



Zero Trust in Action

ISC2 East Bay Chapter
March 2025



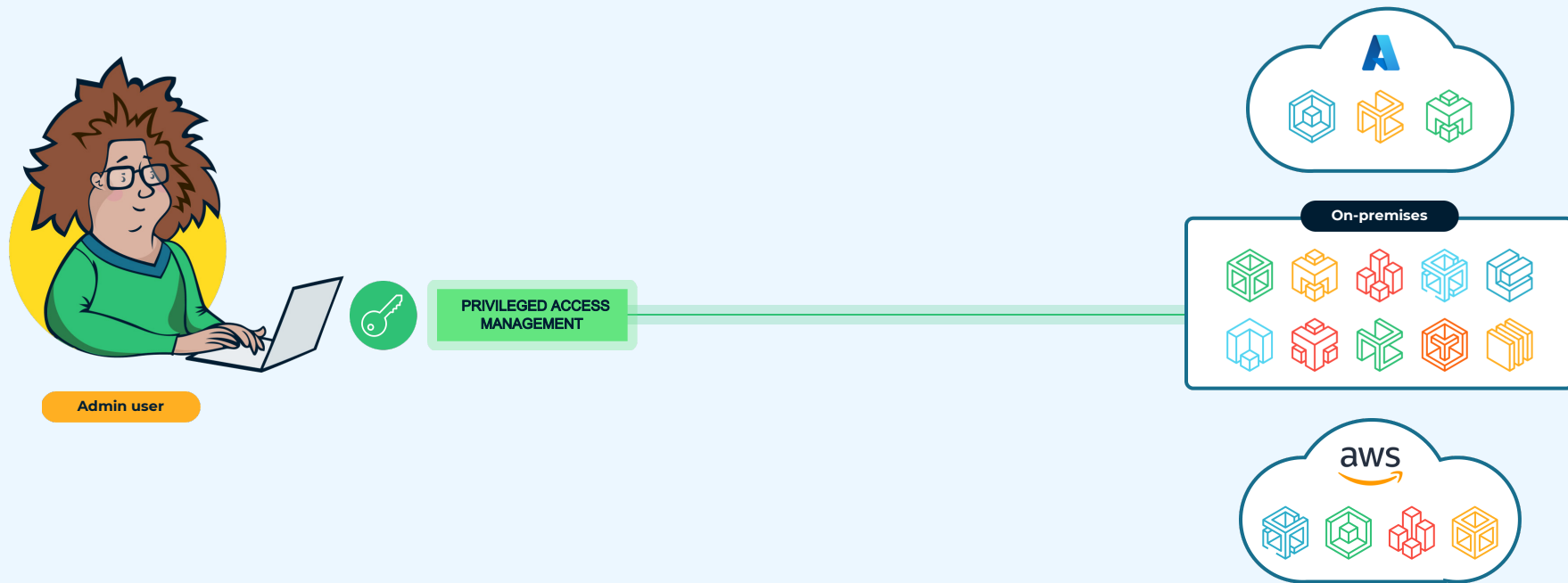
EAST BAY



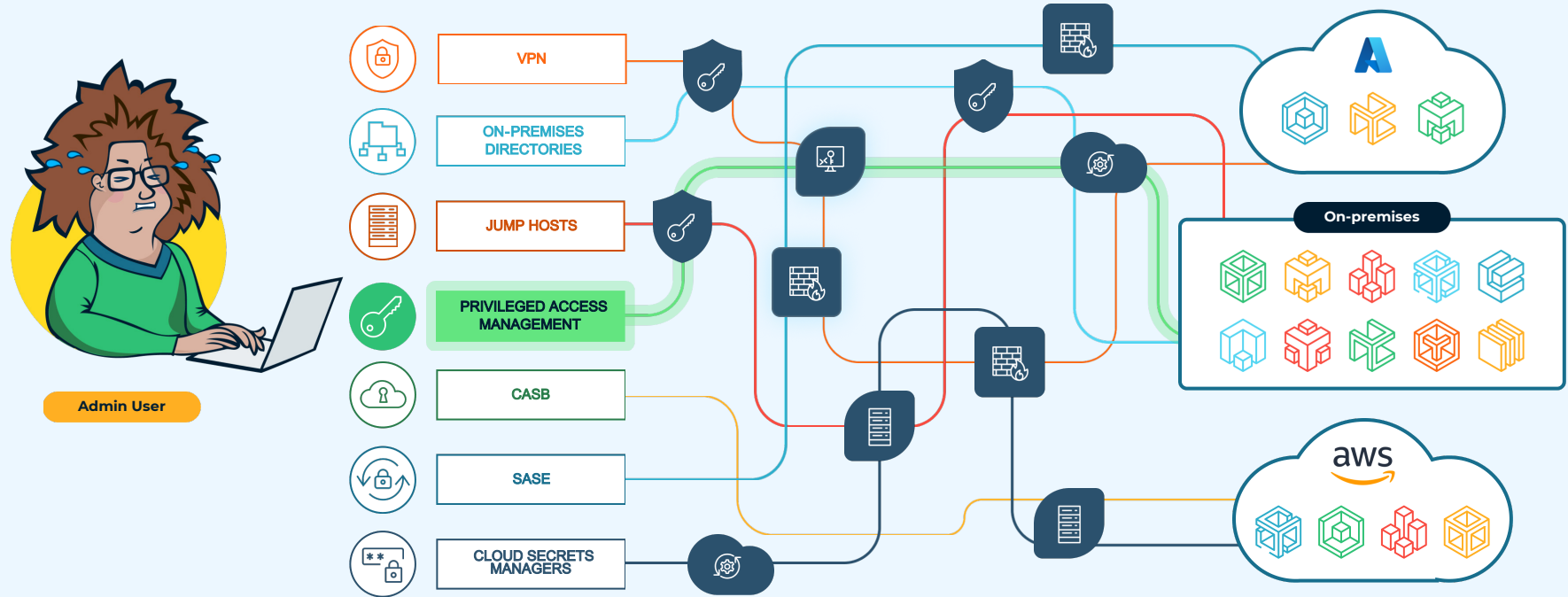
John Martinez
Technical Evangelist

Let's talk about PAM

What PAM Promised



