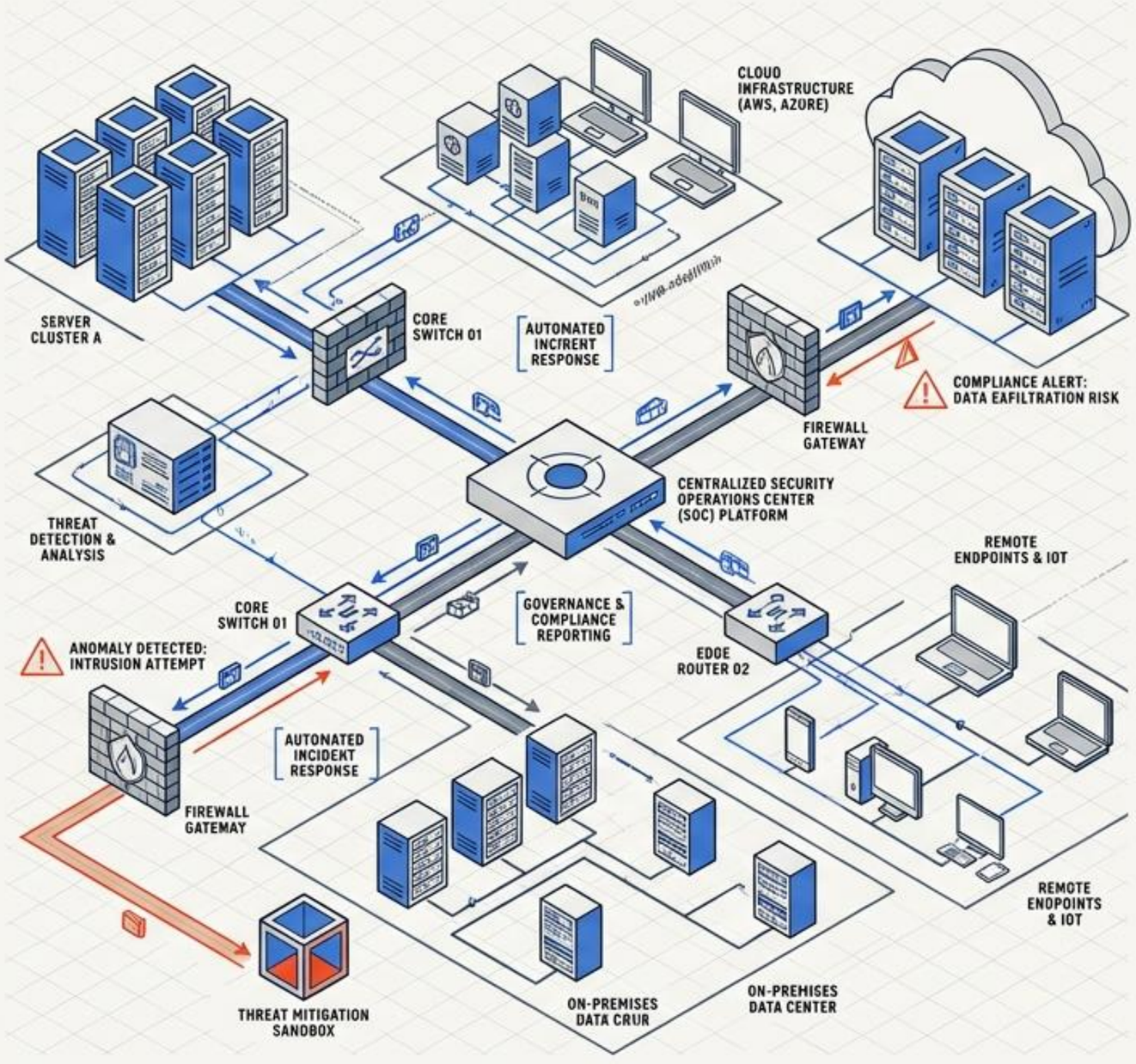
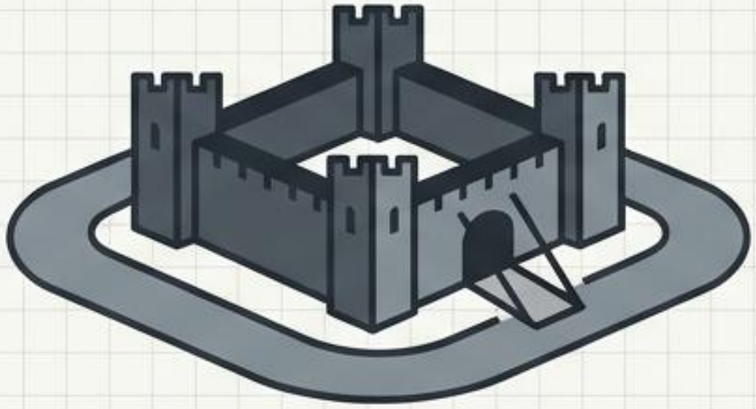
NETWORK SECURITY MANAGEMENT

The Active Defense Playbook: From Governance to Automated Mitigation

Security is not a static product. It is a continuous, dynamic process.

