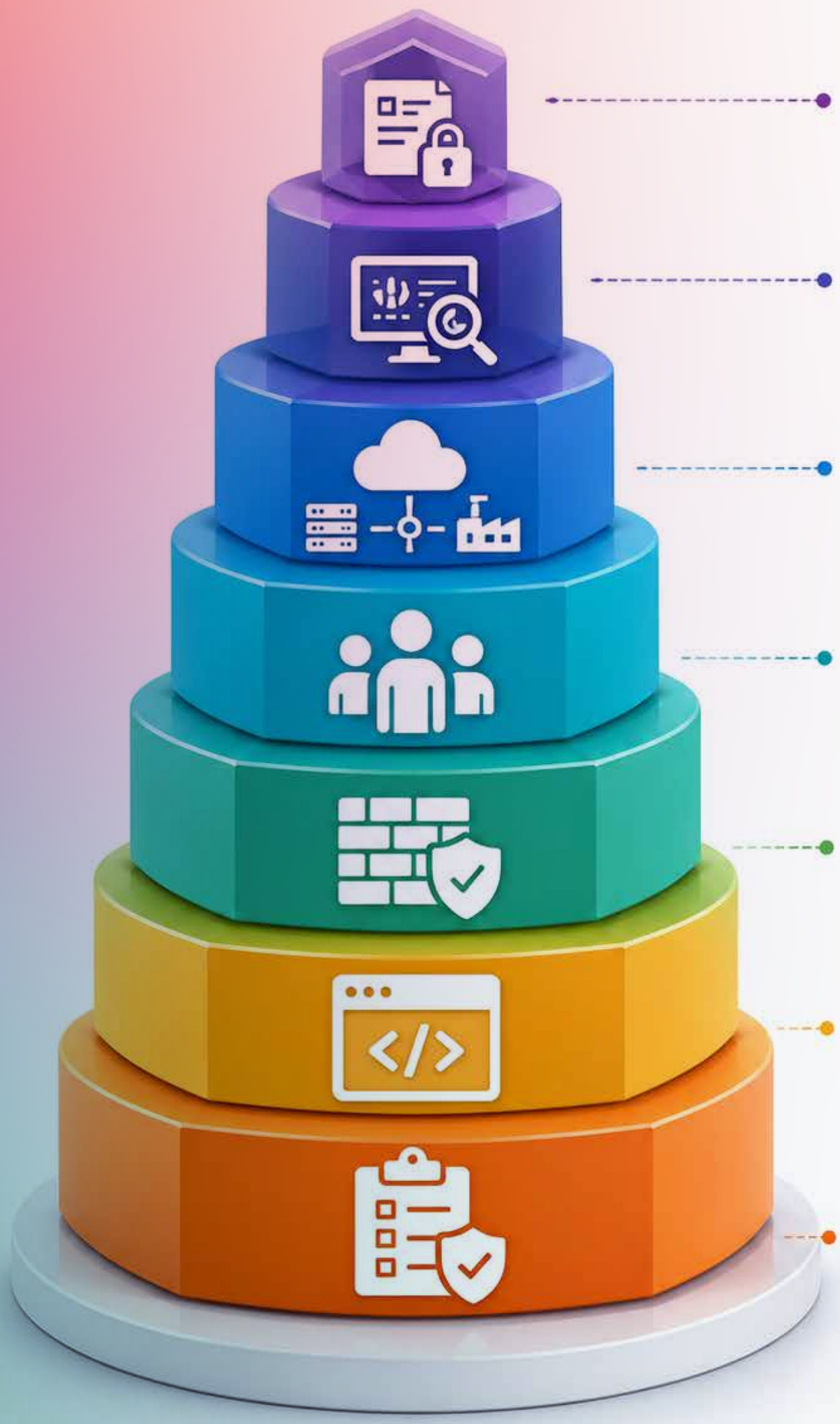
The 7-Layer Security Model :

A Framework Every CISO Should Know



1 Data:
The Asset Every Attacker Is Trying to Reach

2 Monitoring:
You Cannot Defend What You Cannot See

3 Infrastructure:
Cloud, Network, and OT Are Not the Same Problem

4 Human:
Your People Are Not the Weakest Link. Your Culture Is.

5 Perimeter:
The Boundary Attackers Test Before You Do

6 Application:
Where 90% of Attacks Begin and Most Testing Stops

7 Governance:
The Layer That Makes Every Other Layer Accountable

CREST Accredited certin Empanelled

BriskInfosec™
VULNERABILITY TO VICTORY

sales@briskinfosec.com

Layer 1

Data : The Asset Every Attacker Is Trying to Reach

Everything else exists to protect this.
If you don't know what data you have, where it lives, and who can access it – you cannot protect it.

