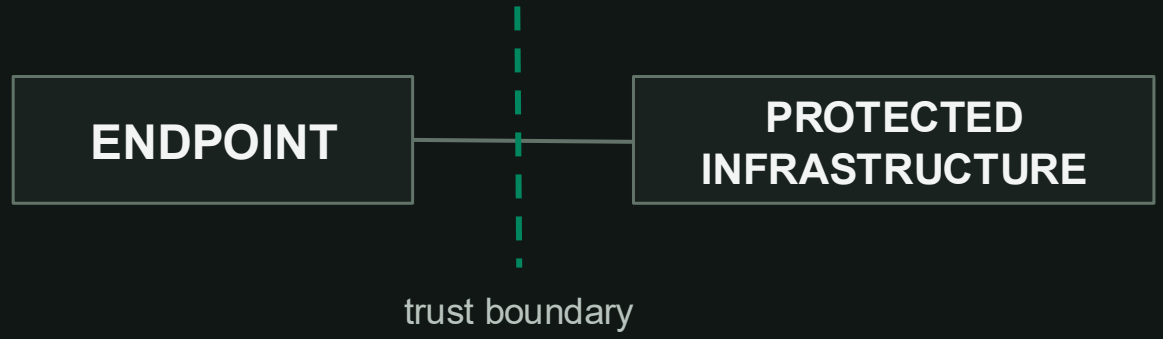
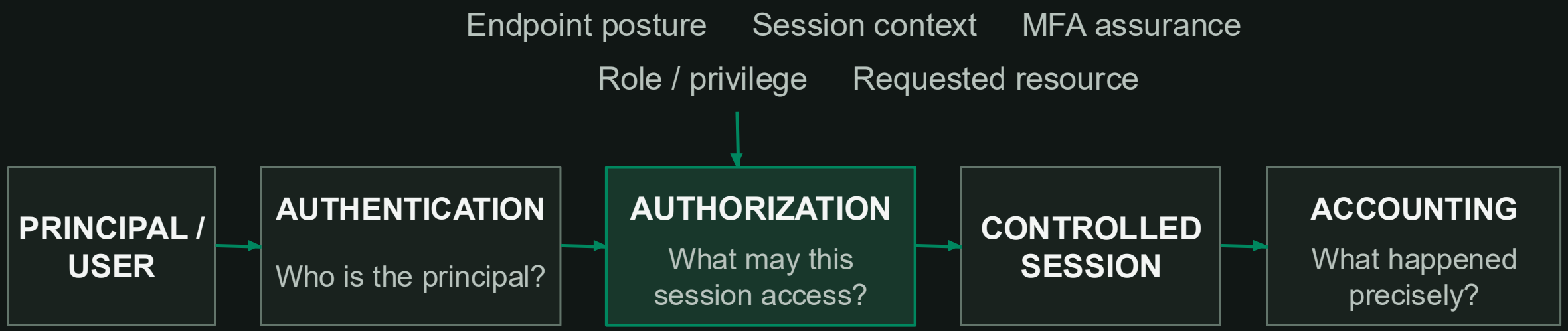
The VPN Is Not the Trust Boundary