...But, Is this your Privileged Access Experience?



Let's Talk About Zero Trust

CISA Zero Trust Pillars

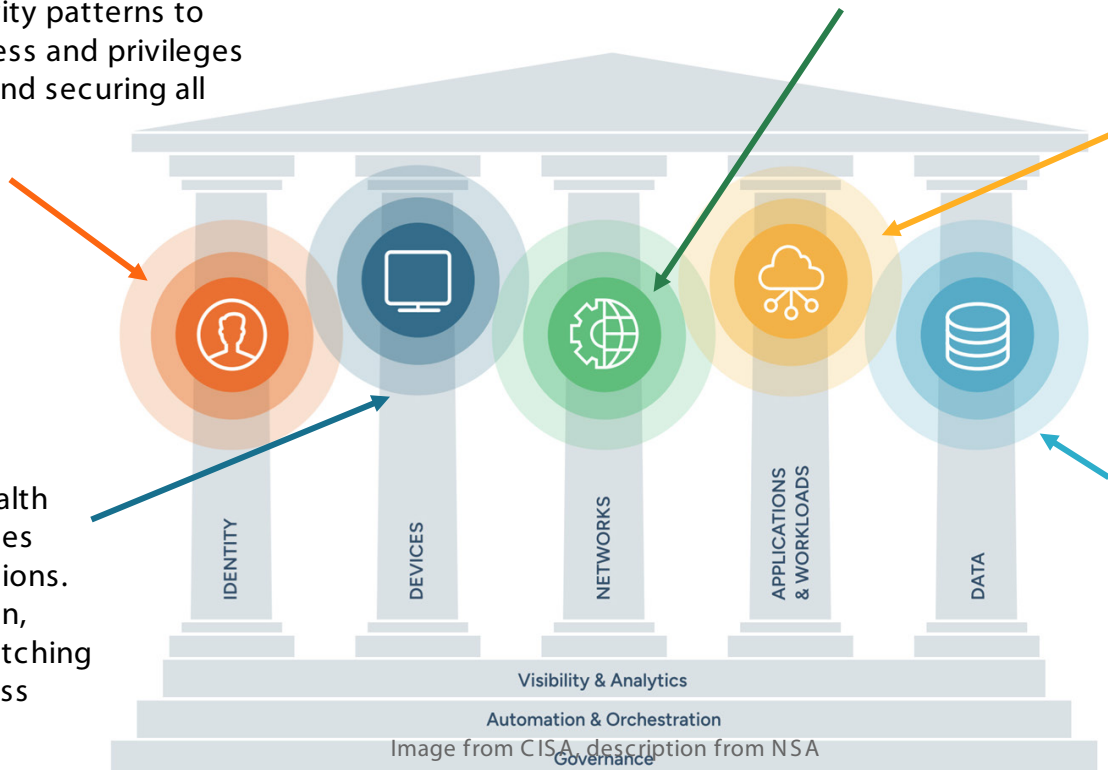
Continually authenticate, assess and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