What This Layer Covers :

- Data Security Audit and DSPM
- Data Masking and Privacy Controls
- Database Penetration Testing
- Data Breach Simulation
- Digital Forensics
- Data Governance
- BCP/DR Planning
- DPDPA and GDPR Compliance

CREST Accredited
certin Empanelled

BriskInfosec™
VULNERABILITY TO VICTORY

sales@briskinfosec.com

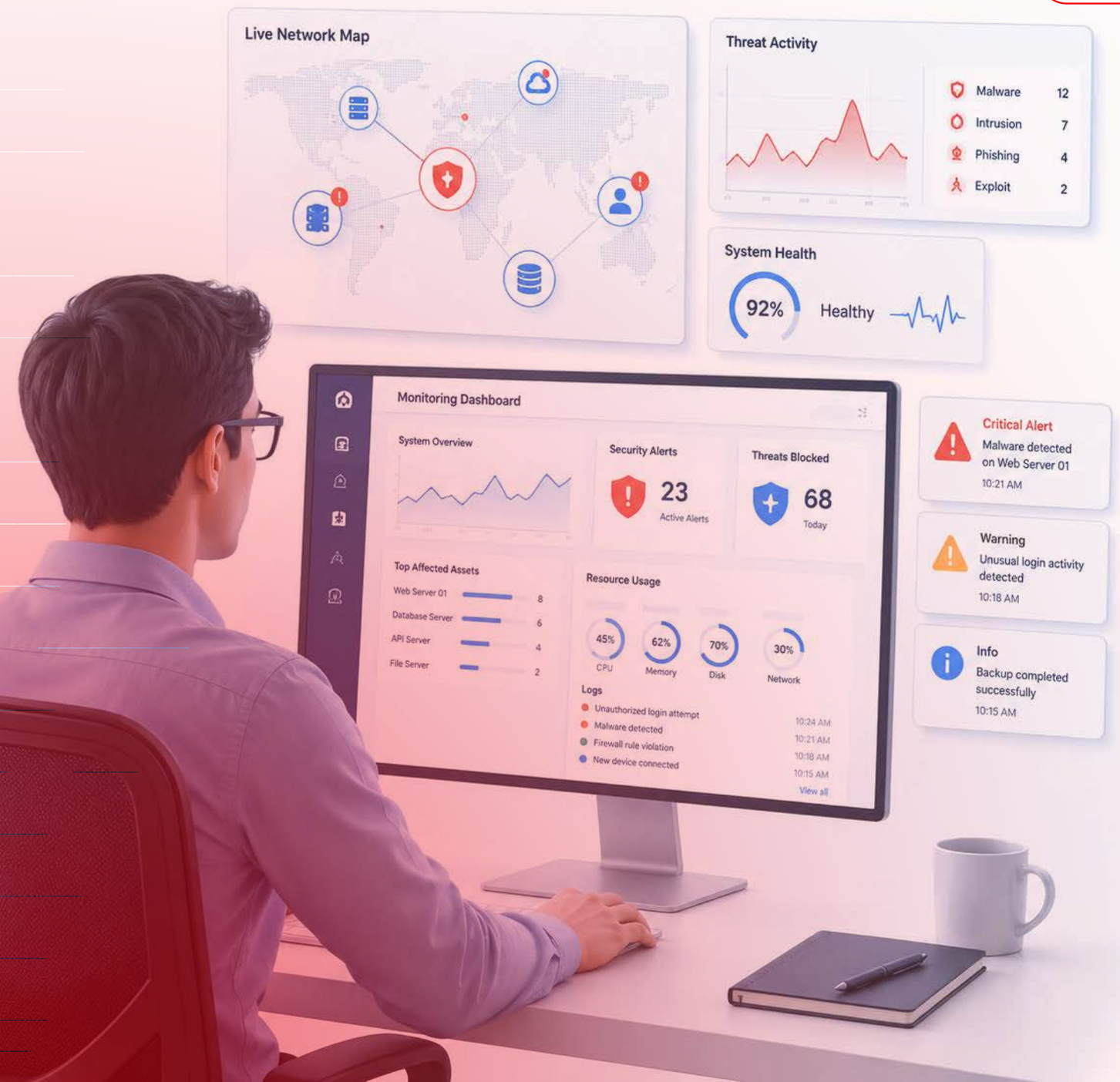
Layer 2

Monitoring : You Cannot Defend What You Cannot

The average attacker dwells inside a network for weeks before detection. Most organizations have tools. Very few have genuine visibility.