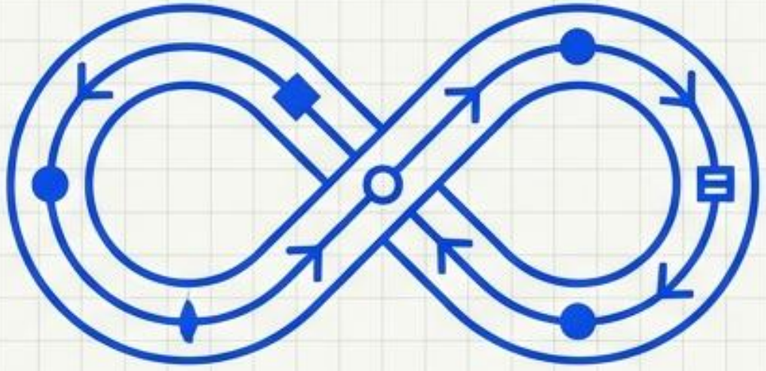


THE PERIMETER MODEL



- Assumes internal trust
- Shattered by remote work and cloud adoption
- Fundamentally fails against zero-day and insider threats

CONTINUOUS RISK MANAGEMENT

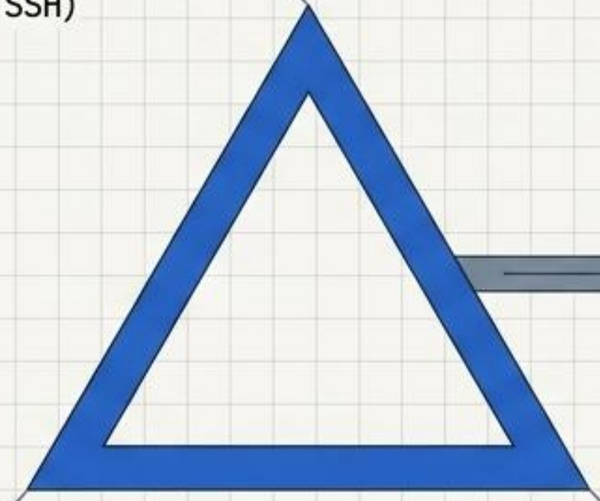


- Absolute security is an operational fallacy
- Objective: Reduce probability and impact to an acceptable business level

TAKEAWAY: SHIFT FROM PURCHASING SECURITY PRODUCTS TO EXECUTING A CONTINUOUS SECURITY PROCESS.

THE CIA TRIAD

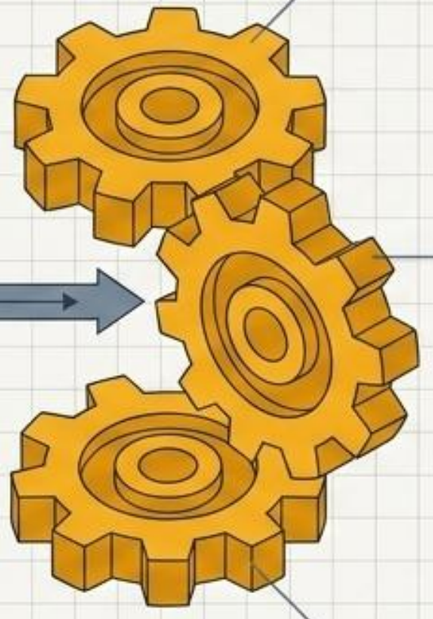
Confidentiality:
Enforcing data privacy
(Encryption via SSH)



Integrity:
Verifying data accuracy
and preventing tampering
(Cryptographic Hashing)

Availability:
Ensuring system uptime
and accessibility
(DDoS defense)

THE AAA FRAMEWORK



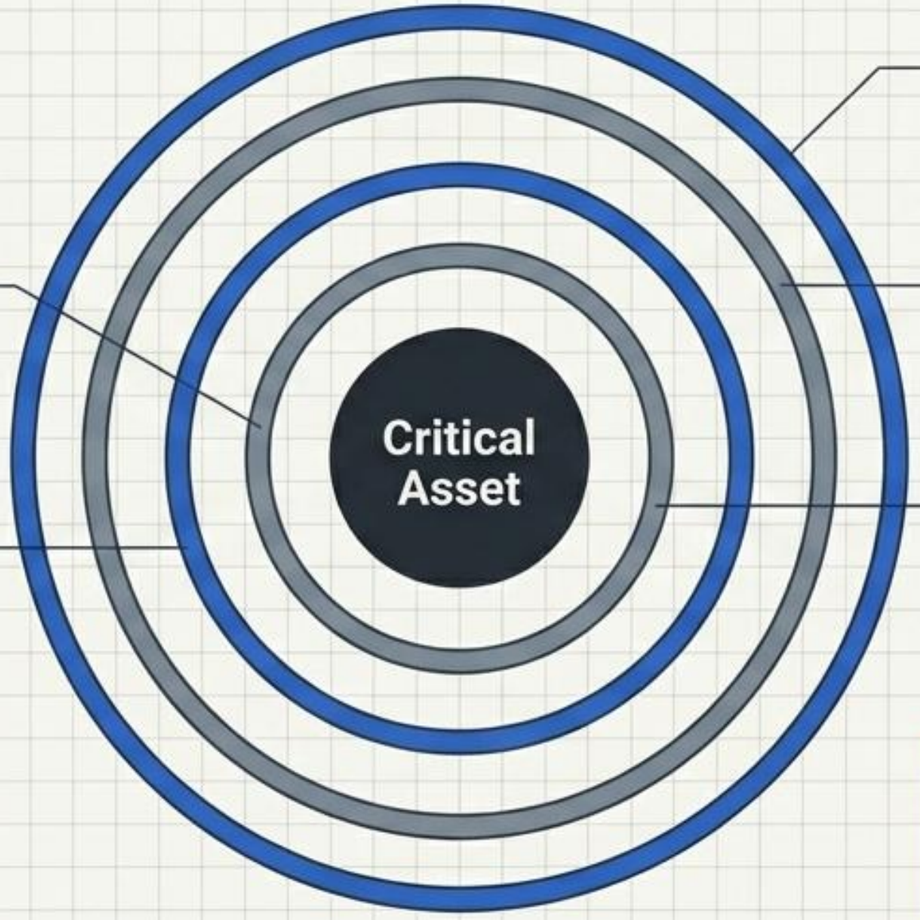
Authentication:
Who are you?
(Identity verification)