Segment, isolate and control (physically and logically) the network environment with granular access controls.

Secure everything from applications to hypervisors to include the protection of containers and virtual machines.

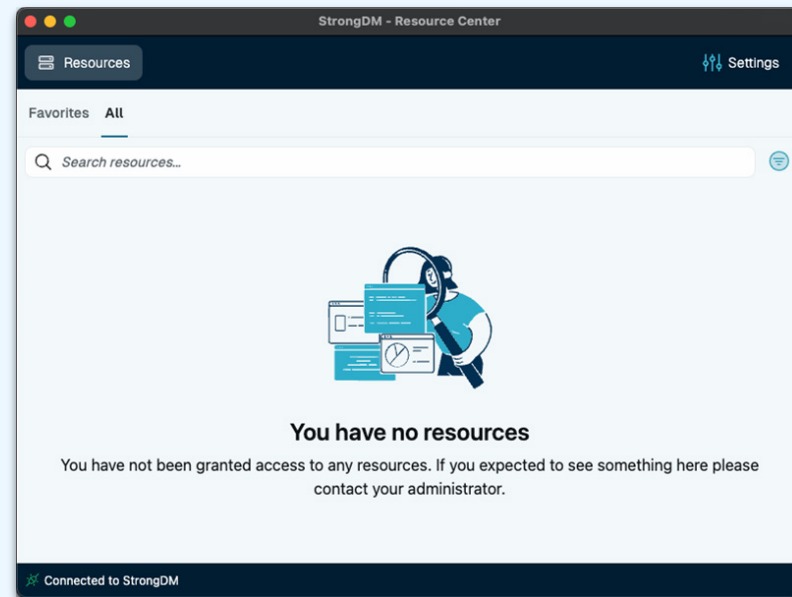
Understand the health and status of devices to inform risk decisions. Real time inspection, assessment and patching informs every access request.

Data transparency and visibility is enabled and secured by enterprise infrastructure, applications and standards, robust end-to-end encryption, and data tagging.



The Ultimate Least Privilege is Zero Standing Privileges

That means when you log into your work laptop in the morning and see zero resources available to you...



Assume a hostile environment: Too much of a good thing?



Assume breach with continuous assessment of actions



Never Trust, Always Verify, & Verify Explicitly

☐ Trust the user (**who**)

- IDP(s) integration
- StrongAuth

☐ Trust the device (on **what**)

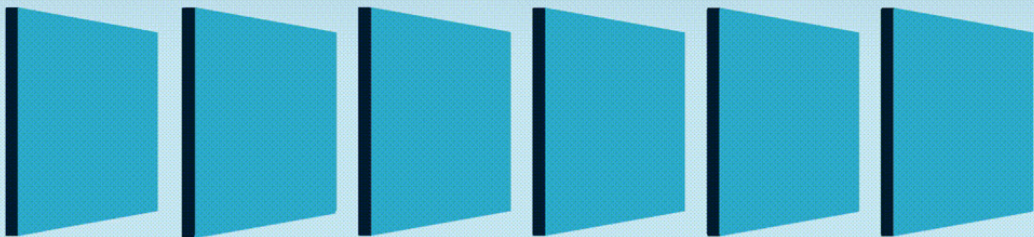
- Endpoint verification
- EPP/EDR integration

☐ Trust the context (**where, when**)


- IP Address
- Time


☐ Trust the action (**what**)


- Is the action okay?





