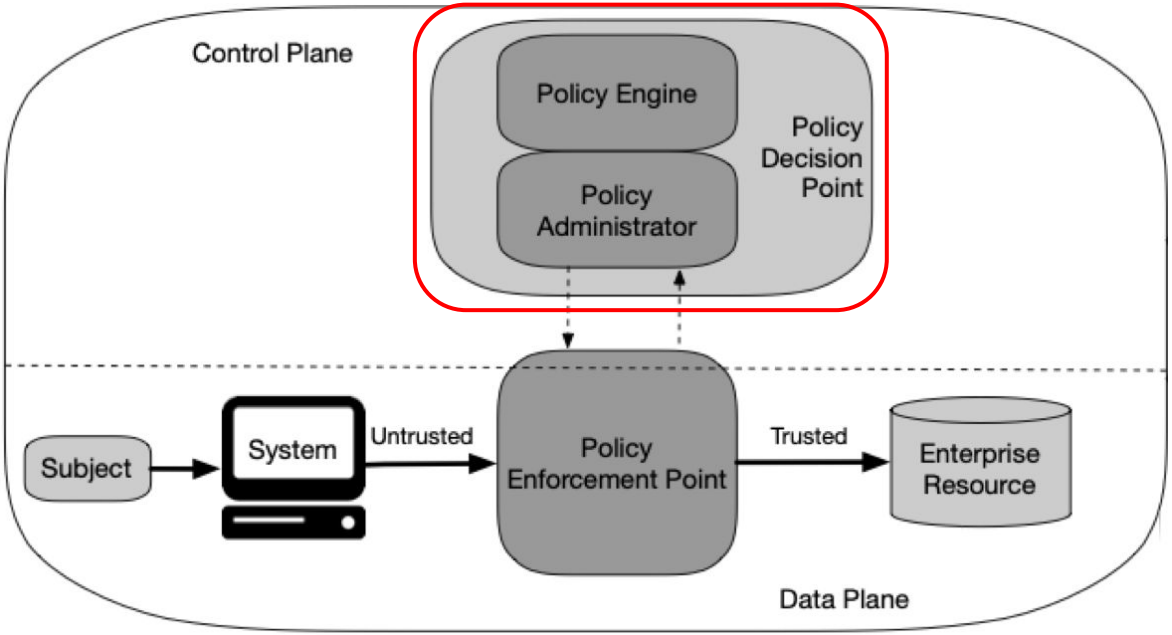
[6]

Policy Enforcement Point (PEP)



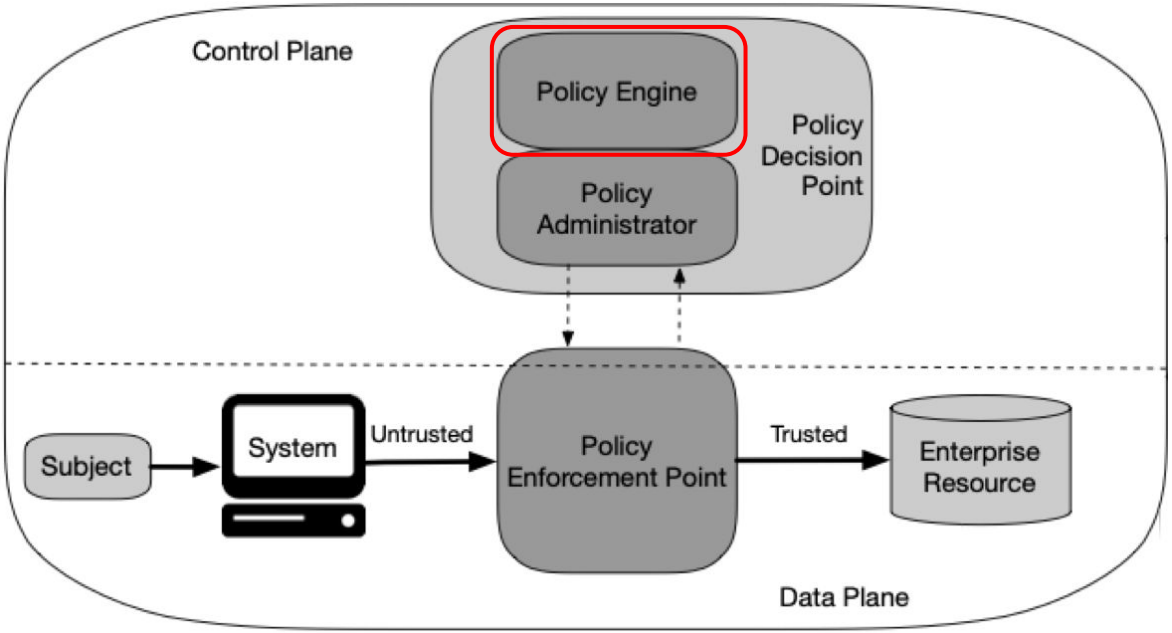
[6]