Authorization:
What can you do?
(Strict permission
granting)

Accounting:
What did you do?
**(Logging for absolute
non-repudiation)**

Defense in Depth

Single points of failure are unacceptable. Attackers must chain multiple distinct exploits to reach the core.



Layer 1: Perimeter
(External firewalls blocking untrusted Internet traffic)

Layer 2: Network
(VLAN isolation, routing segregation)

Layer 2: Network
(VLAN isolation, routing ACLs, segregation)

Layer 3: Endpoint
(Host-based IDS, localized application monitoring)

Layer 4: Data
(Cryptographic encryption of data at rest)

Principle of Least Privilege (PoLP): Enforced across all layers to mathematically limit the blast radius of any localized breach.


Step 1: Business Strategy & Legal
Defining ultimate organizational goals and regulatory obligations (e.g., HIPAA, PCI-DSS compliance).
Step 2: Risk Assessment
Calculating priority.
Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) × Annualized Rate of Occurrence (ARO).
Step 3: Security Policy
High-level, executive-approved intent written in plain language.
Step 4: Technical Controls
Standards, Guidelines, and step-by-step Procedures.
Step 5: NMS Enforcement
Network Management Systems executing continuous automated auditing of device configurations to prevent drift.

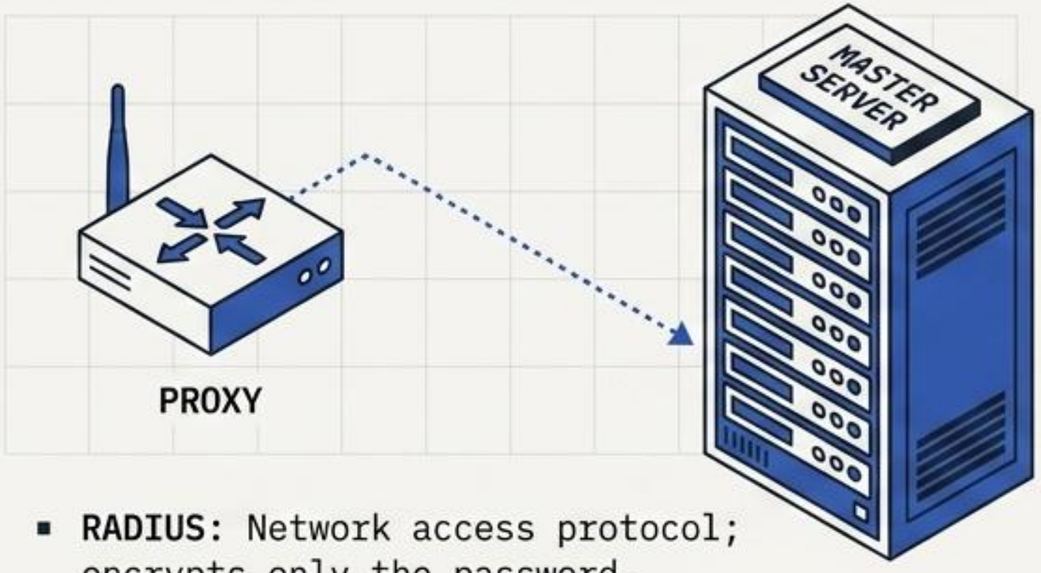
Security Standards (The What)	Security Frameworks (The How)
Nature: Mandatory, compliance-focused, and highly auditable.	**Nature:** Voluntary, methodology-focused, strategic guidance.
Purpose: Establish the minimum acceptable level of protection.	**Purpose:** Guide organizations in building mature, risk-based security programs.
Examples: ISO 27001 (ISMS), PCI-DSS (Payment data), HIPAA (Healthcare).	

Insight: Compliance ≠ Security. You can be 100% legally compliant and still remain highly vulnerable to sophisticated threats.

The Flaw of Local Auth

Managing local databases across 5,000 devices causes massive provisioning overhead and leaves dangerous orphaned accounts when employees exit.