What This Layer Covers :

- 24/7 SOC as a Service
- SOAR Integration
- Cyber Threat Intelligence
- Threat & Vulnerability Management
- Lateral Movement Detection
- Security Monitoring
- Security Governance
- Third Eye Security Review



CREST Accredited
certin Empanelled

BriskInfosec™
VULNERABILITY TO VICTORY

sales@briskinfosec.com

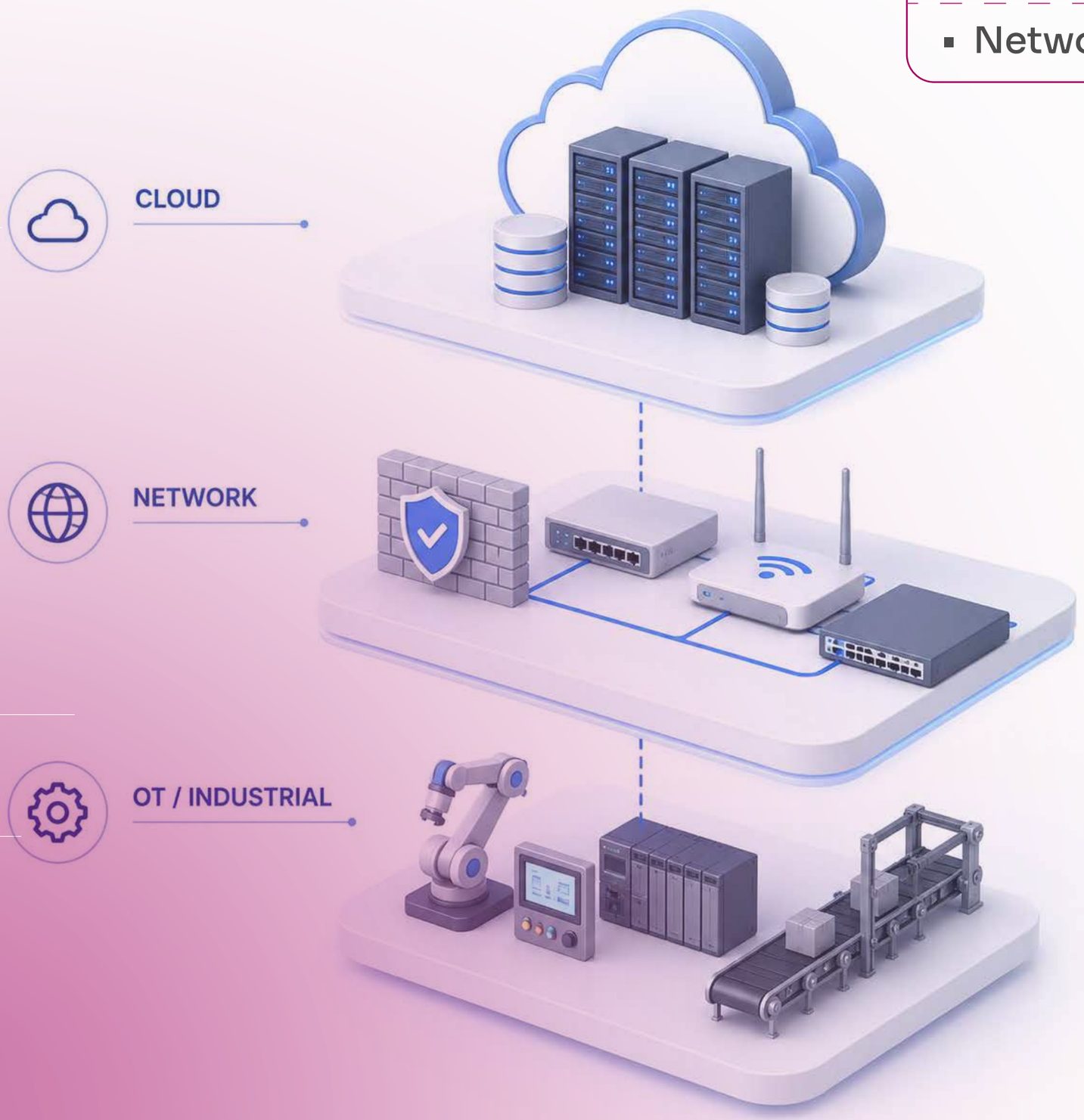
Layer 3

Infrastructure : Cloud, Network, and OT Are Not

Misconfigured clouds, unpatched networks, and undefended OT systems are separate problems. Treating them as one causes breaches.