Policy Decision Point (PDP)



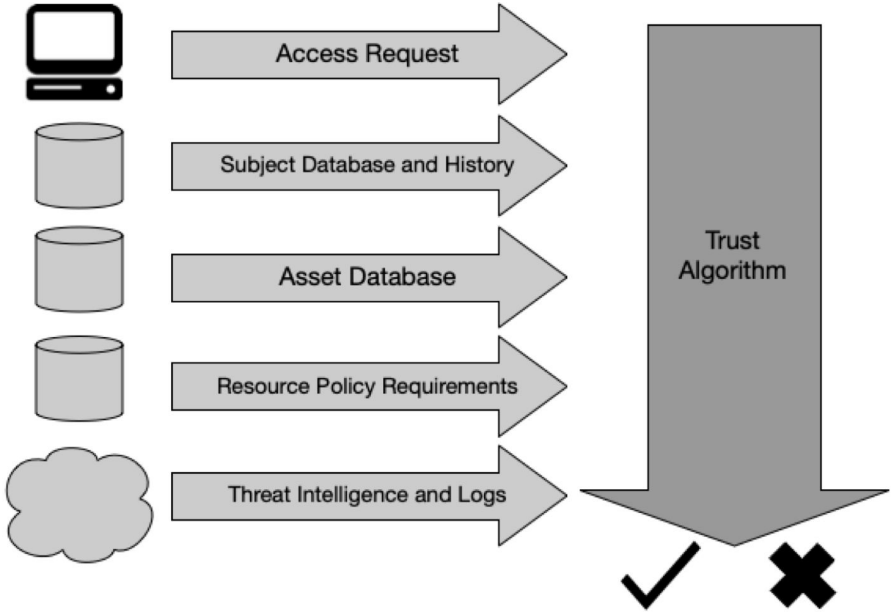
[6]

Policy Engine (PE)



[6]

