HashiCorp
an IBM Company

Enabling Secure Innovation Without Sacrificing Compliance

A Practical Zero Trust Playbook for CISOs

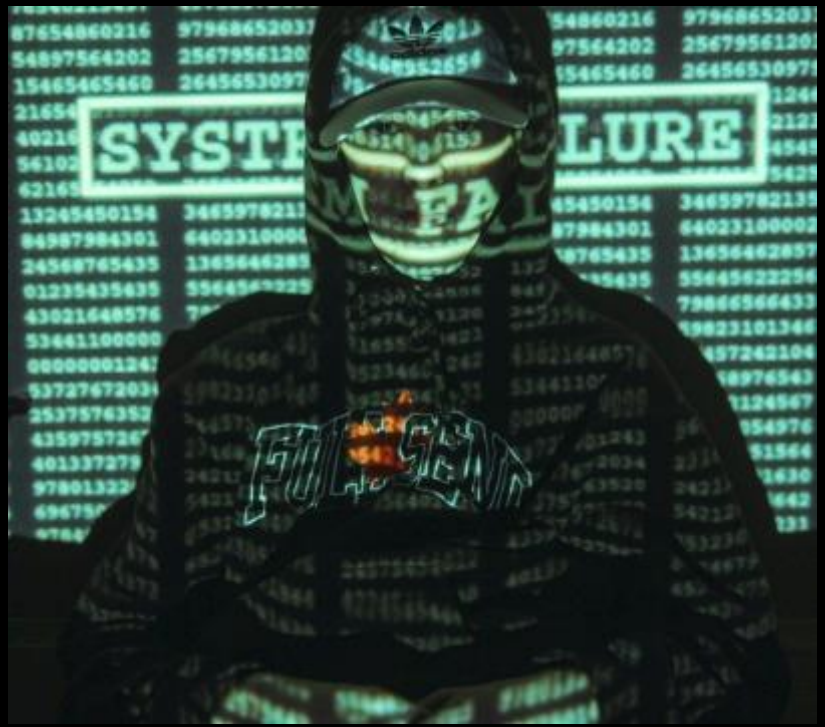
Andrew Brydon

Andrew Brydon

CTO A/NZ
HashiCorp, an IBM company

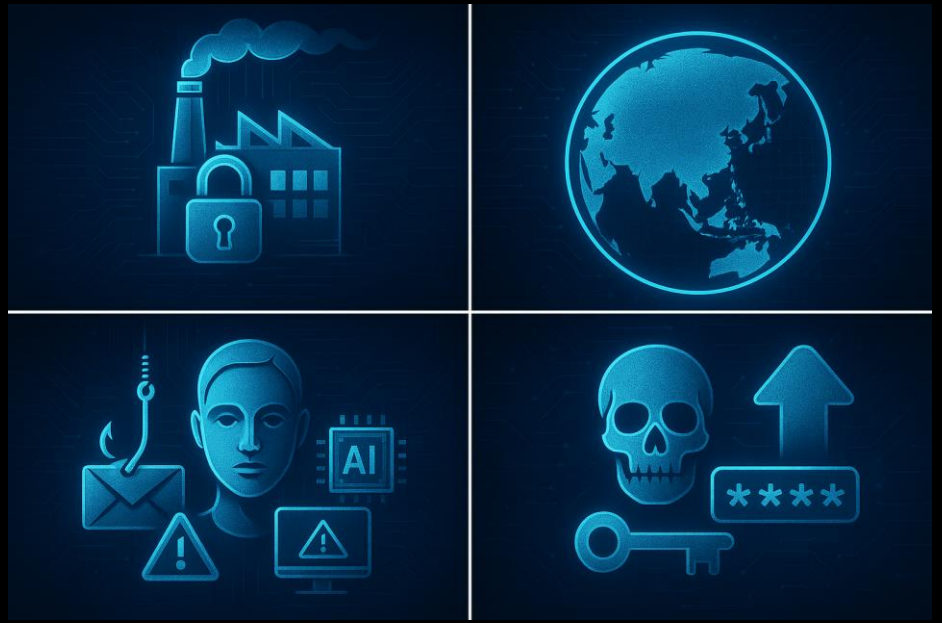
2025 Reality Check: Breaches, Ransomware & Third-Party Risk

- 22,052 incidents - 12,195 confirmed breaches (latest DBIR)
- Ransomware in 44% of breaches
- Median payout ≈ $115k **- 64% refuse to pay**
- Exploited vulnerabilities now ~20% of initial access
- Third-party involvement ~30%
- AI double-edged: synthetic phishing growth
- 15% of employees using GenAI from corp devices