The Centralized Solution

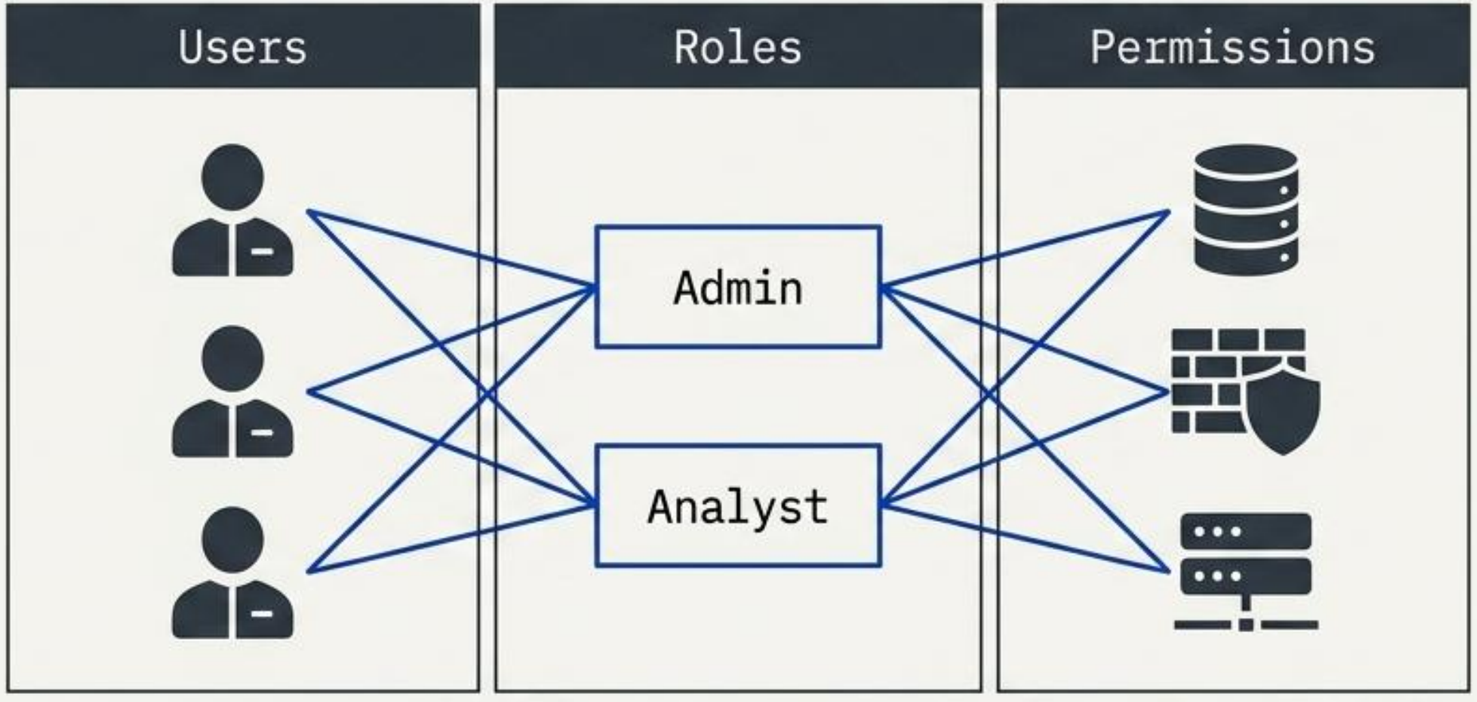


- **RADIUS:** Network access protocol; encrypts only the password.
- **TACACS+:** Device administration protocol; encrypts full payload, separates Auth/Auth.

Multi-Factor Authentication (MFA)

The Problem: Direct mapping of 10,000 users to 500 systems creates 5,000,000 rules. DAC is too loose; MAC is too rigid.

The Solution: Role-Based Access Control (RBAC)



Assign permissions to Job Functions (Roles) rather than individuals.

Operational Wins:

- Simplifies onboarding and deprovisioning.
- Strictly enforces the Principle of Least Privilege (PoLP).
- Ensures Separation of Duties.

