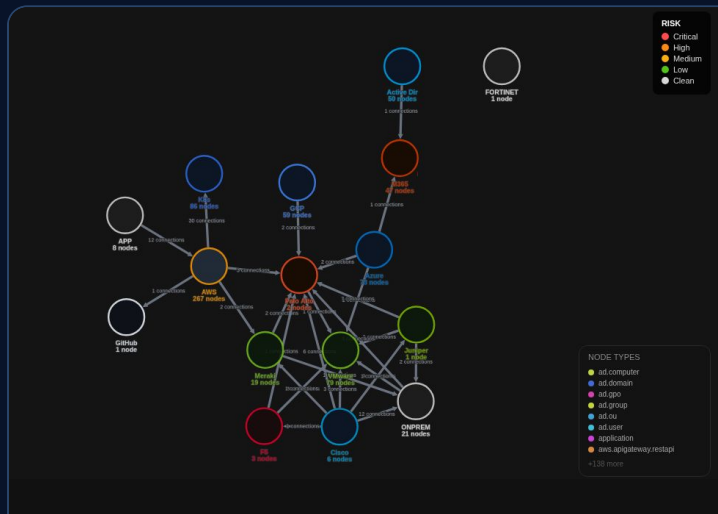


See the business. Prioritize the risk. Back it with evidence.

Connect infrastructure exposures to the applications and services your business depends on. Bring security, operations, and compliance teams together around one discovered infrastructure graph.



Actual demo topology · Sample data

FROM ASSETS TO BUSINESS SERVICES

Know which services need attention first.

Follow dependencies across cloud, on-premises, network, and identity. Combine potential attack paths, asset criticality, and vulnerability intelligence to focus investigation.

Roll findings into applications and business services, with ownership and dependency context that helps teams decide where to act.

01 / SECURITY

Focus remediation

Analyze routing, identity relationships, and chained findings. Use EPSS and CISA KEV context to prioritize exposures and provide actionable fix guidance.

02 / OPERATIONS

Keep pace with change

Inspect configuration and infrastructure-code drift, software inventory, DNS posture, and TLS certificates alongside the assets they affect.

03 / COMPLIANCE

Make evidence reusable

Combine technical checks with questionnaires and review workflows. Generate signed evidence, SOC 2 packages, and ISO 27001 assessment materials.

Built for enterprise and regulated environments.

Healthcare: understand infrastructure supporting patient care and ePHI. Financial services: connect exposures to critical services. Enterprise: align remediation and assessment work across teams.

Assessment support SOC 2 · ISO 27001 · HIPAA · PCI DSS · NIST CSF

Flexible operations SaaS and private deployment · ServiceNow GRC and Archer integrations

Capabilities vary by plan, module, and deployment. Assessment materials require organizational input and review.

Explore business-service risk →

infracast.io · info@azgardtek.com

Or start a 14-day Pro trial.