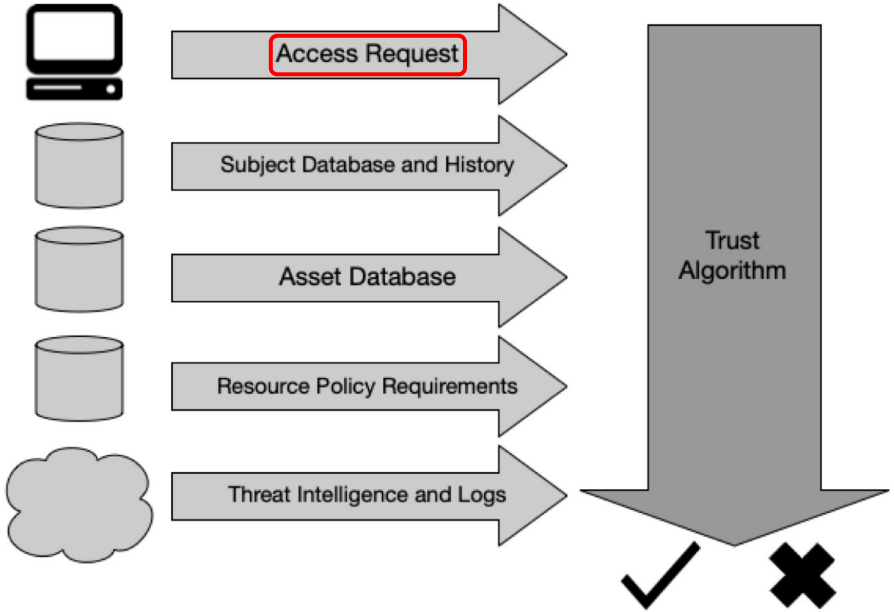
Trust Algorithm



[6]

Trust Algorithm

Access Request: Info about what is being requested and by whom

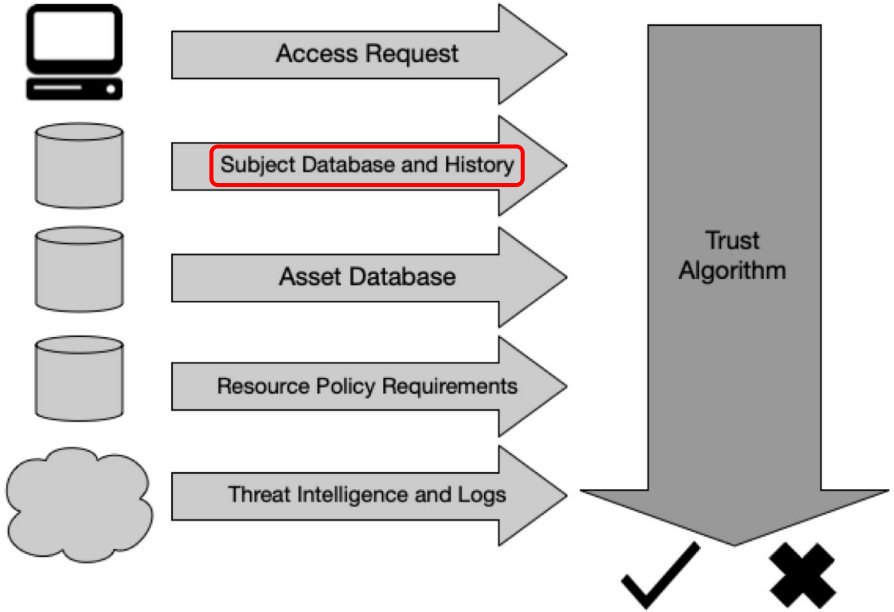


[6]

Trust Algorithm

Access Request: Info about what is being requested and by whom

Subject Database and History: Who is requesting and their past behavior



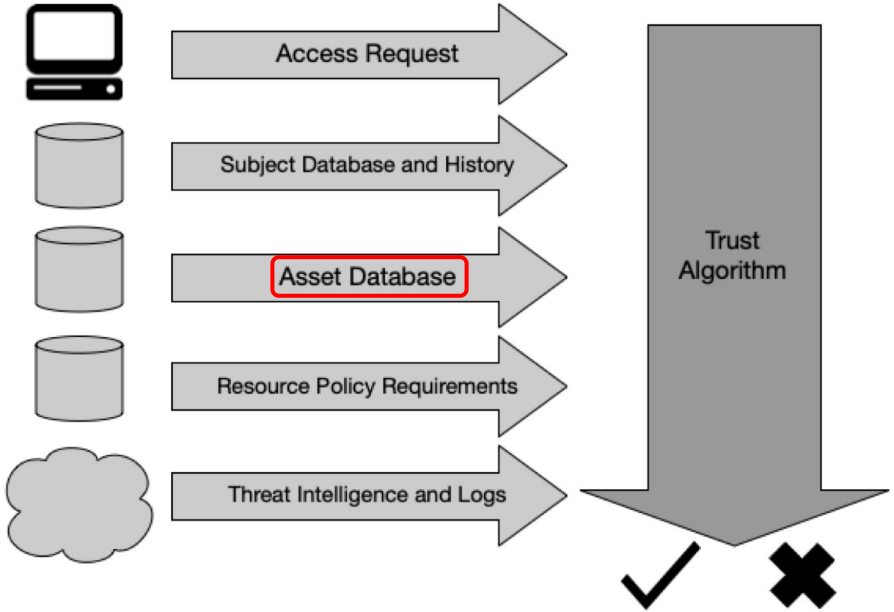
[6]