1. Prevention (Harden)

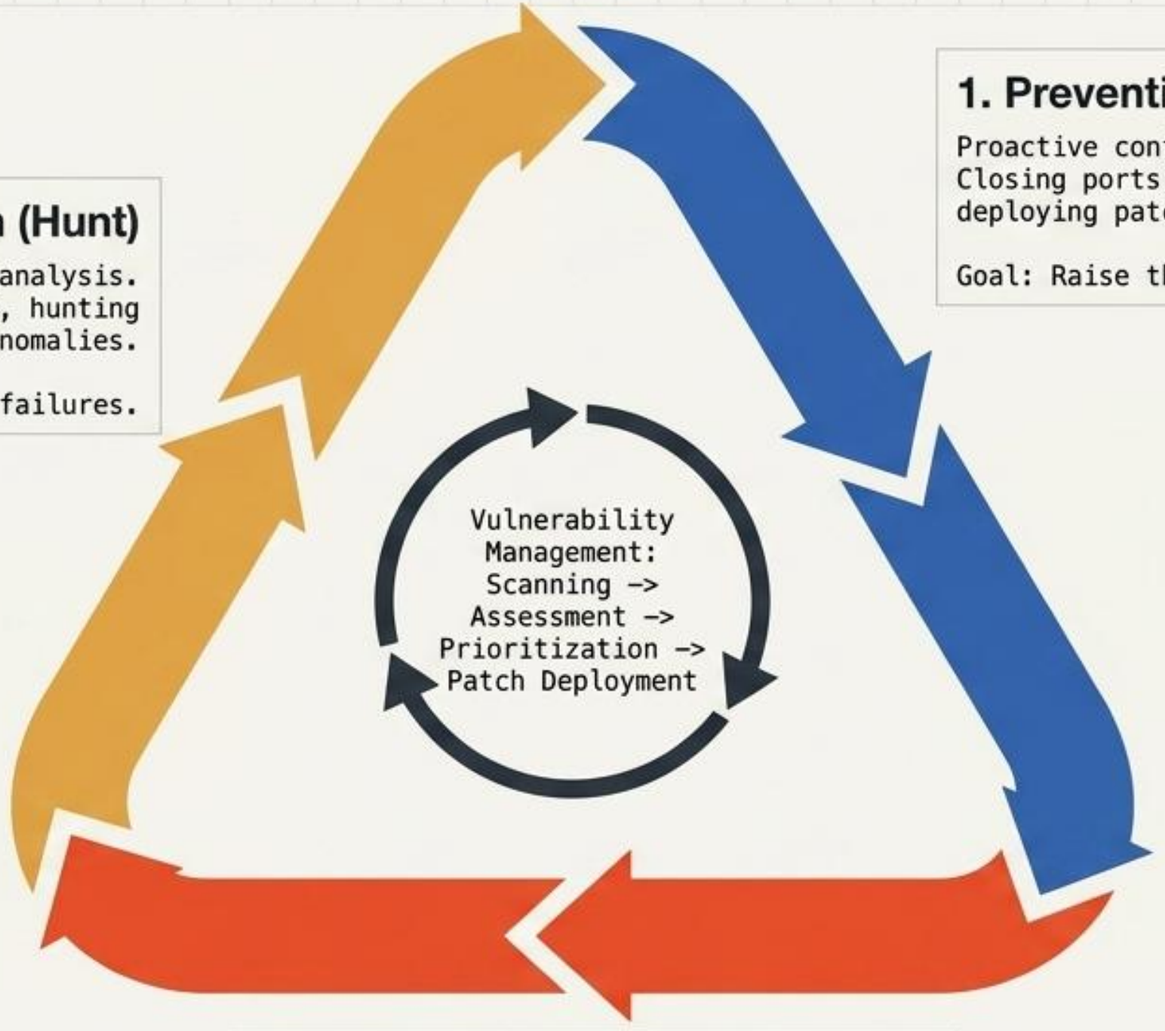
Proactive configuration management. Closing ports, enforcing strong ACLs, deploying patches.

Goal: Raise the attacker's cost of entry.

2. Detection (Hunt)

Continuous telemetry analysis. Baselining normal traffic, WIPS, hunting for anomalies.

Goal: Rapidly identify preventative failures.



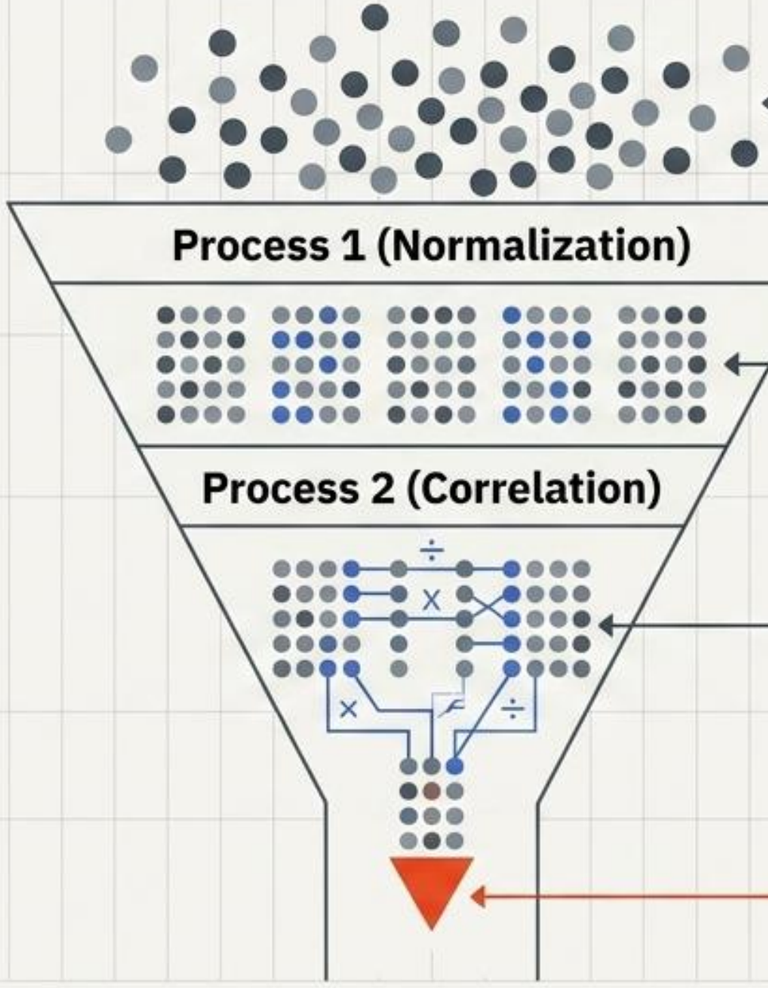
3. Response (Contain)

Tactical intervention. Shutting down switch ports, blackholing IPs, restoring snapshots.

Goal: Minimize downtime and lateral movement.