2025 Cyber Threat Landscape: Targets & Tactics

- Manufacturing remains the top target (29% extortion, 24% data theft)
- APAC leads in incidents: 34% of global total
- AI adopted by attackers: phishing, deepfakes, malicious code
- Infostealer surge: +84% weekly in 2024, +180% early 2025
- Credential attacks: ~30% of intrusions



Attack Vectors & Impact Overview

Initial Access Methods:

- Public-facing app exploits (~30%)
- Valid credentials (~30%)

Malware Trends:

- Ransomware = 28% of malware incidents
- 4 of top 10 dark-web vulnerabilities exploited in <2 weeks

Impact Snapshot:

- Credential harvesting: 28%
- Data theft: 18%
- Extortion: 12%

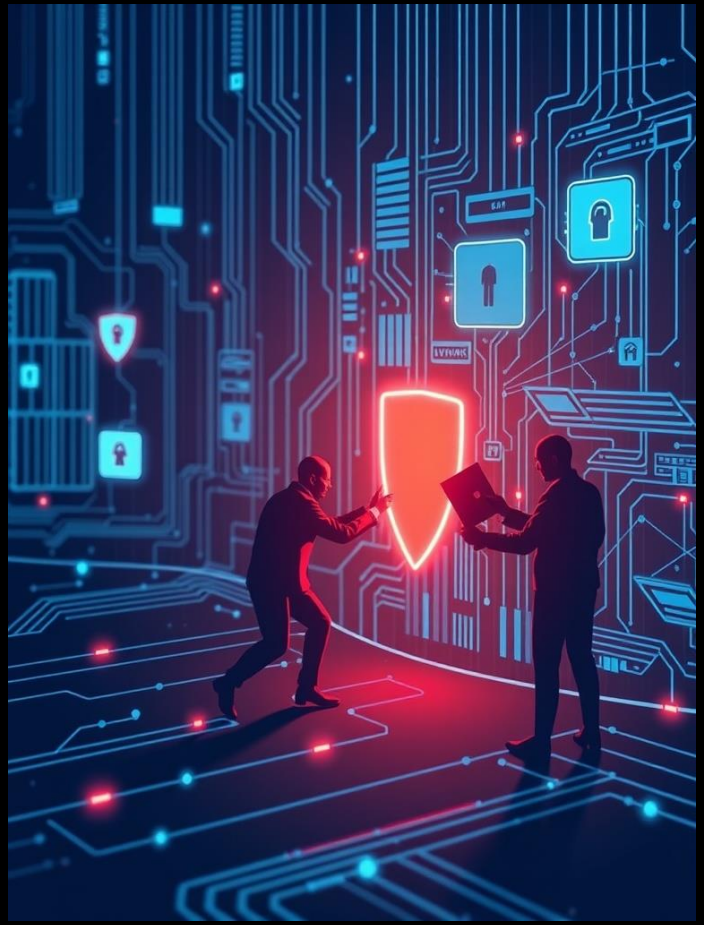
Emerging Tactics & Cyber Resilience Roadmap

Cloud & Phishing Trends:

- Rise of cloud-hosted phishing (LATAM focus)
- Shift of attachments to PDFs & obfuscated URLs

Defense Recommendations:

1. Monitor dark web for threat intelligence
2. Secure AI pipelines (data, models, infra)
3. Strengthen identity strategy (MFA, passkey)
4. Leverage AI-driven threat detection
5. **Adopt zero trust & reduce IT complexity**



Why Zero Trust —

- Compliance ≠ security; must assume breach and verify continuously
- CISA ZT Maturity Model guides pillars & outcomes
- Australia: Essential Eight, Hosting Certification Framework, IRAP, APRA CPS 230
- Sovereignty-by-design: approved patterns and platform guardrails

From Perimeter to Identity-Driven Security

Key Elements of Trust Evolution:

- **Identity:** which encompasses the notion of personal and organizational identification in various contexts
- **Context:** referring to the situational and environmental factors that influence perceptions of trust
- **Continuous verification:** highlighting the ongoing need for validation of trustworthiness through consistent actions and transparency

From Perimeter to Identity-Driven Security

Key Elements of Trust Evolution:

- **Identity:** which encompasses the notion of personal and organizational identification in various contexts
- **Context:** referring to the situational and environmental factors that influence perceptions of trust
- **Continuous verification:** highlighting the ongoing need for validation of trustworthiness through consistent actions and transparency