Trust Algorithm

Access Request: Info about what is being requested and by whom

Subject Database and History: Who is requesting and their past behavior

Asset Database: Trusted device list



[6]

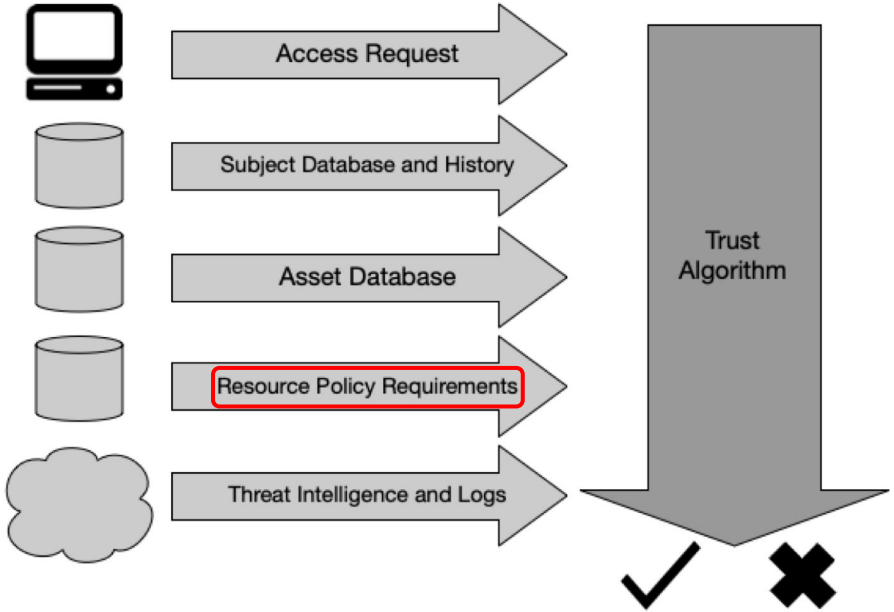
Trust Algorithm

Access Request: Info about what is being requested and by whom

Subject Database and History: Who is requesting and their past behavior

Asset Database: Trusted device list

Resource Policy Requirements: Rules for accessing the resource



[6]