EVERYTHING & ANYTHING


 MAINFRAMES


 DATABASES


 WINDOWS & UNIX SERVERS

 CLOUDS

 KUBERNETES

 WEB APPS

 ROUTERS & SWITCHES

 SIM/SIEM/SYSLOG

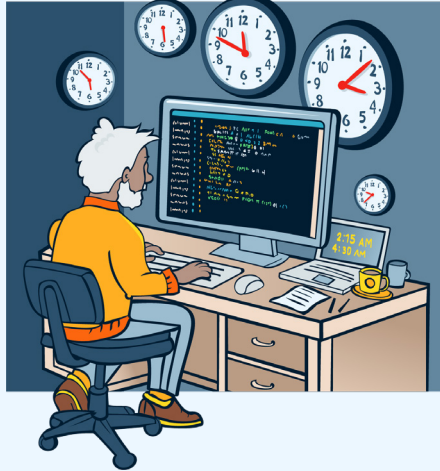
Our evolving threat landscape necessitates more Zero Trust

On-start & context -lite authorization is failing us

Malware Kicks Off Mid -Session



Tasks Performed at
Odd Hours



Actions that Require
Additional Approvals



A Note on Security frameworks

Great to understand, but you need a plan for reacting to breaches in real time.

- MITRE ATT&CK
TTPs are a good place to start thinking like an attacker
- **NEW: MITRE D3FEND**
Good techniques to detect and contain attacks
- CIS DB Benchmarks
All about hardening your databases
- OWASP Top 10
Focuses on Web apps, with information on injection risk

The logo for DEFEND, featuring the word "DEFEND" in a stylized, bold, sans-serif font with a trademark symbol (TM) to the upper right.The logo for MITRE ATT&CK, with "MITRE" in blue and "ATT&CK" in red, both in a bold, sans-serif font, with a trademark symbol (TM) to the lower right.The logo for OWASP, featuring a stylized fly icon inside a circle on the left, followed by the text "OWASP" in a bold, sans-serif font.The logo for CIS Center for Internet Security, featuring a blue circular graphic on the left, followed by the text "CIS" in a bold, sans-serif font, and "Center for Internet Security" in a smaller, sans-serif font to the right, with a registered trademark symbol (®) at the end.

Practical Steps Towards Zero Trust Access

Requirements First! *for Zero Trust Privileged Access*



Breadth of Coverage



Ease of Use and Developer Workflow Integration



Auditing / Reporting for Compliance



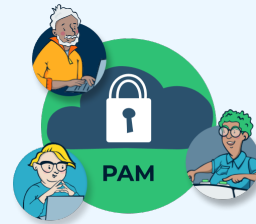
Context -Based Continuous Authorization



JIT & ZSP




Real-Time Visibility and Monitoring



Multi -Cloud and Hybrid Environment Support

Step 1: Identify and Prioritize High -Risk Resources

What to Do:

- Map out all privileged resources (databases, Kubernetes, cloud instances, on-prem servers).
 - Assess risk levels based on sensitivity, regulatory impact, and exposure.
- 

High-Risk Resources & Critical Systems

- Production Databases & Servers
- Financial Systems
- Intellectual Property Repositories
- Infrastructure Management Tools
- Systems Outside of Current PAM Deployments

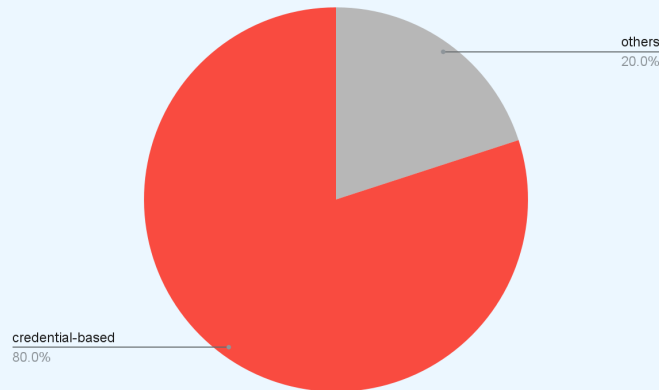
Breadth of coverage ensures every privileged operation across resources is accounted for.

