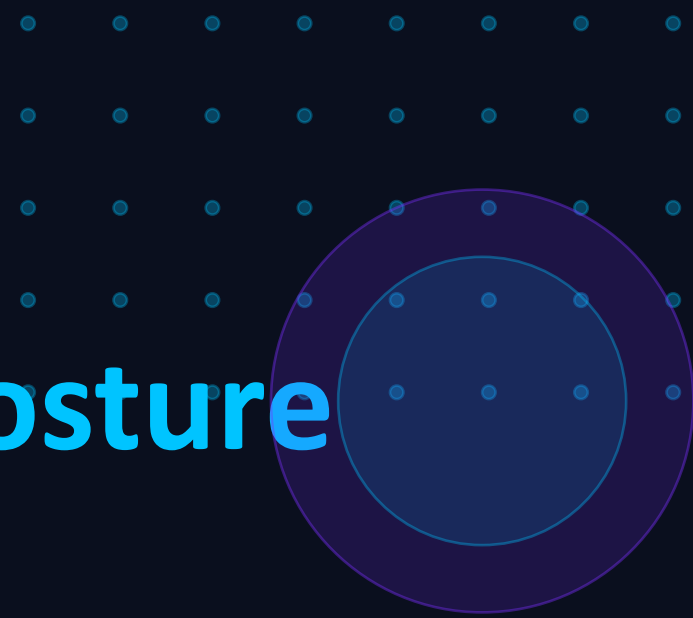


Creating a Unified Security Posture

A decorative graphic in the top right corner consisting of a grid of small blue dots. Overlaid on this grid are two concentric circles: an outer dark purple circle and an inner medium blue circle. Both circles also contain the same grid of dots.

Integrating People, Technology, and Process
Across Every Environment

Abhijit Chakravarty | 09-Sept-2026

Today's Reality: Security in Silos

Fragmented Visibility

Security tools operate in isolation. Cloud, on-prem, and endpoint data never converge into a single view.

Alert Fatigue

Teams drown in thousands of daily alerts with no unified context—critical threats get buried in noise.

Compliance Gaps

Disparate systems make demonstrating regulatory compliance a manual, error-prone, and costly effort.

Integrating Security Across Every Environment

1

Unified Data Plane

Consolidate telemetry from AWS, Azure, GCP, on-prem data centers, and OT/IoT into a single security data fabric.

2

API-First Integration

Adopt vendor-agnostic APIs so new cloud services are onboarded into the security perimeter within hours, not months.

3

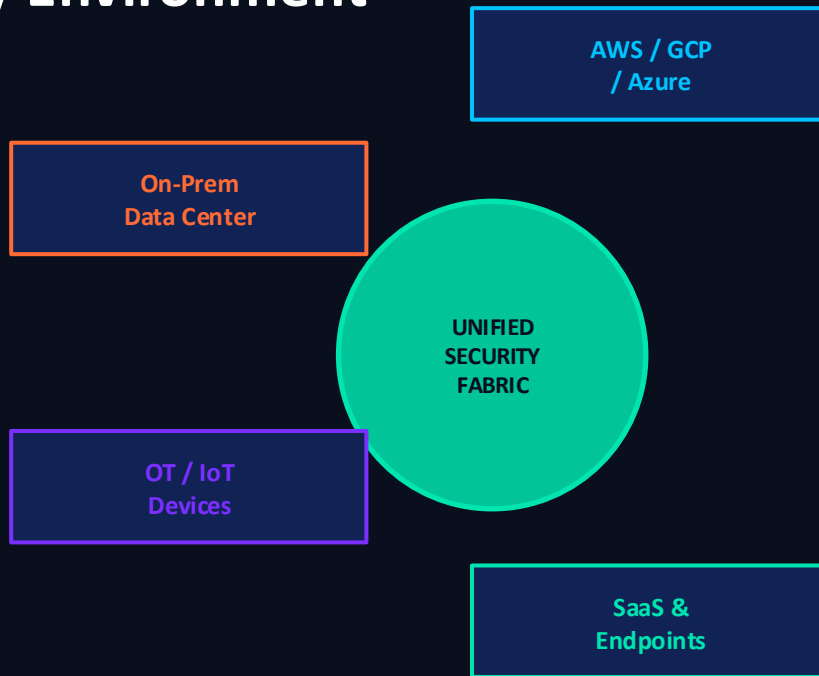
Policy Synchronization

Enforce a single set of data classification and access policies across environments—no more environment-specific exceptions.

4

Hybrid-Native SIEM/SOAR

Deploy detection and response tools designed for hybrid scale, not retrofitted from legacy on-prem architectures.