The Zero Trust Playbook: Repair, Repave, Rotate

1. Mandate & Maturity Baseline
2. Identity First (Human + Machine)
3. Network as Service-Mesh (mTLS, L7 intentions)
4. Data Sovereignty & Classification
5. Automate Everything (IaC + pipelines + drift detection)
6. Policy-as-Code (guardrails, not gates)
7. Secure the AI Lifecycle (Gov/reg)
8. Auditability & measurable outcomes

1 Mandate & Maturity Baseline

- Executive mandate, risk appetite, operating model
- Baseline vs CISA ZTMM + Essential Eight per system
- Prioritise high-blast-radius estates (IDP, CI/CD, data, AI)
- 12-month roadmap with quarterly OKRs

2 Identity-First (Human & Machine)

SSO + MFA + conditional access everywhere

Machine identities: short-lived certs/keys auto-rotate, vault all secrets

JIT privileged access; session recording, no standing prod creds

Outcome: requests verified, time-bound, least-privileged

3 Network Mesh

Encrypt east-west with mTLS: authorise by workload identity

L7 intentions: retire flat trusts & split-tunnel VPNs

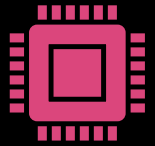
Harden edge: 14/30-day patch SLAs for internet-facing services

Outcome: micro-segmentation with context; confined blast radius

4 Data Sovereignty & Classification

Map data/systems to HCF & ISM; IRAP-assessed platforms where needed

Encrypt at rest/in transit; BYOK/HSM for high-sensitivity systems



Tokenise PII/PHI (format-preserving) to minimise risk

Outcome: sovereignty by design; approved hosting patterns; audit-ready

5 Automate Everything (IaC)

- Standard modules & golden images; drift detection; immutable deploys
- Approvals shift-left via automated checks in pipelines
- Evidence capture embedded in runs
- Outcome: speed with safety; reproducible state

6 Policy-as-Code

1. Map guardrails to ISM, PSPF, CPS 230/234, PCI/HIPAA
2. Enforce tagging, IAM, KMS, network, data zones pre-prod
3. Deny risky changes at runtime
4. Require explicit exec sign-off for exceptions
5. Achieve compliant-by-default paved roads outcome

7 Secure the AI Lifecycle (Gov & Regulated)

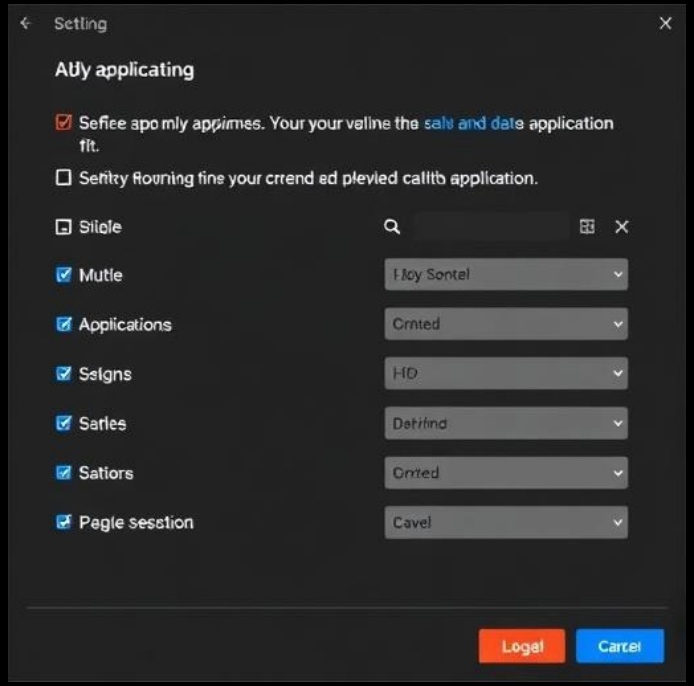
Governance & Risk

- Inventory models, prompts, datasets, vectors, plugins
- Adopt NIST AI RMF & NCSC/CISA Secure AI Dev Guidelines
- Tame shadow AI: SSO, egress control, logging
- ML-BOM/SBOM; supply chain validation

Technical Controls

- All keys in Vault; short-lived tokens for model access
- Network isolation + mTLS; JIT access to model infra/data
- PII minimisation and tokenisation for training and inference logs
- Red-team prompt injection, exfiltration, misuse

8 Auditability & Telemetry



- Centralize logs from IDP, IaC runs, vaults, mesh, access brokers
- Correlate identity, change, and data for quick forensics
- Automate evidence packs to prove control effectiveness
- Achieve simpler audits and faster investigations