Step 2: Eliminate Standing Access to Reduce Risk

What to Do:

- Grant access only when requested for a specific task and revoke it immediately after.
- Implement approval workflows integrated into existing systems (e.g., Slack, ServiceNow).

ZSP and automated JIT access workflows minimize the attack surface without disrupting operations.



80% of breaches
can be attributed to
stolen privileged credentials

Step 3: Use Real-Time Context to Enforce Policies

What to Do:

- Create policies that take context into consideration.
- Monitor real-time signals like device posture, geolocation, time of day, and user behavior & actions.
- Ensure access is revoked and sessions are terminated if trust conditions fail during a session (e.g., device becomes non-compliant).

Continuous authorization ensures policies dynamically adapt without manual intervention.

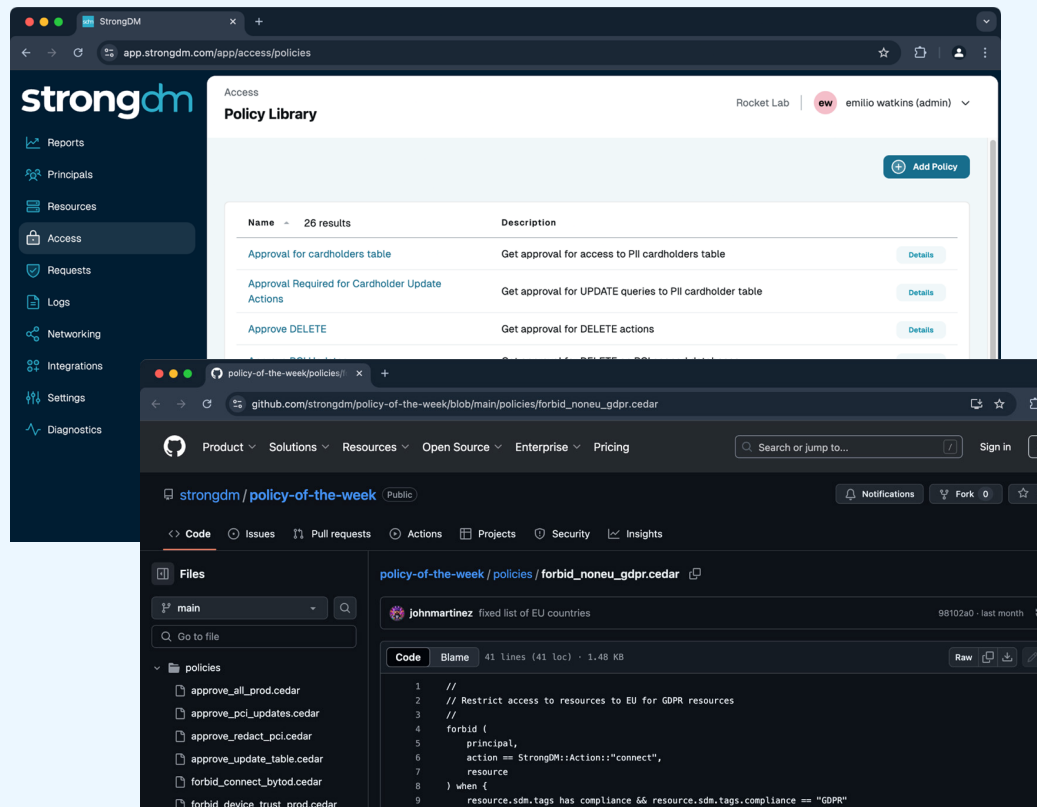


Step 4: Unify & Automate Policy Management Across Environments

What to Do:

- Centralize policy management so policies are enforced across cloud, Kubernetes, and on-premises environments.
- Automate policy updates and reviews to ensure they remain aligned with evolving business needs.