Designing Remote Access for Untrusted Endpoints

Rohan Puranik
President
KIZATEL
rohan@kizatel.com



AAA Does Not Authenticate Your Laptop’s Innocence



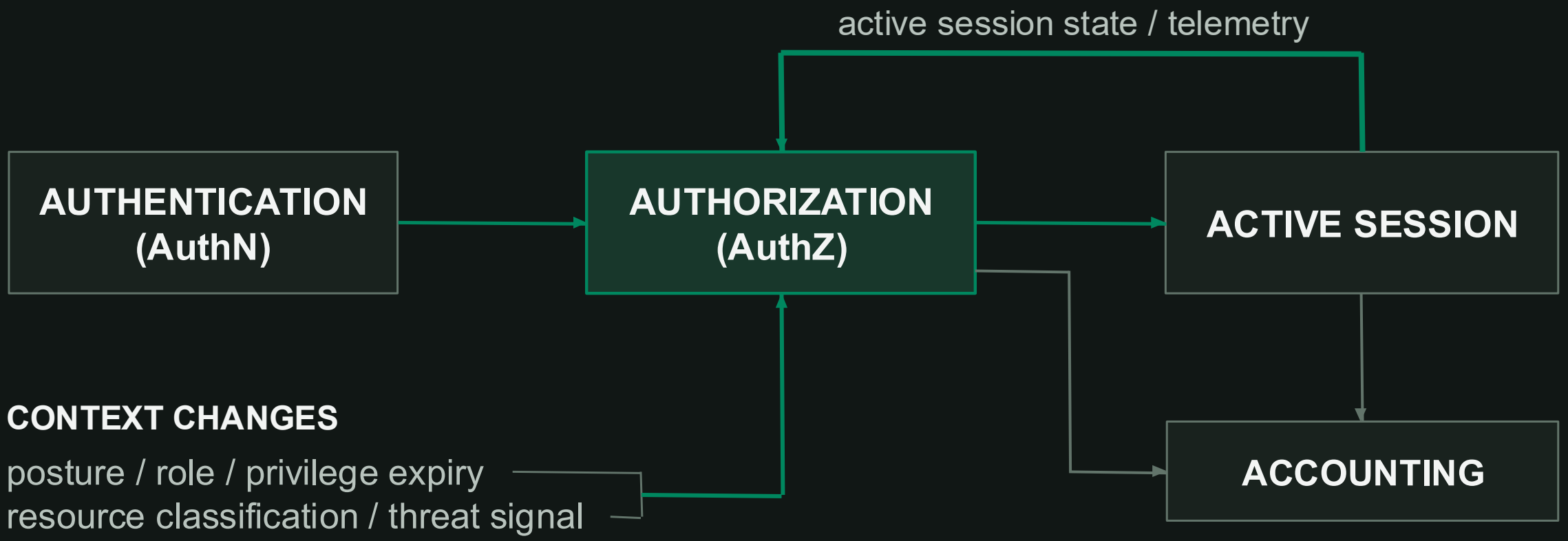
Authenticated principal: YES

Endpoint integrity:
NOT ESTABLISHED BY AuthN

AAA: Authentication, Authorization, Accounting MFA: Multi-factor authentication

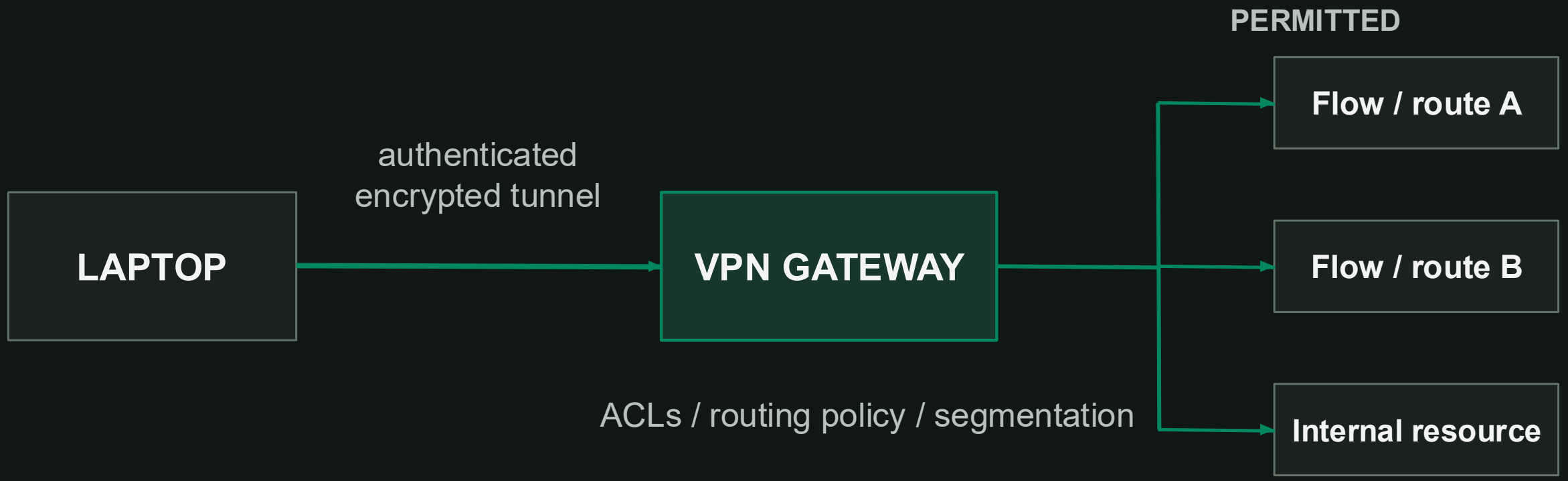
> **Successful authentication establishes confidence in the principal.**
> **Endpoint integrity remains a separate authorization input.**

Authorization Is Revisable State



Authorization must not freeze at login.