Trust Algorithm

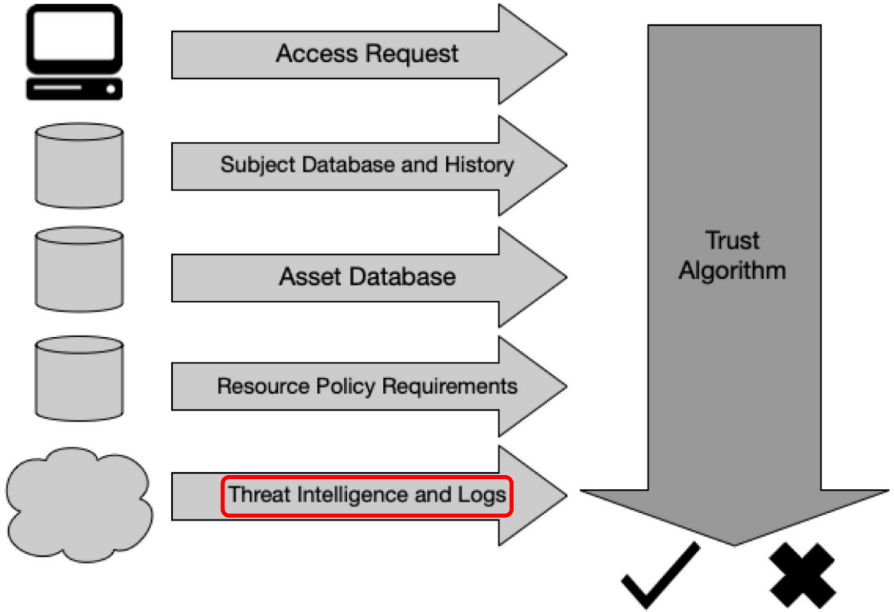
Access Request: Info about what is being requested and by whom

Subject Database and History: Who is requesting and their past behavior

Asset Database: Trusted device list

Resource Policy Requirements: rules for accessing the resource

Threat Intelligence and Logs: Info about current threats



[6]

Trust Algorithm

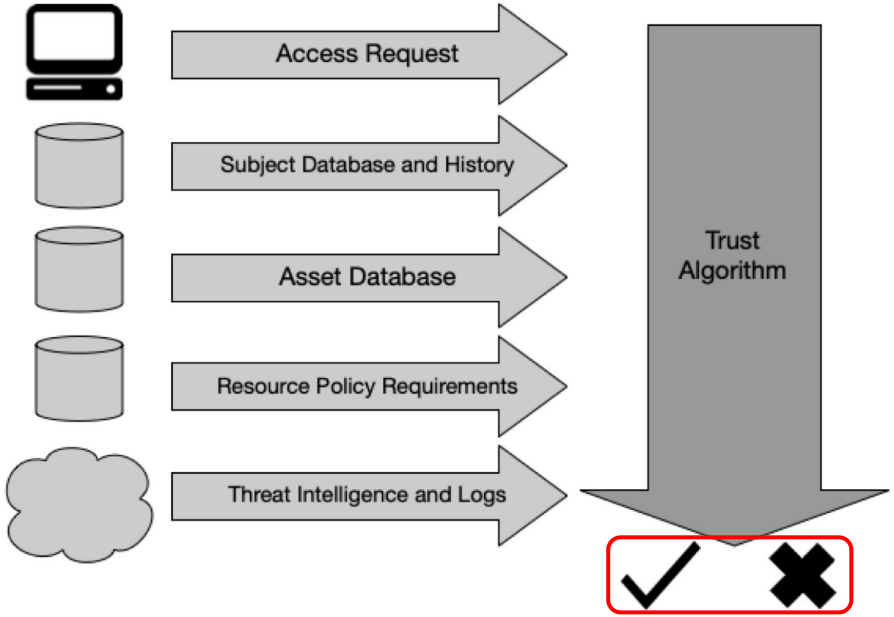
Access Request: Info about what is being requested and by whom