What This Layer Covers :

- Network Security Audit
- Cloud Security Assessment
- Cloud Configuration Review
- OT/SCADA Security
- IoT and Hardware Security
- Wireless Security Assessment
- Infrastructure Risk Assessment
- Network Architecture Review



CREST Accredited
certin Empanelled

BriskInfosec
VULNERABILITY TO VICTORY

sales@briskinfosec.com

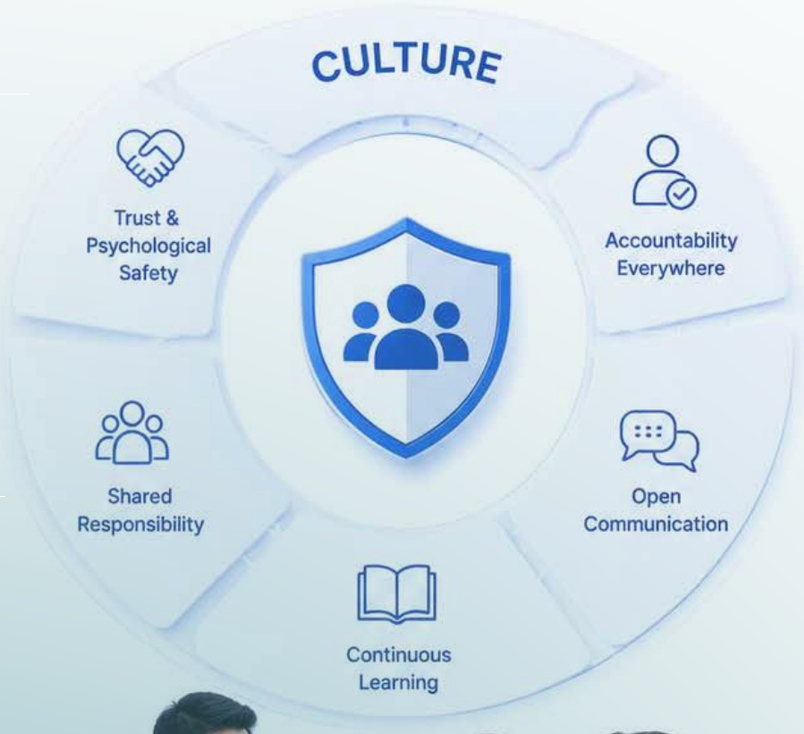
Layer 4

Human : Your People Are Not the Weakest Link.

Attackers study your people as carefully as they study your systems. Annual training and phishing click rates are measuring the wrong thing entirely.

What This Layer Covers :

- Phishing Simulation
- Security Awareness Training
- Tabletop Exercises
- Incident Response Training
- Leadership and Culture Programs
- Hacker's POV Awareness
- Secure Code Training
- V-CISO and Virtual Security Team



PEOPLE

Make Mistakes

- Need Training
- Need Tools
- Need Support

VS.

CULTURE

Drives Behavior

- Ignores Risks
- Blames Others
- Breaks Silos

Build a culture where security is everyone's responsibility—every day.

CREST Accredited · certin Empanelled

BriskInfosec™ VULNERABILITY TO VICTORY

sales@briskinfosec.com

Layer 5

Perimeter : The Boundary Attackers Test Before You Do

Attackers will probe your perimeter. The question is whether you test it first. An untested perimeter is not a defended one - it is an untested assumption.