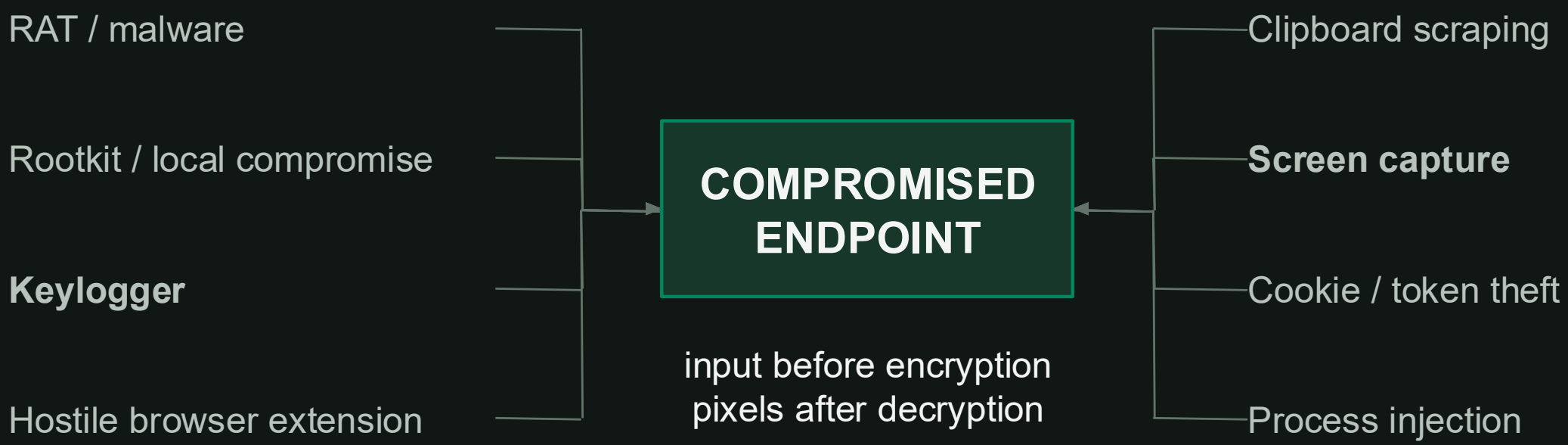
What Does a VPN Actually Grant?



The endpoint still originates packets toward permitted resources.

> **Secure transport is not the same thing as a trustworthy endpoint.**

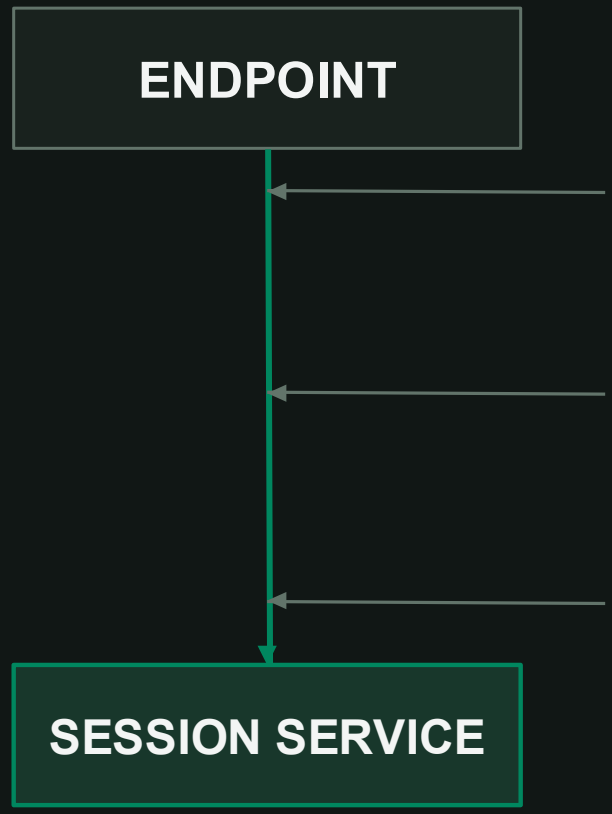
Attack Surface I — The Endpoint



Encryption may begin too late to protect information already captured inside a compromised endpoint.

Security is risk reduction, not proof of invulnerability.