Subject Database and History: Who is requesting and their past behavior

Asset Database: Trusted device list

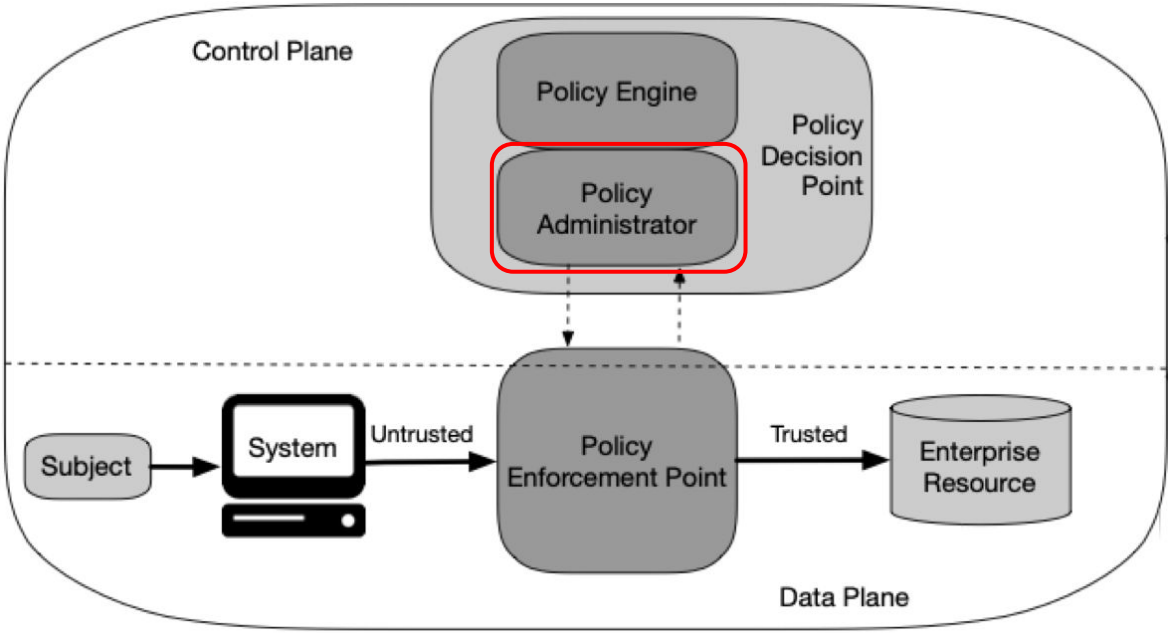
Resource Policy Requirements: rules for accessing the resource

Threat Intelligence and Logs: Info about current threats



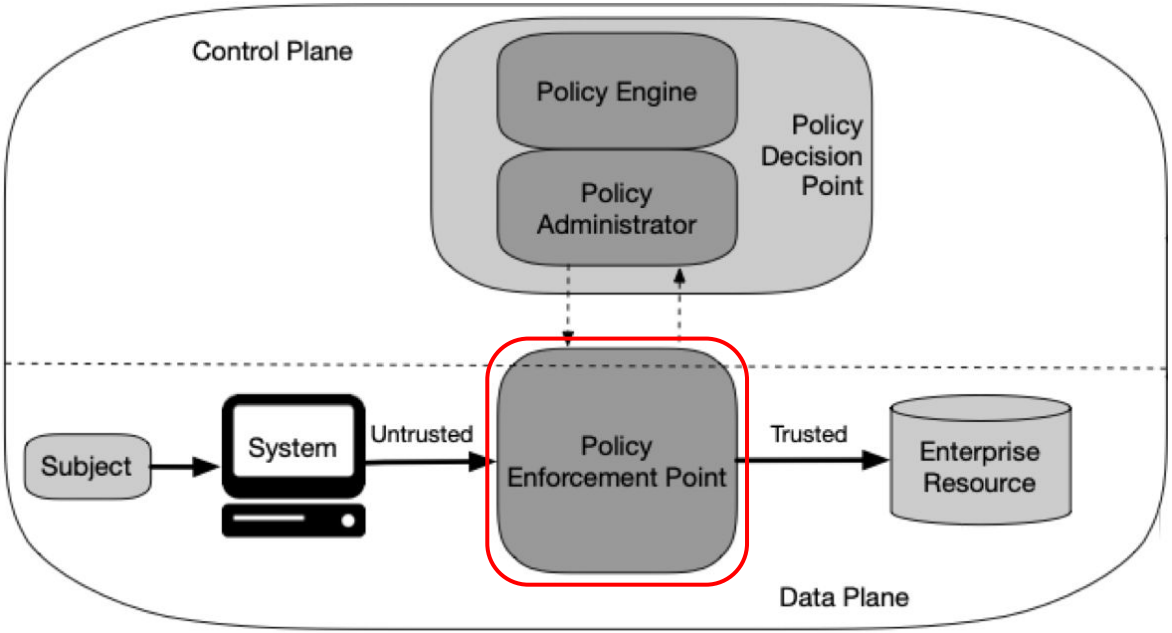
[6]