The 30 to 90 Day Plan

Initial 30 Days Action Plan

1. Establish baseline maturity and select key estates
2. Activate Just-In-Time admin access and secure secrets
3. Implement SSO/egress for GenAI and initiate model inventory

Actions for Days 31–90

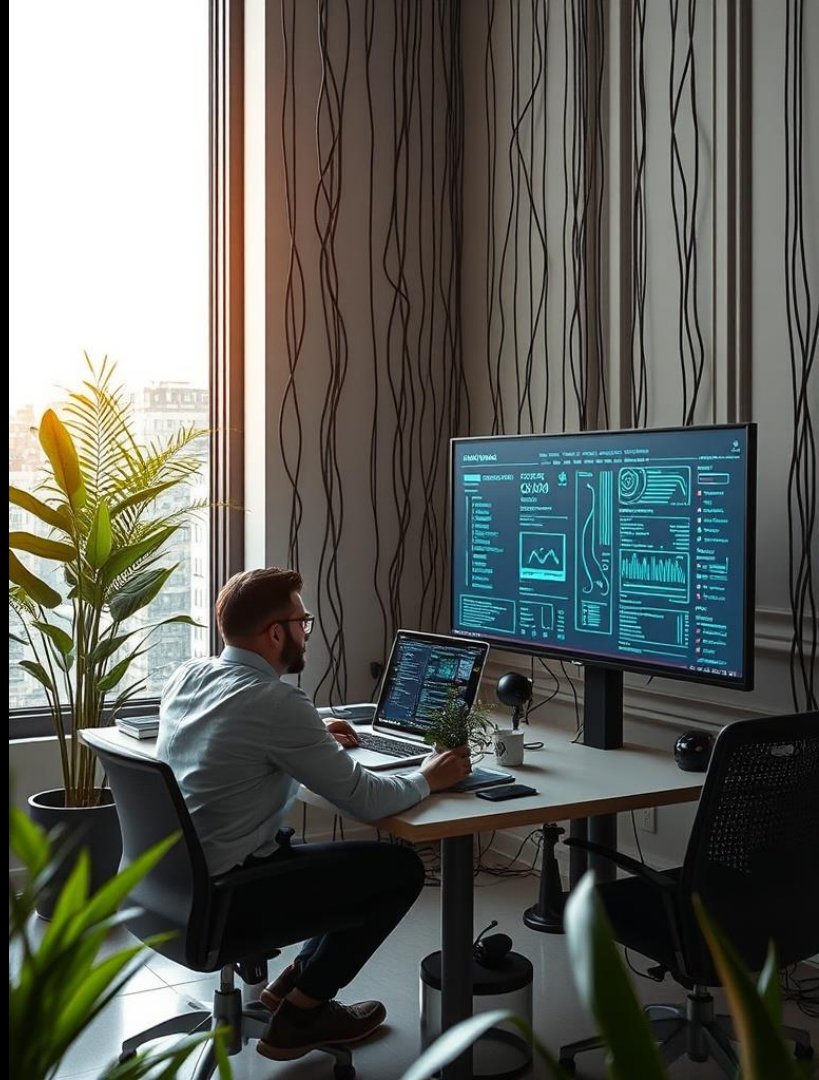
1. Implement policies in pipelines and golden modules/images
2. Launch pilot service mesh on key application
3. Integrate evidence into SIEM and activate AI governance policy

What “Good” Looks Like in 12 Months

- 100% human admin access via JIT; zero standing prod creds
- 80% secrets dynamic & auto-rotated; zero plaintext in repos
- 70% east-west traffic under mTLS + L7 intentions
- 90% infra changes via pipelines with passing policy checks
- AI systems inventoried; periodic red-team & model risk reviews

Security Benefits

- Less privileged access reviews since people are not involved in the change
- Less noise and volume to the SIEM meaning less false positives sent to the SOC
- Less accounts in the PAM



How HashiCorp Powers the Playbook

HashiCorp

Key Controls and Outcomes	HashiCorp Key Features
• Manage secrets and encryption	• Vault for dynamic secrets and HSM
• Implement JIT privileged access	• Boundary for JIT access and credential injection
• Use mTLS with service authorization	• Consul for service mesh and mTLS CA
• Apply IaC and golden images	• Terraform + HCP Packer for IaC and drift detection
• Enforce policy-as-code with evidence	• Sentinel/OPA for policy management
• Maintain audit logs and telemetry	• HCP logging integration with SIEM/SOAR

Call to Action for CISOs

1. Run the 90-day play in two high-impact areas
2. Fund or create the platform team for identity, IaC, policy-as-code
3. Publish Zero Trust KPIs to the board or equivalent quarterly
4. **Engage HashiCorp to blueprint your reference architecture**