Attack Surface II — The Path and the Session



THREAT	DEFENSIVE CONCEPT
MITM attempt / hostile or rogue network	→ Authenticated peer identity + authenticated encryption
Replay attempt	→ Freshness / anti-replay protection
Stolen session material	→ Short-lived scoped credentials + re-authentication / revocation

MITM: Man-in-the-middle
PKI: Public key infrastructure (supports peer identity)

The network path can be defended cryptographically.
Endpoint compromise and session theft remain separate risks.

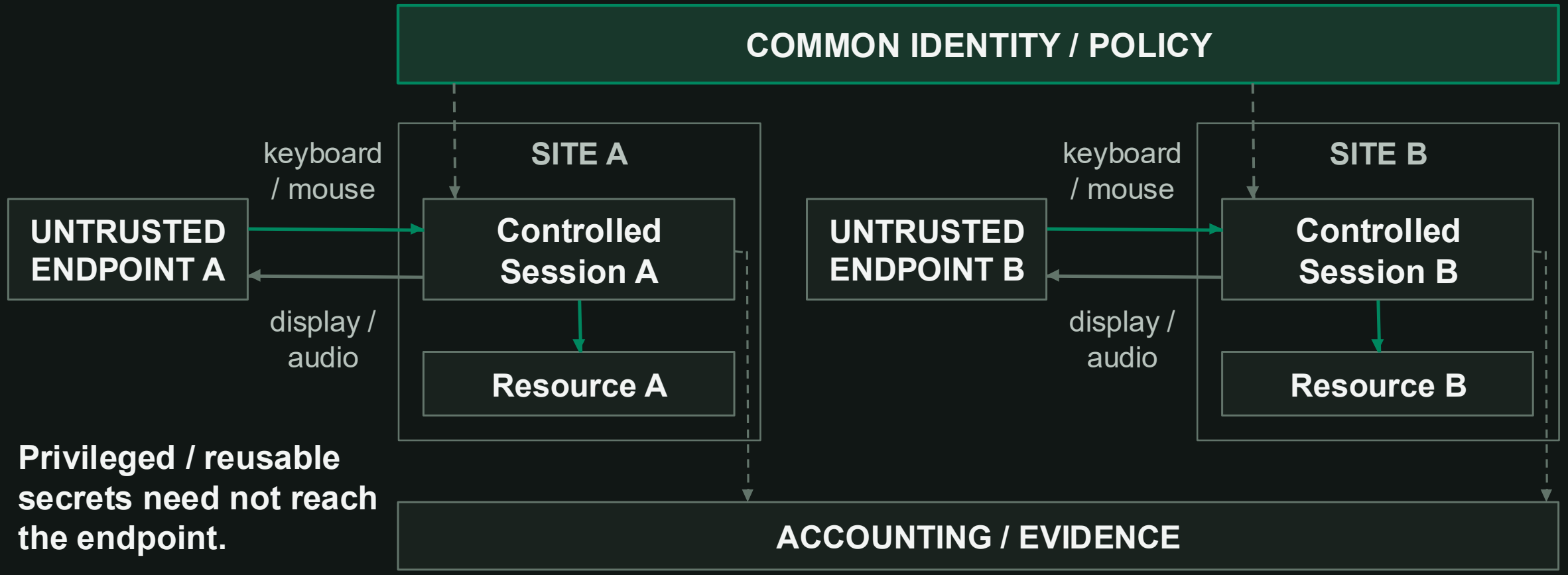
After Authentication: Assume Breach in 2026

VALID CREDENTIALS	Stolen account / VPN credentials	→	**Accepted login***
COMPROMISED HOST	RAT / backdoor	→	**Remote commands / covert tunnel**
LEGITIMATE SERVICE	HTTPS / WebSocket / MQTT / Matrix	→	**Possible command-and-control**
INTERNAL FOOTHOLD	Credentials / RDP / privileged access	→	**Lateral movement / persistence**

* If the attacker satisfies the required factors or reuses accepted session material.

An attacker may wait for the user to complete MFA.
Prevent one compromise from becoming unrestricted trust.

Move the Work, Not the Trust Boundary



Execution location can be a security decision.