Policy Administrator (PA)



[6]

Policy Enforcement Point (PEP)



[6]

Key ZTA Ransomware Mitigation Strategies

- Least Privilege Access and Identity Based Controls
- Continuous Monitoring and Behavioral Detection
- Micro-Segmentation and Containment

Least Privilege Access and Identity Based Controls

- Users get only the access they need
- Access tied to verified identity
- Enforced with authentication (e.g., MFA)
- Limits attacker capabilities if compromised

Continuous Monitoring and Behavioral Detection

- Monitor activity in real time
- Detect unusual behavior patterns
- Identify threats early
- Enable rapid response and containment

Continuous Monitoring: Objective & Experimental Setup

- **Objective**
  - Develop a machine-learning–powered security monitoring system using Wazuh to improve threat detection and reduce false positives
- **Setup**
  - 15,427 security events from a simulated enterprise environment
  - Data preprocessed and labeled by threat level
  - Tested on realistic multi-endpoint infrastructure

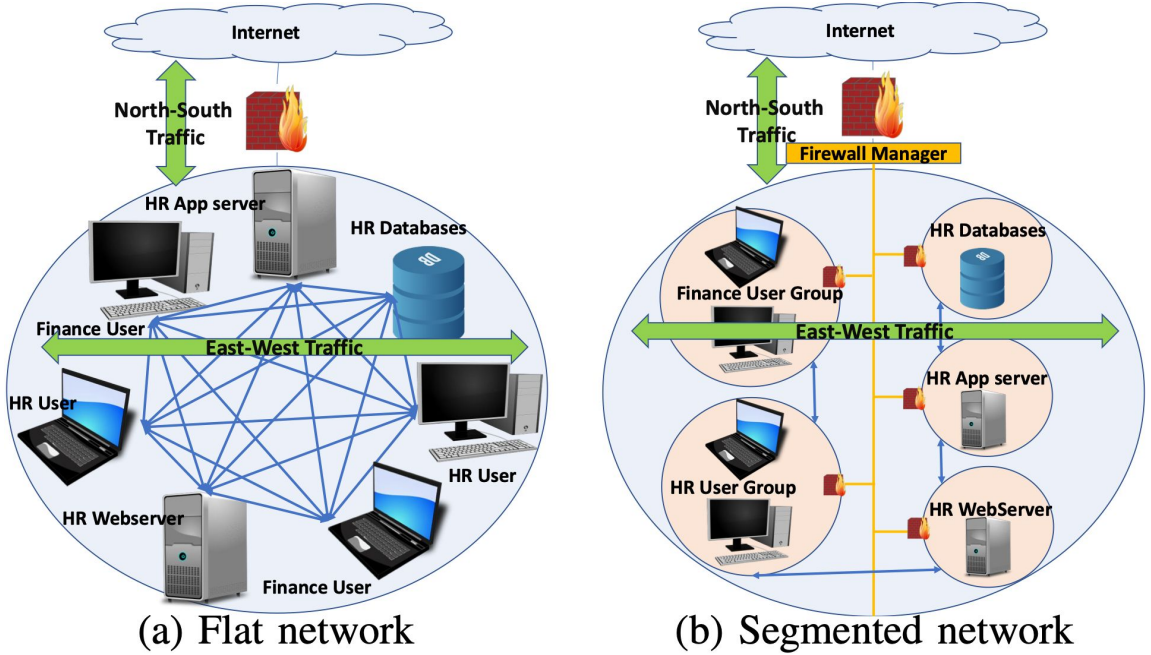
[2]