Breaking Down Silos: End-to-End Visibility & Control

⚠ WITHOUT Unified Visibility

- SIEM, DLP, EDR, CASB—each has its own console
- Data access events on-prem are invisible to cloud teams
- Mean Time to Detect (MTTD) stretches to weeks
- Shadow IT and unsanctioned data movement go undetected
- Compliance reporting requires manual data aggregation



✓ WITH Unified Visibility

- Single-pane-of-glass across all tools and environments
- Real-time data lineage: who accessed what, where, when
- MTTD reduced from days/weeks to minutes
- Data-centric visibility spots insider threats and misconfigurations
- Automated evidence collection for audit readiness

Leveraging AI & Automation for Proactive Threat Management



Behavioral Baselining

AI learns normal activity patterns for every user and entity, instantly flagging deviations—not just known attack signatures.



Automated Triage

SOAR playbooks auto-contain compromised accounts, quarantine infected endpoints, and revoke excessive permissions without human intervention.



Predictive Risk Scoring

Machine learning continuously scores risk across identities, data assets, and devices—prioritizing analyst attention where it matters most.



Threat Intelligence Fusion

Ingest global threat feeds and correlate with internal telemetry in real time to detect emerging TTPs before they weaponize.



Natural Language Queries

Security analysts investigate threats using plain English—no query language expertise required. AI translates intent to action.



Continuous Remediation

AI doesn't just detect—it recommends and executes fixes: closing exposures, removing stale permissions, and hardening configurations.

What AI-Driven Security Looks Like in Production

DAY 1

Insider Threat Detection

A finance analyst downloads 3,000 sensitive records at 11:45 PM—outside their normal working pattern. AI flags it within seconds. SOAR auto-suspends the session and alerts the SOC.

✓ Breach contained before data leaves the network.

DAY 7

Ransomware Early Warning

AI detects mass file rename events matching known ransomware staging behavior on a Windows server. Endpoint is automatically isolated. Threat intel fusion identifies the strain as a new LockBit variant.

✓ Attack stopped at the staging phase—zero encryption events.