Authorize the Session and Resource — Not Merely the Network

Identity

Phishing-resistant MFA

Endpoint posture

Role / privilege level

Requested resource

Session state



SESSION 147 — EFFECTIVE POLICY

Resource A	**PERMIT**
Resource B	**DENY**
Admin network	**DENY**
Clipboard	**DENY**
File transfer	**DENY**

Step-up authentication

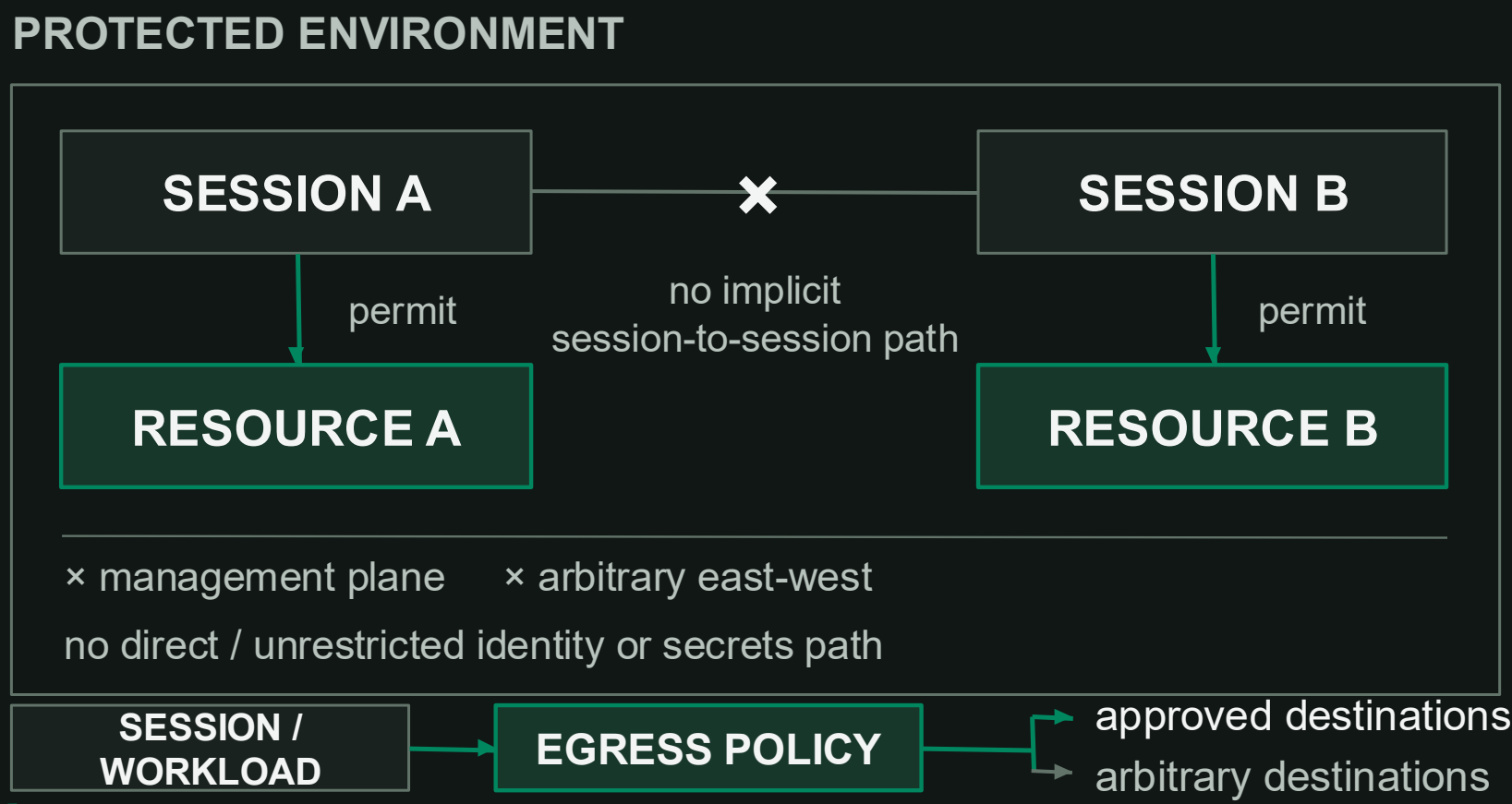
PAM / just-in-time privilege

Short-lived credentials

> **Authentication can remain constant while authorization changes.**

PAM: Privileged Access Management

Contain the Blast Radius



Default-deny east-west

Per-session / per-resource segmentation

Management-plane isolation

Constrained egress

PAM / JIT privilege

A compromised workload is still an incident.
It must not automatically become a bridge to everything else.