What This Layer Covers :

- Red Team Operations
- CREST VAPT
- Threat Modeling
- Lateral Movement Assessment
- DevSecOps Integration
- Cyber Resilience Audit
- Military Grade Review
- Access Control Review

CREST Accredited

certin Empanelled

BriskInfosec™

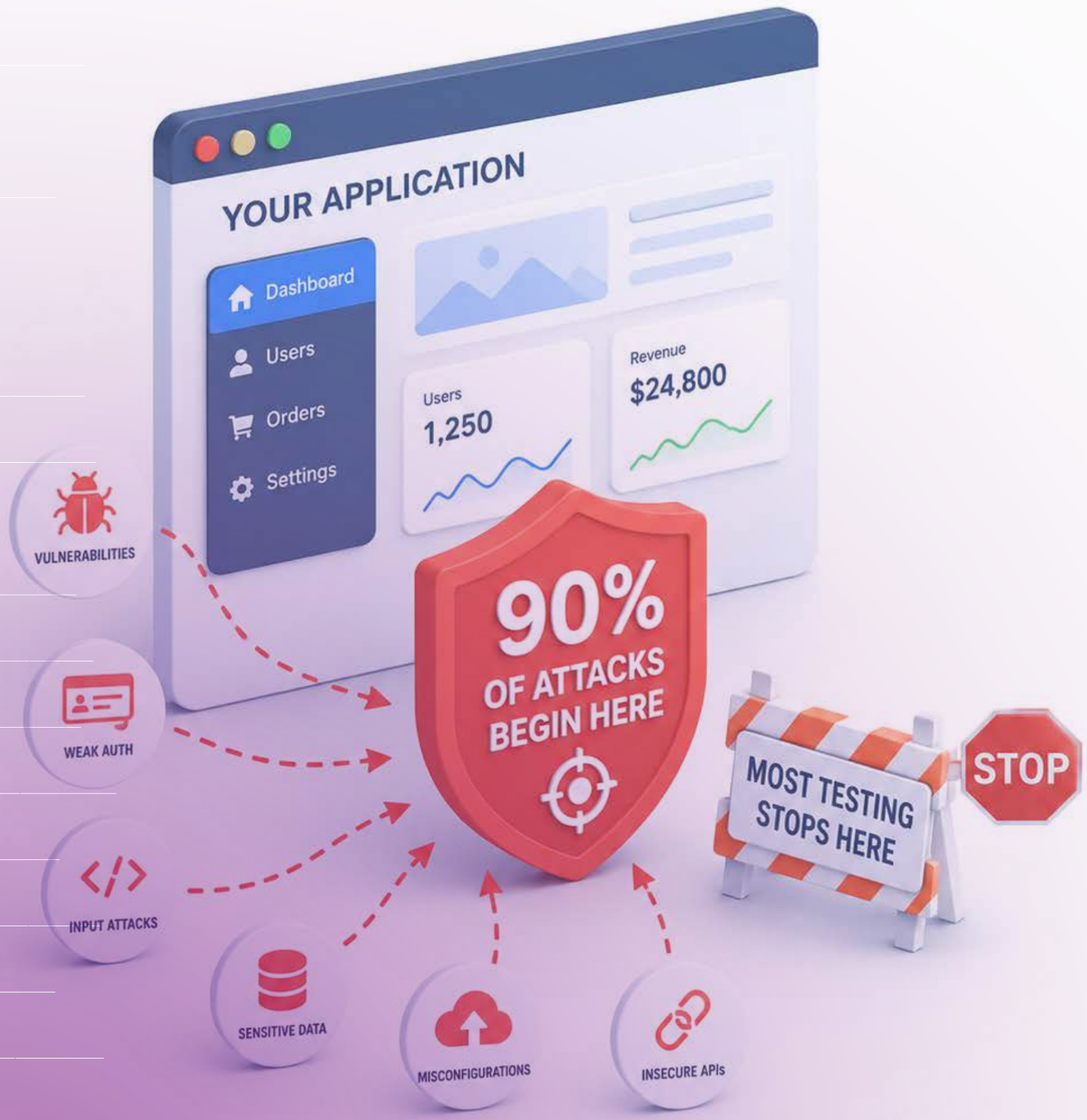
VULNERABILITY TO VICTORY

sales@briskinfosec.com

Layer 6

Application : Where 90% of Attacks Begin

Web apps, APIs, mobile apps, and code are in constant contact with the outside world. Most organizations test once a year. Attackers probe continuously.



