Elevating Breach Resilience

Shifting from reactive compliance to continuous preventative security

The challenge:

The compliance paradox

Enterprises today face a daunting reality: despite significant investments in security policies and compliance frameworks, breaches continue to occur. Organizations often find themselves in a paradox where they appear compliant on paper, yet remain vulnerable to attacks. Attackers don't exploit policy binders; they target configuration drift, shadow IT, and the subtle weaknesses that emerge in fast-moving cloud environments.

Traditional security assessments are often snapshots in time—outdated the moment they are completed. Security Operations Centers (SOCs) are left in a perpetual state of reactive firefighting, cleaning up after incidents rather than preventing them.

KPMG Resolve:

Automating proactive prevention

KPMG Resolve is a daily automated cyber resilience solution that finds weaknesses attackers exploit to breach organizations—before they can be exploited. Our platform embeds the expertise of incident responders who've investigated hundreds of breaches to identify what will get you compromised.

Built for enterprise security teams managing complex, federated IT ecosystems, the platform scales breach risk assessment across subsidiaries, affiliates, or business units in a single resilience view. It delivers continuous, actionable intelligence on actual breach risks in Microsoft 365 and Azure environments—enabling proactive incident response instead of reactive forensics. With optional advisory services from KPMG LLP cybersecurity professionals, organizations can transform findings into remediation at unprecedented speed.

Key capabilities

Identity & access intelligence

Credential compromise remains the #1 attack vector. We provide deep visibility into your identity posture:

MFA coverage analysis

Detect users with missing or weak Multi-Factor Authentication (e.g., SMS/Voice).

Authentication hygiene

Identify legacy authentication protocols and password spray indicators.

Privilege management

Spot excessive user rights and "toxic combinations" of permissions that lead to account takeovers.

Application & cloud governance

Regain control over your cloud ecosystem:

Third-party risk

Audit OAuth2 permission grants and identify high-risk third-party applications with excessive access to your data.

Guest access

Monitor external guest accounts and sharing settings to prevent data leakage.

Supply chain defense

Detect malicious app registrations and expiring secrets that could be exploited.

Advanced attack path detection

Go beyond simple misconfigurations to identify complex kill chains:

Conditional access bypass

Identify pathways where weak device registration policies allow attackers to bypass security controls.

Device enrollment abuse

Detect scenarios where attackers can enroll rogue devices to achieve persistence or takeover accounts, even bypassing MFA.

Dormant app risks

Flag high-risk, unused applications that are susceptible to abuse or mishandling.

Strategic value from this approach

Reporting capability

Turn breach-risk assessments into board-ready and action-ready reports. The platform turns daily assessment data into clear, audience-specific reports—so technical teams get detail, executives get metrics, and compliance gets framework alignment. Every finding is tied to concrete evidence from your environment, so reports support both remediation and audit.

Three report types, one assessment:

- **Classic Assessment Report—Full technical analysis:** Threat-by-threat findings, risk priorities, protective controls, and complete evidence appendices. Built for security teams and technical remediation.
- **Executive Resilience Brief—High-level view for leadership:** Overall resilience score, domain scores (Identity, Data, Detection, Access, Compliance), cross-tenant comparison, and top findings only. Suited for CISOs, board updates, and executive status.
- **Security Manager Checklist—Action-oriented control view:** NIST 800-53 Rev 5 and CIS Controls v8 mapping, compliance status per control, control gaps with severity, and threat-to-control links. Suited for security managers, compliance audits, and remediation planning.

Why this stands out:

Evidence-linked—Every finding links to specific technical evidence (config, users, devices, policies). No "trust us"; everything is verifiable and supports conversations with technical and business stakeholders.

Aligned with industry—Leading practices like NIST 800-53 enrichment turns findings into control-level language, gap analysis, and coverage by control family and implementation group so you can demonstrate alignment with widely adopted frameworks and speak the language of auditors and security programs.

Flexible delivery—Generate on demand from the Reports page, download individual or bulk PDFs, and export data (e.g., JSON, CSV) for integration or further analysis.

Threat-centric focus

Findings are not just a laundry list of bugs; they are organized into primary threat categories based on real-world breach scenarios:

- Third-party compromise
- Credential misuse
- Insider threat
- Misconfiguration
- Impersonation & trust attacks
- External vulnerability

Designed for complex, federated organizations, the platform transforms due diligence and risk assessment from a weeks-long manual process into a rapid, data-driven operation. Whether for M&A due diligence or ongoing global monitoring, get detailed insights in days, not months.

Connect with us

Jordan Barth
Principal, Cyber & Tech Risk
KPMG LLP
E: jbarth@kpmg.com

Andrew Luckenbaugh
Manager, Cyber & Tech Risk
KPMG LLP
E: aluckenbaugh@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**