Audit Trails: Who did what?
(Administrative accountability, NTP-synced time, Non-repudiation)

Security Logs: What is happening?
(Network traffic, blocked connections, Syslog)



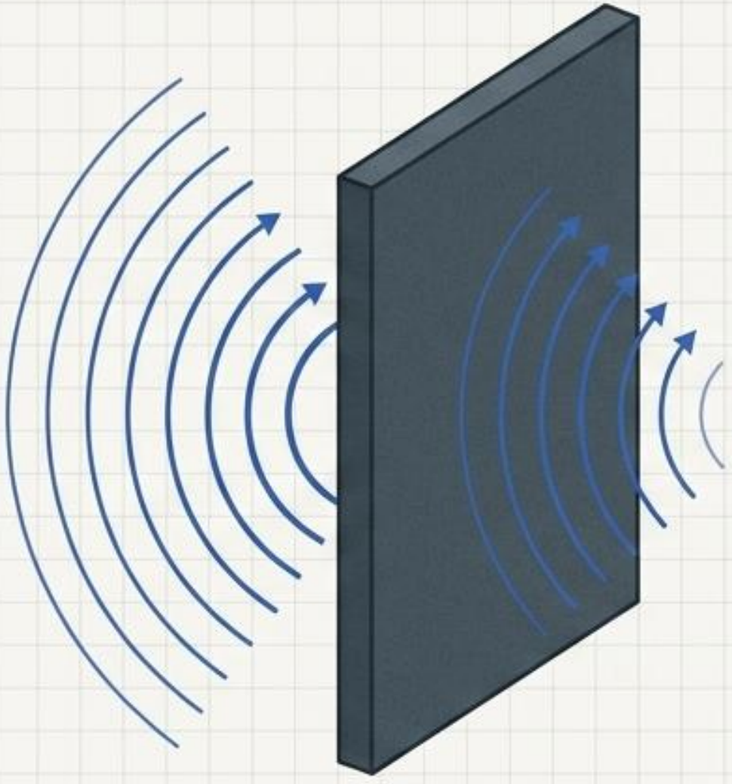
Input: Millions of raw Syslog events from routers, firewalls, and AAA servers.

Translating diverse vendor logs into a unified data structure.

Mathematical algorithms linking disparate events.

Output: A single, high-fidelity, actionable security alarm.

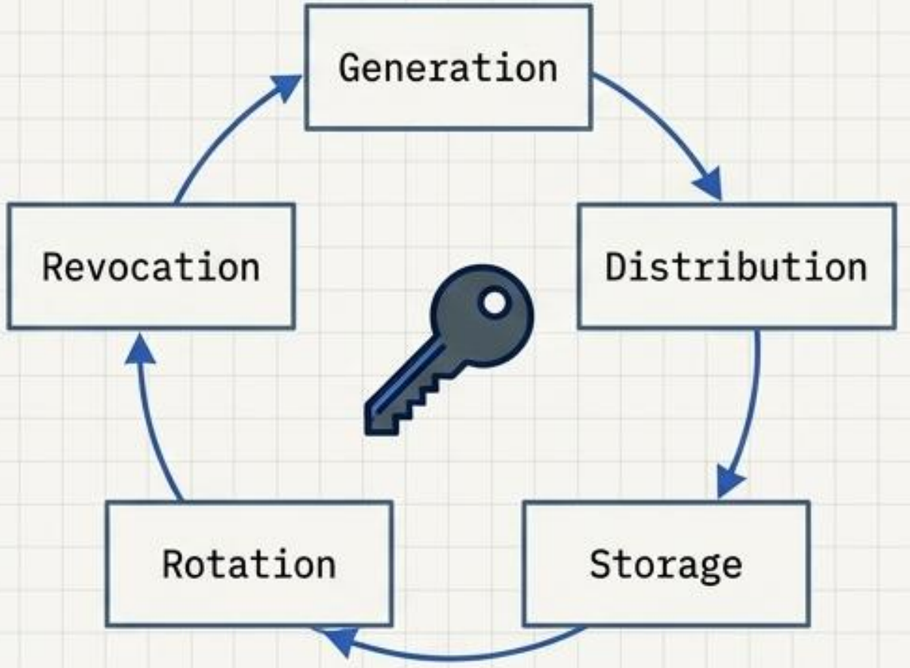
Wireless SecOps



The physical perimeter dissolves. Mitigated via 802.1X Enterprise Auth and WIPS (jamming Rogue APs and Evil Twin broadcasts).

Public Key Infrastructure (PKI)

The operational fragility of cryptography.