Centralized, unified policy management ensures consistency and reduces operational overhead.



Step 5: Monitor Privileged Activity and Optimize Policies

What to Do:

- Audit every privileged action and flag anomalies.
- Use insights to optimize policies, reduce (or increase) friction, and improve security.

Real-time logging and monitoring provide actionable intelligence for immediate response and compliance reporting.

Logs

Rocket Lab | ew emilio watkins (admin) ▼

Activities

Q after:2025-01-16T23:20:33.644Z × → Filter by: Actor ▼ Dates ▼

Date	IP	Activity	Description	User Agent
Jan 23 2025 11:15:02 PM	75.140.152.175	Access request to resource denied	emilio watkins (emilio.watkins@reaction-time.org) denied access to resource prod-rocketlab-postgresql (ADMIN) for emilio watkins (emilio.watkins@reaction-time.org) via workflow Production. The reason for the denial was "You are unauthorized for this access".	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Jan 23 2025 11:14:44 PM	75.140.152.175	Access requested to resource	emilio watkins (emilio.watkins@reaction-time.org) requested access to resource prod-rocketlab-postgresql (ADMIN) via workflow Production for this reason: "DB Maintenance".	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Jan 23 2025 10:32:16 PM	75.140.152.175	Policy updated	emilio watkins (emilio.watkins@reaction-time.org) updated policy Forbid Access unless in Approved Role	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36

StrongDM Zero Trust Policies

Cedar Policy Language: Fine-grained Authorization

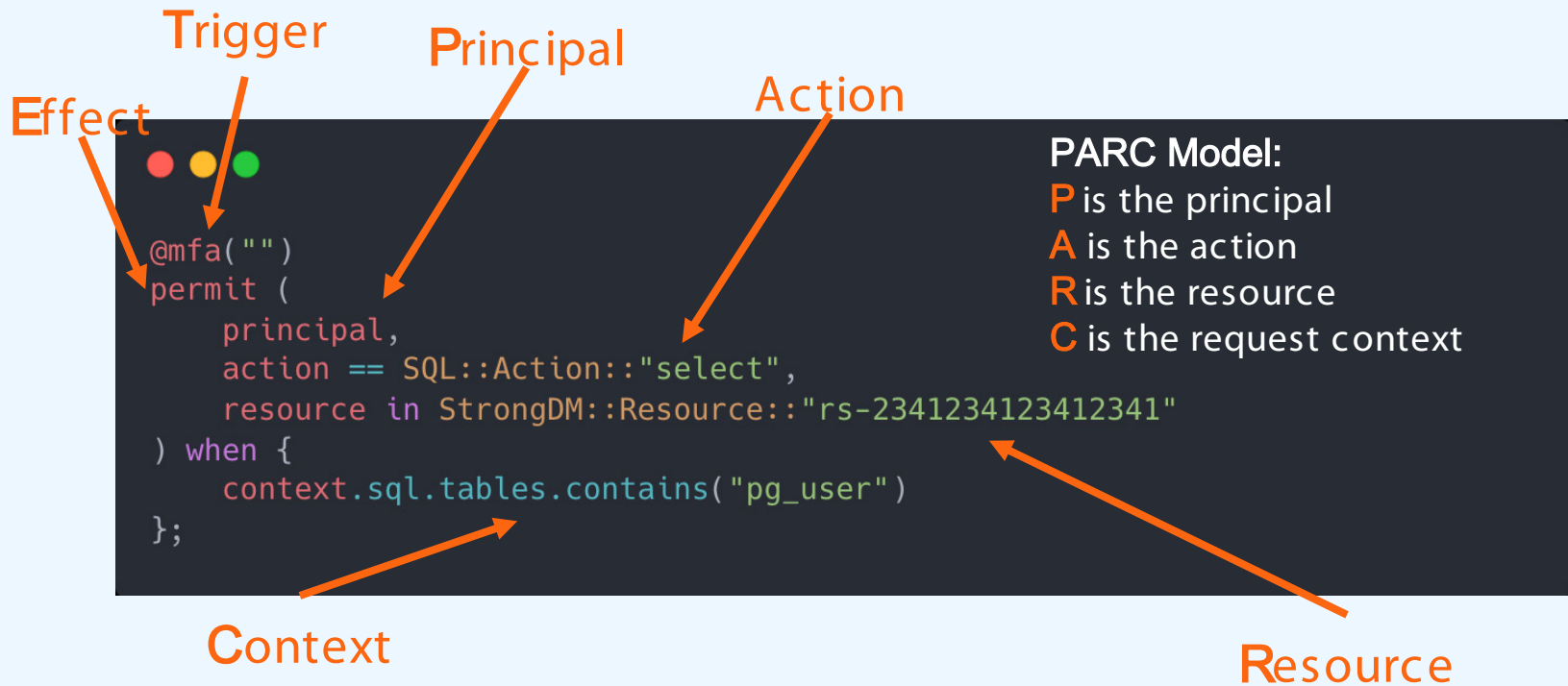
The Cedar Policy Language is:

- Expressive
- Human-readable
- Extremely performant
- Built for scale
- Open Source

<https://www.cedarpolicy.com/>



How do StrongDM Policies implement granularity?





Forbid and Revoke
Sessions to Prod
Resources from
Unhealthy Endpoints



MFA for Database Actions

StrongDM Zero Trust PAM

Zero Trust policy -based action control: Unparalleled precision in *dynamic* privileged action control for any infrastructure or application.

- **Frustration -free access:** Enable users to securely access the resources they need to get their job done without frustration.
- **Stop Unsanctioned Actions:** On demand access reduces the attack surface and eliminates excess privileges. Continuous detection and mitigation instantly blocks harmful actions.
- **Continuous Compliance:** Policy-based action control ensures real-time, verifiable Zero Trust compliance.

Questions?

Thank you!
Let's Connect

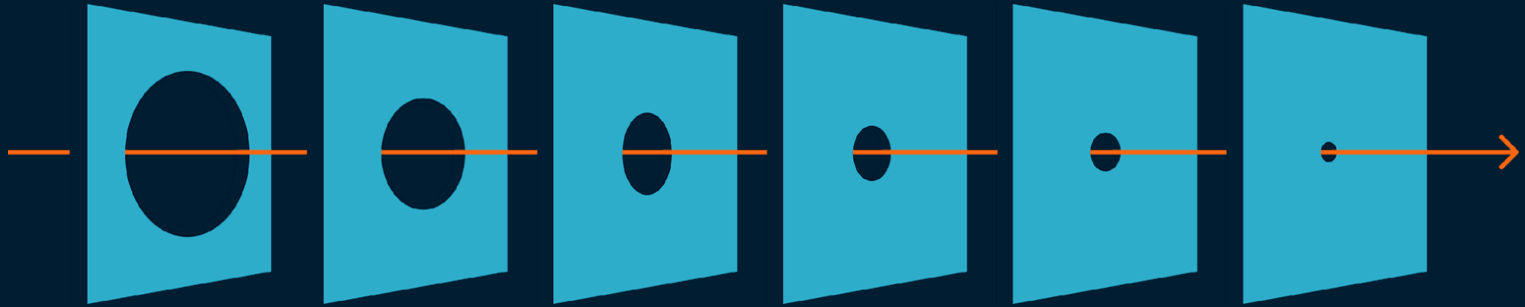


John Martinez

Technical Evangelist | Leadership |
Mentorship & Coaching



Let's look at more examples!



