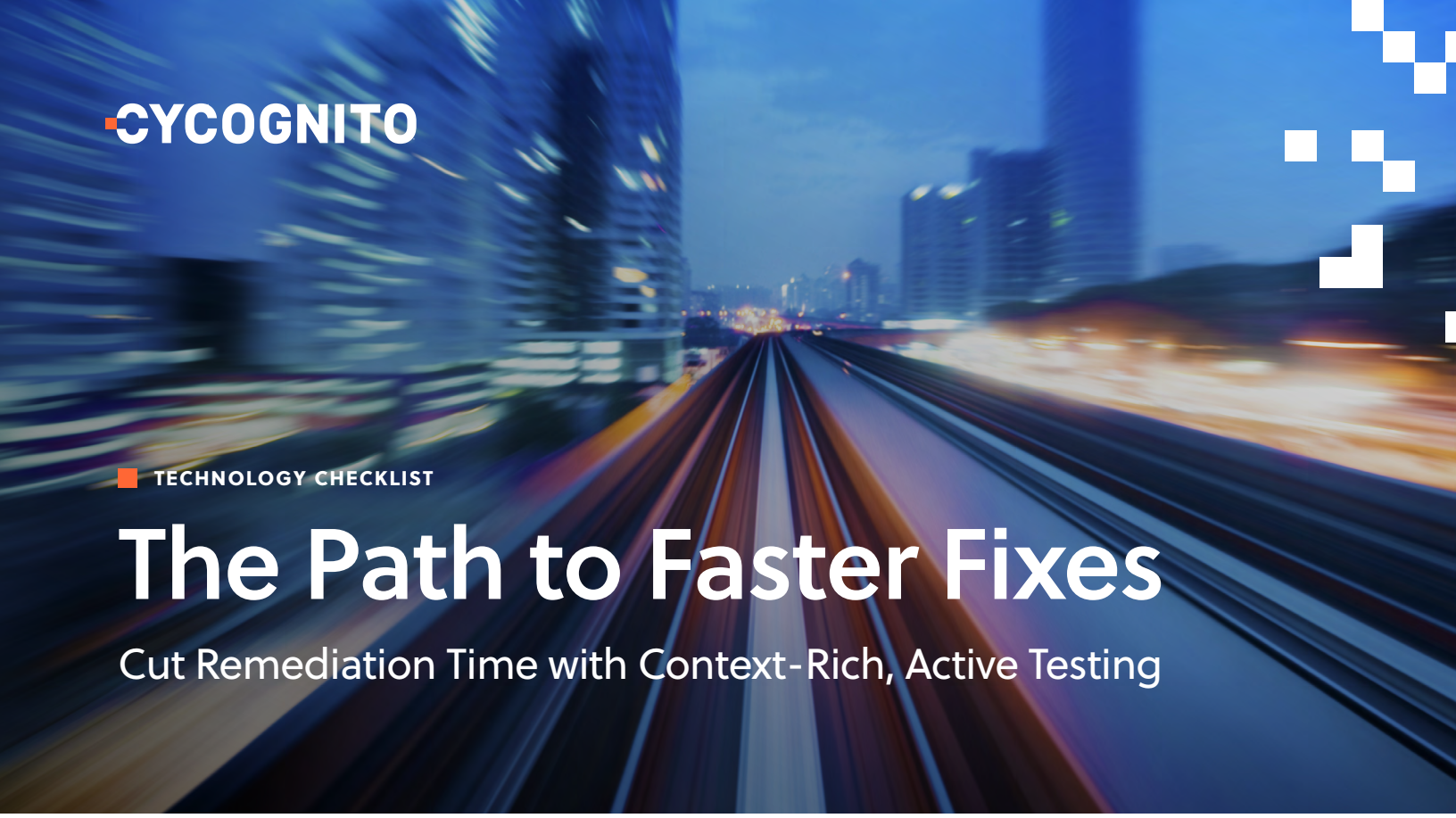

CYCOGNITO

TECHNOLOGY CHECKLIST

The Path to Faster Fixes

Cut Remediation Time with Context-Rich, Active Testing

Active testing delivers real risk visibility, enabling teams to fix what matters, faster. Use this checklist to ensure your organization is implementing scalable, automated testing practices that reduce both time to detection (TTD) and time to remediation (TTR).

To run more active tests you must overcome three challenges:

- Incomplete asset inventories
- Lack of business and attribution context
- Overreliance of inadequate testing levels and technologies

This check list provides guidance on how to address these challenges using automated testing technologies.

COVERAGE CHALLENGES

Incomplete Asset Inventories

What this is: Missing assets delay issue detection and extend dwell time. Infrequent assessment limits visibility into asset state and service exposure. Fully autonomous discovery is essential to eliminate blindspots from manual seed or configuration errors.

To solve this challenge,ensure your automated technology:

- ☐ Conducts **weekly** or **bi-weekly** asset discovery across all business units, both cloud and on-prem. Assets include:
  - ☐ Web applications
  - ☐ IP addresses
  - ☐ API endpoints
- ☐ Performs **daily** active scanning on known assets and infrastructure (e.g. port state, banners, services)

VISIBILITY CHALLENGES

Lack of Business and Attribution Context

What this is: Asset context connects vulnerabilities to risk. Without it, issue prioritization is difficult or incorrect.

To solve this challenge, ensure your automated technology:

- Conducts **bi-weekly** or **monthly** business structure mapping to feed into asset discovery workflows and attribution
- Attributes ownership (team, business unit at a minimum) to each asset
- Tracks asset location (e.g. cloud/on-prem/geo), platform (e.g. ASP.NET), and technology stack
- Tags assets by business function and type (e.g.

TESTING CHALLENGES

Overreliance of Inadequate Testing

What this is: Passive scans alone aren't enough to provide the confidence and depth your teams need to remediate issues. Fully automated active testing is a necessary component of "faster fixes".

To solve this challenge, ensure your automated technology:

- Runs **weekly** unauthenticated active testing across exposed assets running in production
  - Dynamic Application Security Testing (DAST) for web apps
  - Active testing for exposed services
- Provides exploitability evidence like a screenshot of unauthorized access to sensitive data or a session token used for account takeover
- Uses risk-based prioritization to inform prioritization order
- Retests to validate remediations and captures remediation duration per team, geography, system.

How Can CyCognito Help Your Organization?

The CyCognito platform scans and tests billions of websites, cloud applications and APIs to identify the most critical risks and guide your remediation efforts.

CyCognito customers benefit from:

- Autonomous seedless discovery and contextualization engine
- 80K+ automated tests
- Integrated DAST, risk scoring, and revalidation workflows
- Faster mean time to remediate (MTTR)

Check out our website and explore our platform with a self-guided, interactive dashboard product tour. To learn more about how CyCognito can help you identify and remediate emerging threats to your attack surface, request a customized demo.