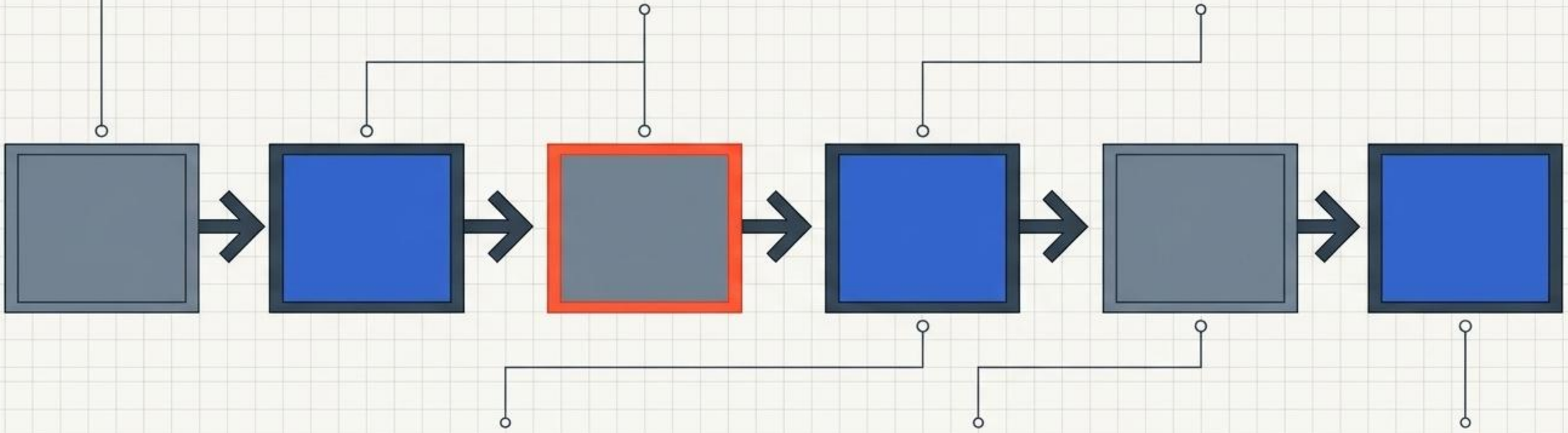


The Danger: Unmonitored certificate expiration is a leading cause of massive, self-inflicted enterprise network outages.

1. Preparation:
Establishing playbooks, deploying IDS, training personnel.

2. Identification:
Validating the event using Signature-based and Behavior-based detection.

3. Containment:
Stopping the bleed. Short-term isolation vs. long-term operational fixes.



4. Eradication:
Removing the root cause (malware deletion, patching).

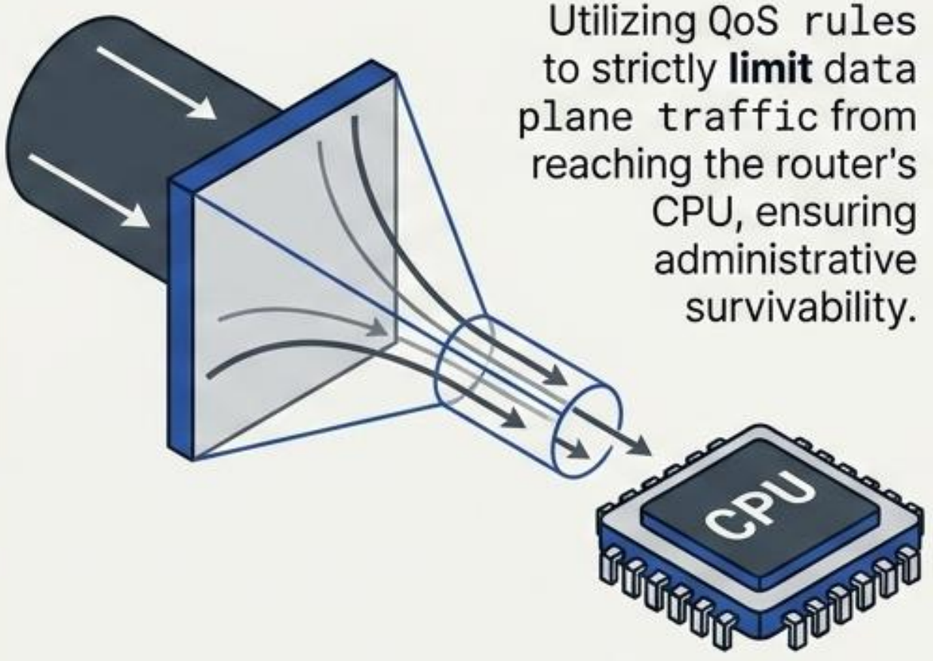
5. Recovery:
Gradual, monitored restoration of services from secure backups.

6. Lessons Learned:
The feedback loop. Analyzing control failures to update Prevention policies.

Attackers do not need to steal data to win; they simply weaponize the network's own resource limits.

Physical Limits (Hardware)	**Failure State:**
CPU, RAM, Bandwidth	Dropped packets, hardware crash.
Logical Limits (Software)	**Failure State:**
State Tables, CAM/TCAM Tables, Sockets	System ignores new traffic while remaining online.

Control Plane Policing (CoPP)

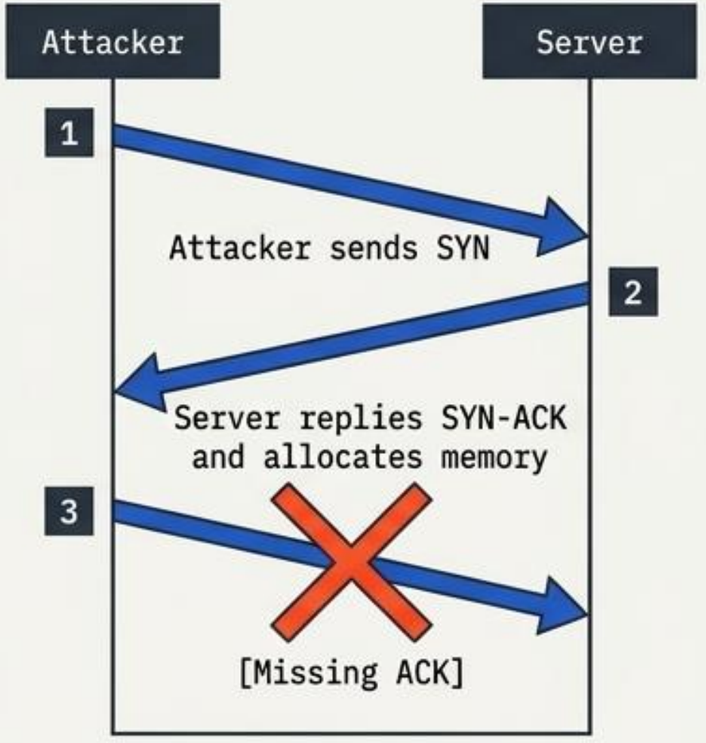


Utilizing QoS rules to strictly **limit** data plane traffic from reaching the router's CPU, ensuring administrative survivability.