Thank you

Strengthening security and governance

Proactive risk management

Mitigating risk within complex cloud environments
Detecting and responding to threats efficiently

Enhanced compliance posture

Advanced zero trust cloud practices

ENHANCED COMPLIANCE POSTURE

Consistent governance across hybrid cloud

Employ a single system of record

Deploy golden images and modules

Actively monitor all users and sessions

Streamline compliance audits

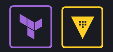
Secure your data with identity-based access control

Secure human access with least-privilege and MFA controls

Authenticate and authorize every machine-to-machine access request

Generate, rotate, or revoke secrets on demand

Automate and dynamically create keys and certificates



PROACTIVE RISK MANAGEMENT

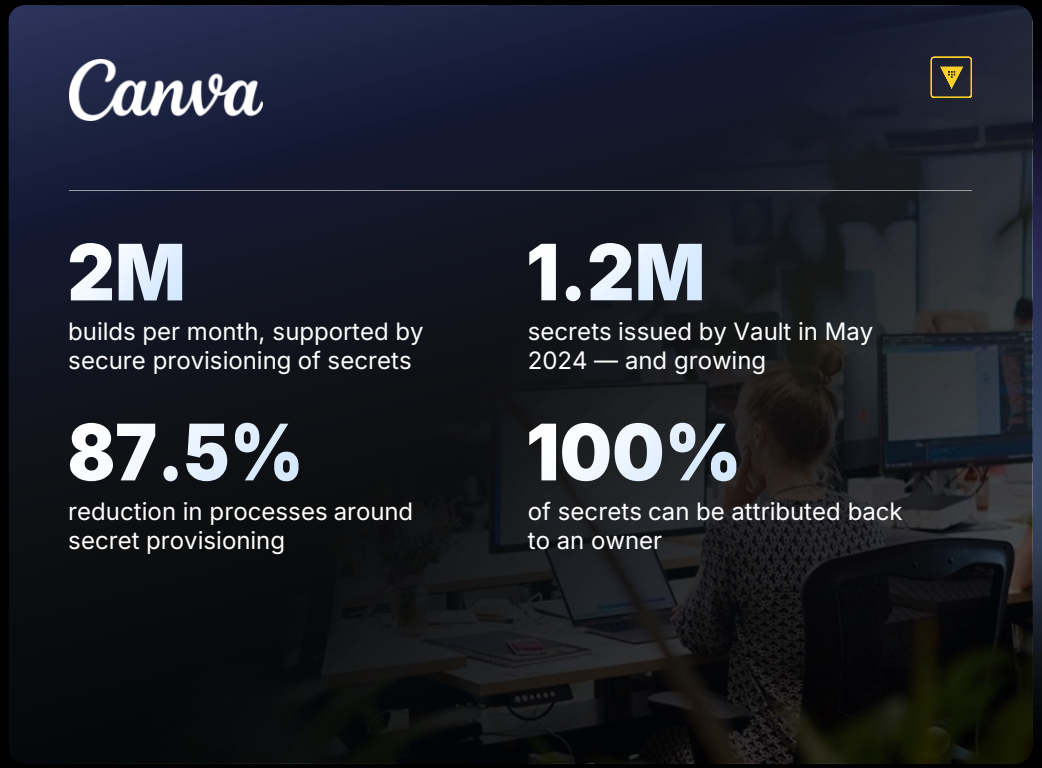
Detect and mitigate threats in complex environments

"Along with policy-driven infrastructure through Terraform, Vault automatically rotates credentials instead of forcing users to store information locally and risk inadvertent exposure. Add in Boundary for standardizing language and protocols for accessing infrastructure and services across our environment, and it creates an end-to-end security posture in line with our zero trust charter."

Benjamin Lara
Automation Engineer at ManTech

ENHANCED COMPLIANCE POSTURE

Streamlining secrets management



"Building developer trust is key to cultural change — by prioritizing testing, observability, and reliability, we ensured Vault could handle secrets migration without compromising trust."

Moe Abbas
Cloud Governance Lead at Canva

Secure your data with identity-based access control

athenahealth

3M
Requests for secrets a day

Eliminated
manual ticketing system and data caching layer

Reduced
operational costs

“By combining Vault's availability with the provisioning and discovery capabilities of HashiCorp's other tools, we've virtually eliminated our old secrets ticketing system and can resolve availability issues in under 30 minutes instead of four hours.”

Jeff Byrnes
Lead site reliability engineer at Athenahealth