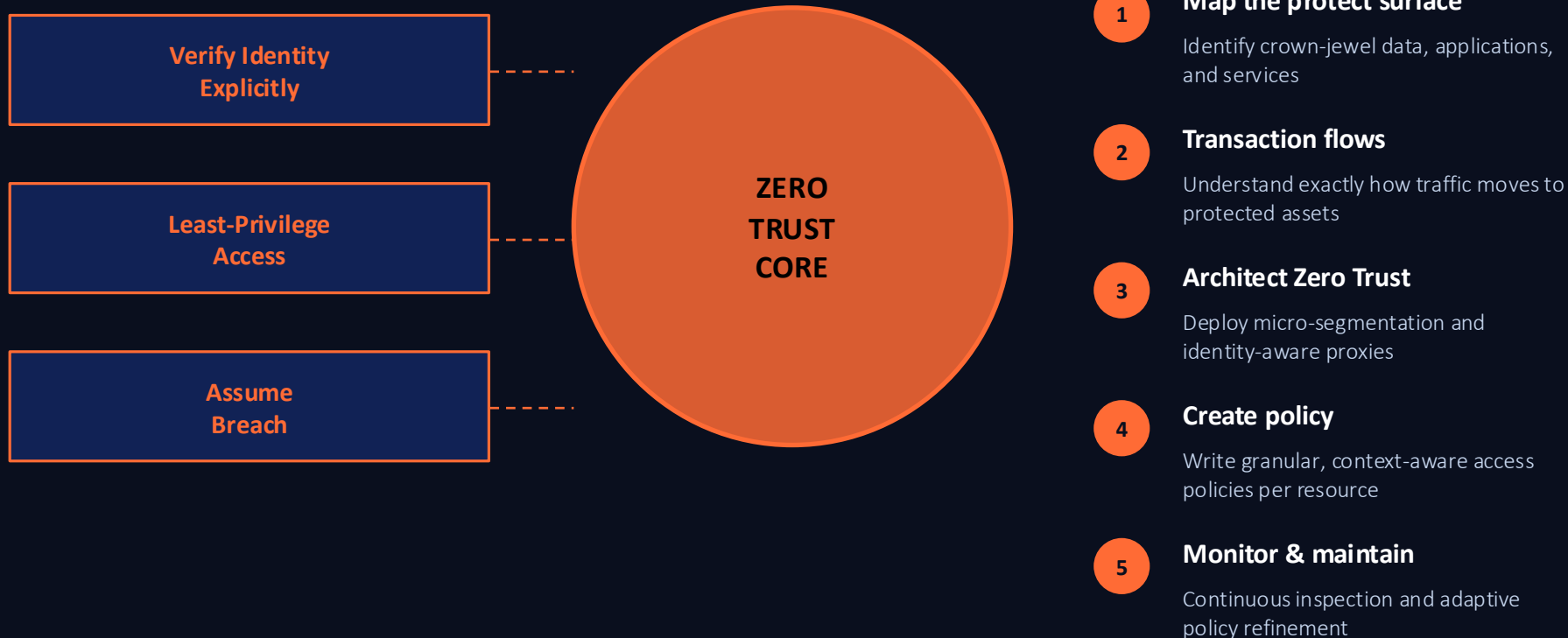
DAY 30

Over-Privileged Identity Discovery

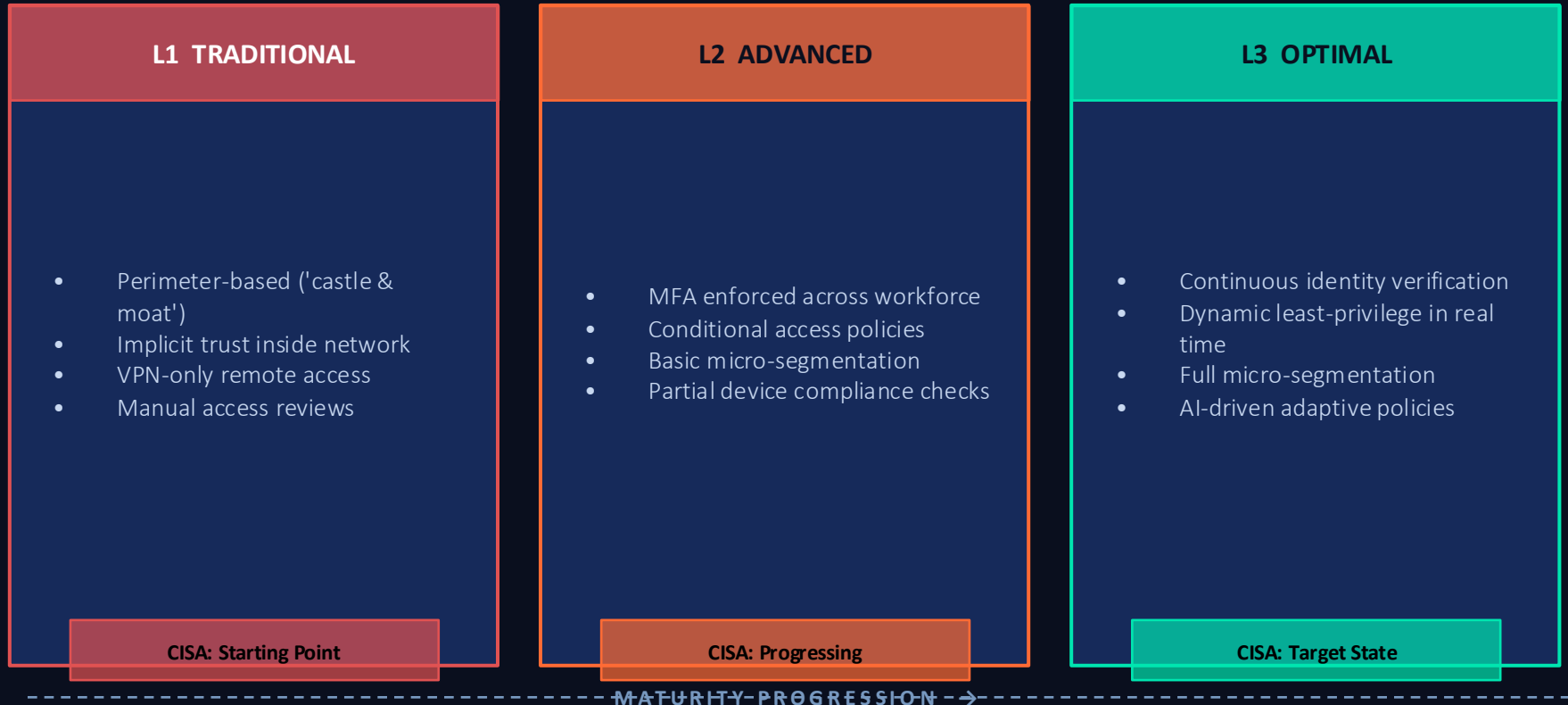
Continuous AI risk scoring surfaces 847 accounts with excessive permissions never used in 90 days. Automated remediation workflow trims access—reviewed and approved by IAM team in a single dashboard.

✓ Attack surface reduced by 62% without a single manual ticket.

Implementing Zero Trust: Never Trust, Always Verify



Where Is Your Organization on the Zero Trust Journey?