Restricting Access by IP Address

Use Case: Using a user's IP address as a way to permit or forbid access to a resource

Protection: Restricting connections to resources from a specific network location (e.g.: within a cloud network)

- MFA required for DB connection
- Restricts access to production SSH servers
- Helps prevent lateral movement in the network

```
@mfa("")
permit (
    principal,
    action == SQL::Action::"connect",
    resource
) when {
    context.location == Location::IP::"192.0.2.1"
};
```


Resource Objects as an Attribute

Use Case: Resource objects such as database tables, can be referenced for precision

Protection: Restricting actions to specific database tables based on security policy, best practices, or compliance

- MFA required for **SELECT** query
- **pg_user** table is scoped
- Helps prevent exfiltration of database users for stolen credential attacks

```
@mfa("")
permit (
    principal,
    action == SQL::Action::"select",
    resource in StrongDM::Resource::"rs-2341234123412341"
) when {
    context.sql.tables.contains("pg_user")
};
```

Approval Workflow for Database Actions

Use Case: Require approvals for database record updates for PCI data.

Protection: Restricts potentially destructive actions on sensitive data.

- Require approval via workflow
- UPDATE database action
- Restrict on sensitive cardholders data table
- Use resource tag attributes to identify resources

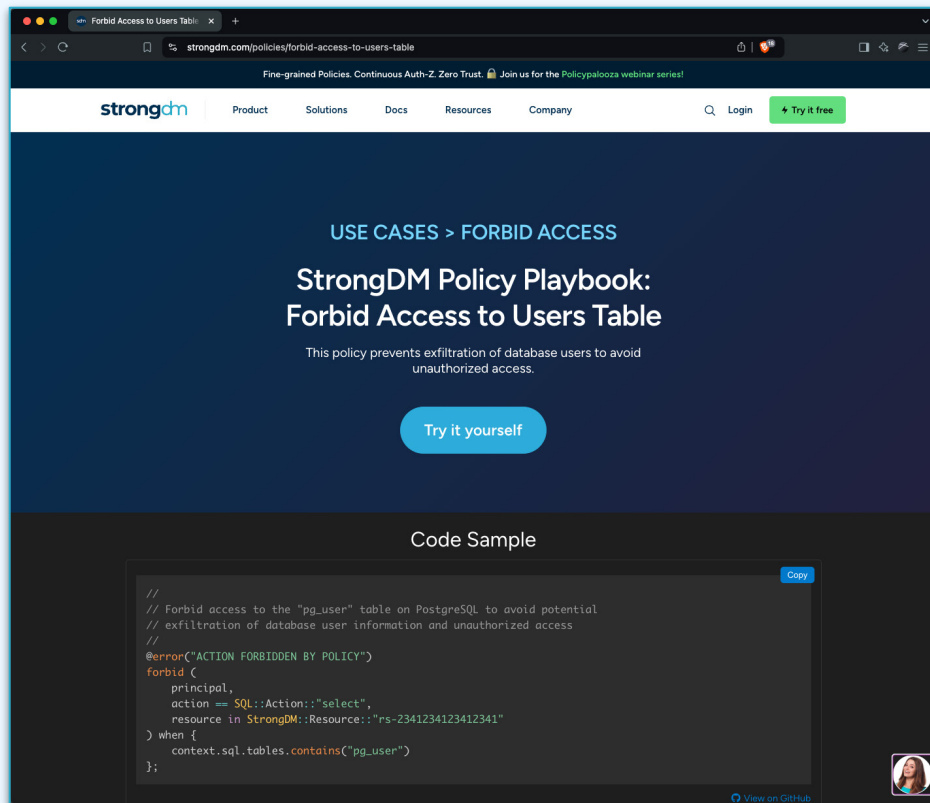
```
//  
// Require approval for UPDATE actions on PCI "cardholders" table  
//  
@approve("af-2341234123412341")  
permit (  
    principal,  
    action == SQL::Action::"update",  
    resource in StrongDM::Resource::"rs-2341234123412341"  
) when {  
    context.sql.tables.contains("cardholders") &&  
    (resource.sdm.tags has "compliance" && resource.sdm.tags["compliance"] =  
"true") &&  
    (resource.sdm.tags has "regulation" && resource.sdm.tags["regulation"]  
== "pci")  
};
```

We're just Scratching the Surface: StrongDM Policy Playbooks

What are they?

Real-world StrongDM policies published weekly, with examples of how you can mitigate adversarial tactics and prevent unauthorized access and use of your sensitive data.

<https://www.strongdm.com/policies>



StrongDM Zero Trust