1. Volumetric Attacks

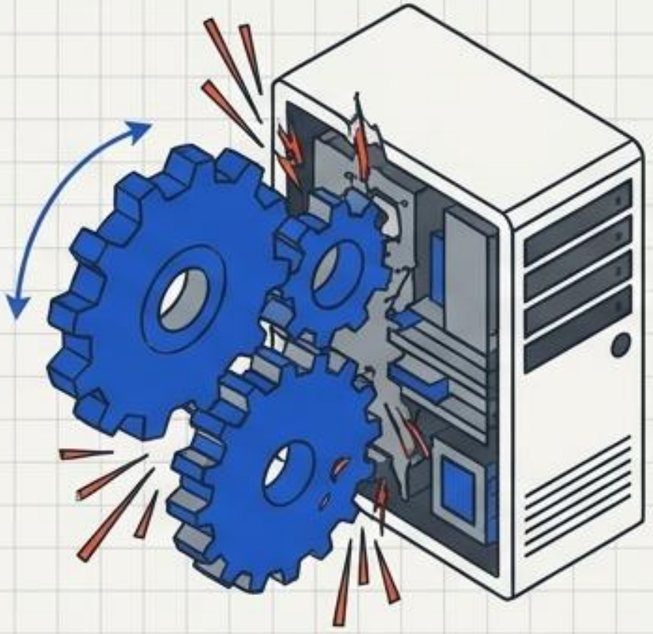
Brute force vector. Saturating physical interface bandwidth using massive torrents of connectionless protocols (UDP Floods).

2. Protocol/State-Exhaustion



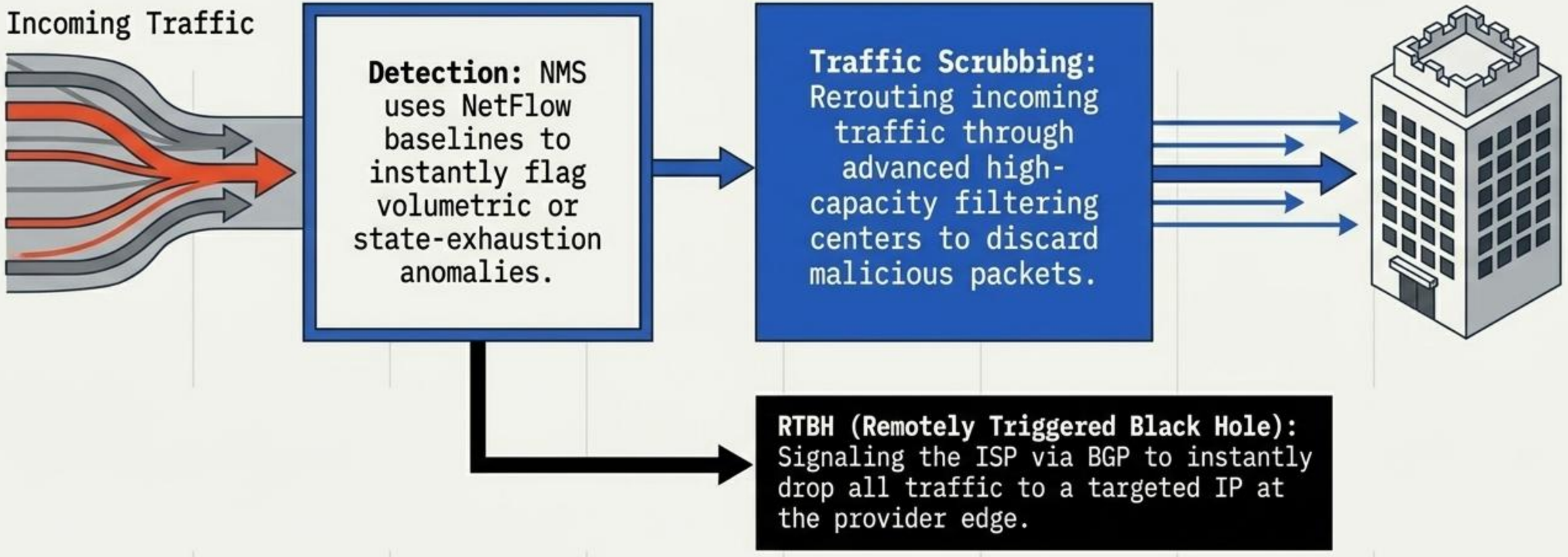
Surgical logical vector. The TCP SYN Flood: State table hits 100% instantly, dropping all new legitimate connections.

3. Application-Layer



CPU/Disk vector. Bypasses the network infrastructure to target backend servers via complex HTTP requests.

Automated Mitigation (Surviving DDoS)



Final Synthesis: True operational security merges legally sound Governance, identity-based Access Control, continuous SIEM Monitoring, and automated Mitigation.