Observe, Correlate, Re-Authorize

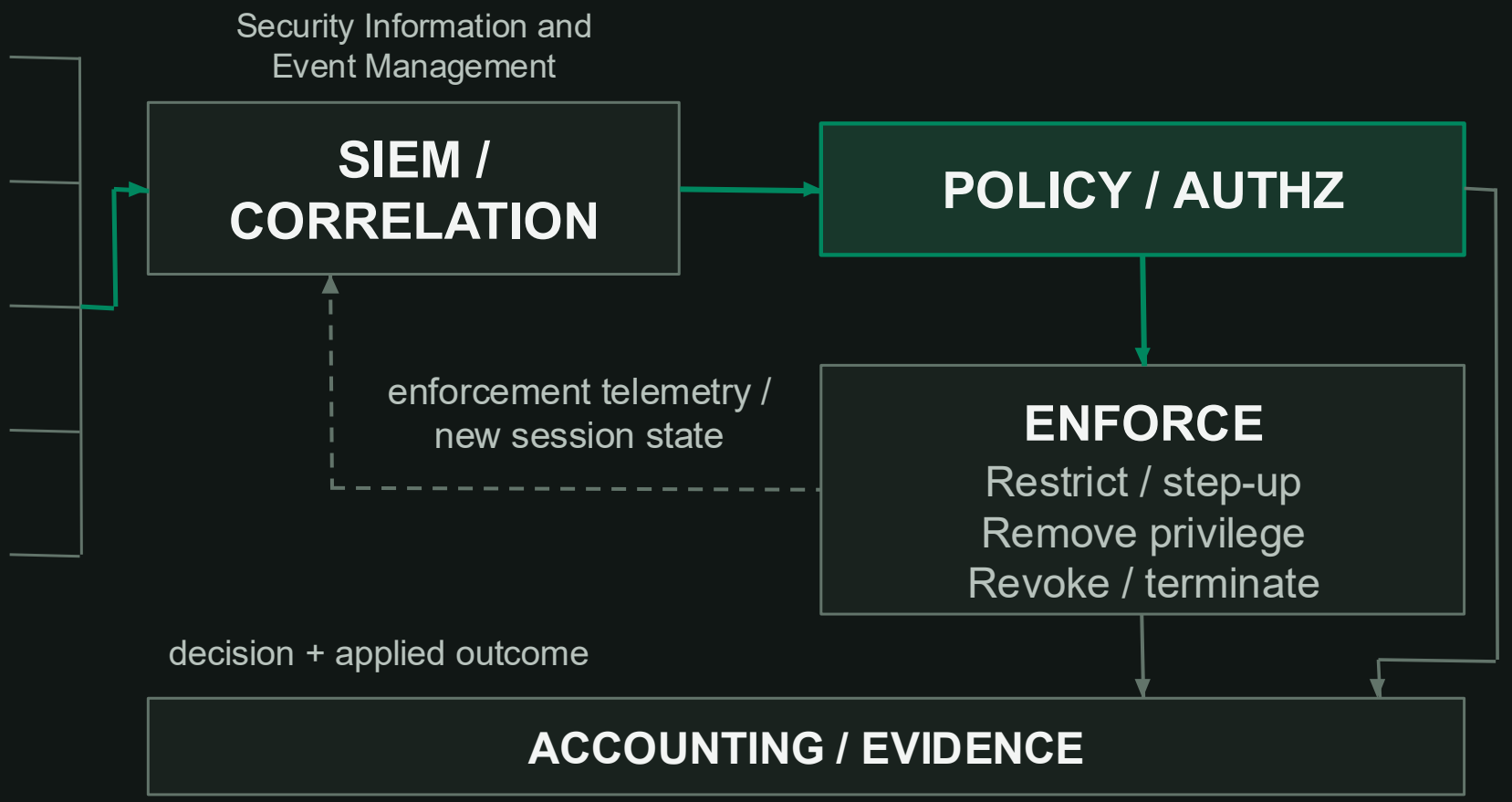
Host / workload telemetry
e.g. Wazuh

Network IDS / flow
Intrusion detection (e.g. Suricata)

PAM privilege events

DAM database activity
Database Activity Monitoring

UEBA risk signals
User and Entity Behavior Analytics



Encrypted payload visibility depends on placement and available telemetry.

The Endpoint Does Not Have to Become Trusted

Authenticate the principal

↓

Authorize the session

↓

Constrain the network

↓

Protect the secrets

↓

Observe continuously

↓

Revoke when context changes

↓

Account for what happened

“An untrusted endpoint does not have to become trustworthy. The architecture has to remain defensible when it doesn’t.”

Authentication establishes identity assurance.
Authorization constrains effective access.
Accounting provides evidence of what occurred.

Reference implementation available for technical discussion.

Rohan Puranik
President
KIZATEL
rohan@kizatel.com