Continuous Monitoring: Experimental Results

- **Overall Accuracy:** 97.2%
- **Real-Time Response:** Critical alerts processed in less than 100 ms
- **Throughput:** Up to 500 events per second
- **False Positives:** 5%, improving analyst efficiency

[2]

Micro-Segmentation and Containment



[1]

Micro-Segmentation: Objective & Experimental Setup

- **Objective**
  - Measure how micro-segmentation improves network security
- **Setup**
  - Modeled enterprise networks as graphs (nodes = assets, edges = connections)
  - Compared flat vs. micro-segmented networks
  - Used real enterprise data (university + healthcare network)
  - Analyzed via simulations/attack graphs

[1]

Micro-Segmentation: Experimental Results

- Allowed connections reduced by more than **99%**
- Average paths to high-value targets **doubled**
- Successful attack opportunities cut by **~93%**
- Entry points for attackers reduced by more than **65%**
- Limits ransomware spread to a single segment, enabling faster containment

[1]

Combining ZTA Methods: Objective & Experimental Setup

- **Objective**
  - Evaluate how Zero Trust improves ransomware detection and containment
- **Setup**
  - Built a controlled lab to simulate ransomware
  - Implemented a working system
    - Monitor, Detect, Block
  - Used a benign ransomware script to safely mimic real attack behavior

[3]

Combining ZTA Methods: Experimental Results

- **Rapid detection:** ransomware identified in ~5.3 seconds
- **Effective containment:** ~80% of files protected; lateral movement blocked
- **High alert accuracy:** all malicious events flagged; no false positives
- **Micro-segmentation & least privilege:** prevent escalation and network spread

[3]

Challenges and Limitations of ZTA

- Complex policy management
- Performance & system overhead
- Integration complexity
- Legacy & adoption barriers
  - Older systems not designed for Zero Trust
  - Cost, training, and infrastructure upgrades

Conclusion

- Ransomware is an evolving and costly threat
- Traditional perimeter security is insufficient
- Zero Trust Architecture mitigates risk via:
  - Least privilege access & identity verification
  - Continuous monitoring & behavioral detection
  - Micro-segmentation to contain attacks
- Implementation requires careful planning and resources

References

[1] Nardine Basta, Muhammad Ikram, Mohamed Ali Kaafar, and Andy Walker. 2022. Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework. In NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. 1–7. doi:10.1109/ NOMS54207.2022.9789888

[2] Samir Achraf Chamkar, Mounia Zaydi, Yassine Maleh, and Noreddine Gherabi. 2025. Improving Threat Detection in Wazuh Using Machine Learning Techniques. Journal of Cybersecurity and Privacy 5, 2 (2025). doi:10.3390/jcp5020034

[3] Atharva Dhumal, Mustafa Ghaleb, Samah Abdelsalam, Arghir-Nicolae Moldovan, and Mosab Hamdan. 2025. Zero Trust Architecture for Ransomware Defense in Virtualized Environment. In Proceedings of the IEEE/ACM 12th International Conference on Big Data Computing, Applications and Technologies (BDCAT '25). Association for Comput- ing Machinery, New York, NY, USA, Article 24, 7 pages. doi:10.1145/3773276.3774876

[4] Muhammad Liman Gambo and Ahmad Almulhem. 2025. Zero Trust Architecture: A Systematic Literature Review. Journal of Network and Systems Management 34, 1 (Nov. 2025). doi:10.1007/s10922-025-09998-x

[5] Microsoft Threat Intelligence. 2022. Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself. https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

[6] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. 2020. Zero Trust Architecture. Technical Report Special Publication (SP) 800-207. National Institute of Standards and Technology (NIST), Gaithersburg, MD. doi:10.6028/NIST.SP.800-207

[7] SOPHOS. 2026. https://www.sophos.com/en-us/content/state-of-ransomware

Questions?