Building a Culture of Security Collaboration



Security ↔ IT Ops

- Joint runbooks for incident response
- Shared dashboards, unified alerting
- DevSecOps pipelines with security gates

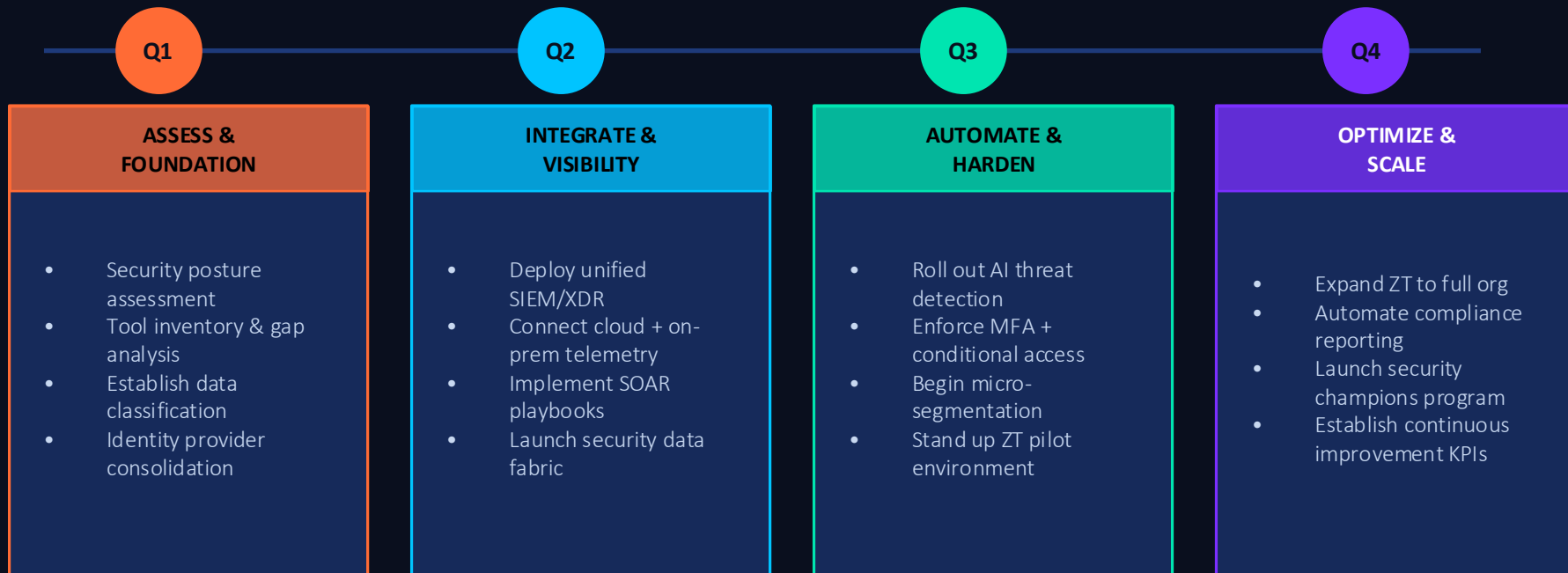
Security ↔ Business

- Risk language translated to business impact
- Executive security scorecards (monthly)
- Business unit security champions program

All Three: Governance

- Cross-functional Security Steering Committee
- Shared OKRs tied to security outcomes
- Annual tabletop exercises with C-suite

Your 12-Month Unified Security Posture Roadmap



KPIs That Prove Your Unified Security Posture is Working



70%

Mean Time to Detect (MTTD)

From days to hours through unified telemetry and AI-driven detection



65%

Mean Time to Respond (MTTR)

Automated containment and SOAR playbooks slash response timelines



95%

Asset Visibility Coverage

All cloud, on-prem, and hybrid assets discovered and monitored continuously



80%

Over-Privileged Accounts

Least-privilege enforcement via just-in-time access and AI remediation

↑ 4x

Analyst Productivity

AI triage eliminates false positives, freeing analysts for high-value work



50%

Audit Preparation Time

Automated evidence collection and continuous compliance monitoring

Security is Not a Product. It's a Unified Posture.

01 Integrate security across cloud, on-prem, and hybrid environments

02 Break down silos to achieve end-to-end visibility and control

03 Leverage AI and automation for proactive threat management

04 Implement Zero Trust principles across identity, data, and networks

05 Build a culture of collaboration between Security, IT, and Business



Start Today: Assess your current posture → Identify your biggest visibility gap → Build your cross-functional security team



Today we discussed people, process, technology, and AI.

Three things we can manage, and the one thing Well, we're still negotiating.

And you all know which one I am referring to.