What This Layer Covers :

- Web Application VAPT
- Mobile App Security
- API Security Testing
- AI and LLM Security Audit
- Secure Code Review
- SBOM and SCA
- Penetration Testing as a Service
- Secure SDLC & AppSec Governance

CREST Accredited
certin Empanelled

BriskInfosec™
VULNERABILITY TO VICTORY

sales@briskinfosec.com

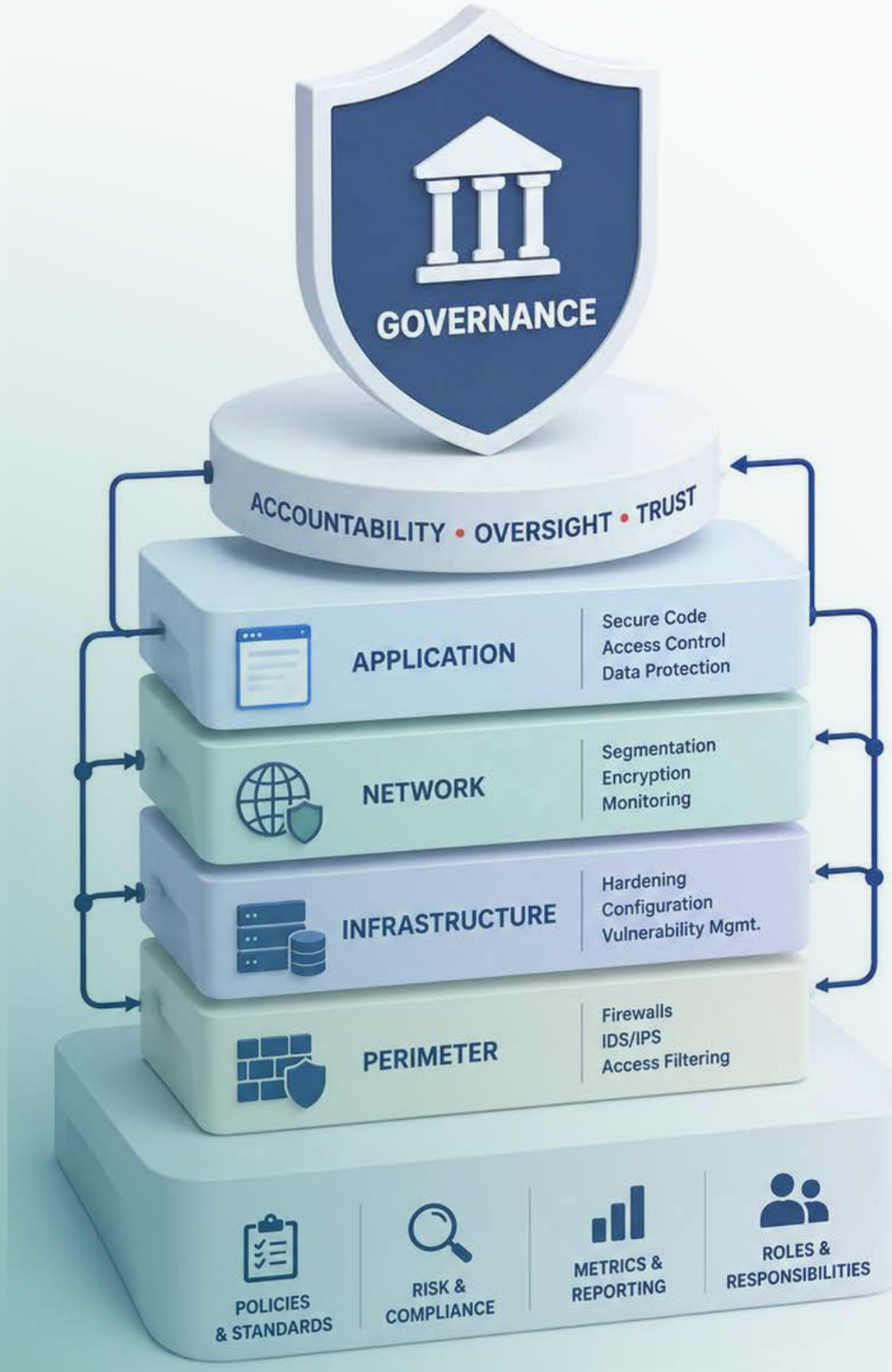
Layer 7

Governance : The Layer That Makes Every Other

Without governance, security investments lack direction and accountability. Being certified is not the same as being secure. Governance closes that gap.

What This Layer Covers :

- ISO 27001, SOC 2, PCI-DSS
- DPDPA, IRDAI, NIST CSF, IEC 62443
- ISO 42001 (AI), ISO 21434
- GRC Framework & Risk Assessment
- Third-Party Risk Management
- Cybersecurity Maturity Assessment
- Business Impact Analysis
- HIPAA, GDPR



sales@briskinfosec.com

Which Layer Is Your Organization's

Weakest Point?

Measure your security score to uncover the areas that need stronger defense.

Get Your Security Score

sales@briskinfosec.com