RSU SECURITY BRIEF

End-to-End Business Security Architecture

A practical high-assurance model for identity, devices, networks, applications, data, operations, and recovery.

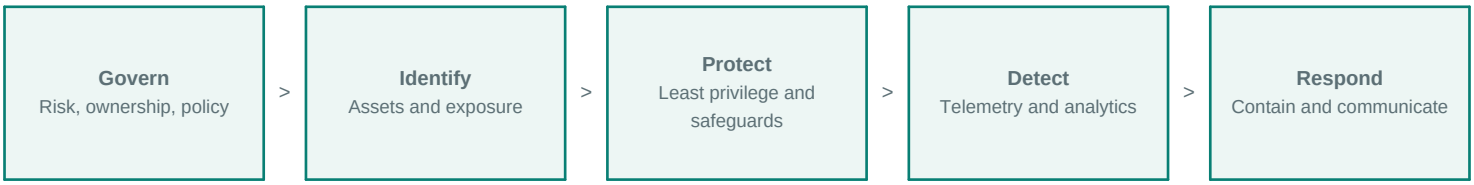
A high-level, public reference for business and technology leaders

Executive perspective

Strong security is not a single product or perimeter. It is a governed system of preventive, detective, responsive, and recovery capabilities that work together. This paper translates widely recognized public guidance into a business-focused reference architecture.

This is not classified guidance and does not certify any environment. It draws on public NIST and CISA practices appropriate for organizations seeking a mature, risk-based security program.

The continuous security decision loop



Architecture principles

• Verify explicitly: evaluate identity, device, resource, context, and risk for each access decision.

• Use least privilege: grant only the access required, for only as long as required.

• Assume compromise: segment systems, constrain lateral movement, and maintain independent recovery paths.

• Protect data throughout its lifecycle with classification, encryption, access control, retention, and monitored disposal.

• Design operations for evidence: centralized logging, tested response procedures, configuration baselines, and accountable ownership.

Reference architecture

People & identity	Devices & workloads	Network & access
Phishing-resistant MFA Conditional access Privileged access controls Joiner/mover/leaver governance	Inventory and ownership Secure configuration EDR and vulnerability management Workload identities	Segmentation Policy enforcement points Encrypted connections Controlled administrative paths
Applications & APIs	**Data**	**Operations & recovery**
Secure development lifecycle Secrets management Strong service authorization Dependency and code testing	Classification and minimization Encryption at rest and in transit DLP and access monitoring Immutable backup copies	Central telemetry and alerting Incident playbooks Recovery objectives Restoration exercises

How access should be evaluated

Implementation roadmap

- Establish executive ownership, risk appetite, critical services, and measurable target outcomes.
- Create authoritative inventories for identities, devices, applications, data, dependencies, and recovery requirements.
- Prioritize identity security, administrator isolation, MFA, asset visibility, endpoint protection, segmentation, and logging.
- Integrate signals into consistent access policy and incident workflows.
- Test controls through tabletop exercises, technical validation, restore tests, and continuous improvement.

Minimum executive questions

- Can we identify every privileged identity and require strong verification?
- Can we isolate a compromised endpoint before it reaches critical systems?
- Do we know where sensitive data is stored and who can access it?
- Can we detect and investigate abnormal access across cloud and on-premises systems?
- Can we restore critical services from protected backups within agreed objectives?
- Are security exceptions documented, approved, time-limited, and reviewed?

Public references

NIST Cybersecurity Framework 2.0 - https://www.nist.gov/cyberframework
NIST SP 800-207, Zero Trust Architecture - https://doi.org/10.6028/NIST.SP.800-207
NIST SP 1800-35, Implementing a Zero Trust Architecture - https://csrc.nist.gov/pubs/sp/1800/35/final
CISA Zero Trust Maturity Model Version 2 - https://www.cisa.gov/zero-trust-maturity-model

Next step

RSU can translate this reference model into an assessment, prioritized roadmap, architecture, implementation plan, and recovery validation program tailored to your business.