MICROSOFT CONTROL VALIDATION

Accelerynt Security Platform

Your Microsoft security controls are configured. Are they working? Now you can prove it.

Accelerynt Security Platform reads your Microsoft tenant configuration, maps it against your approved baseline and compliance frameworks, and shows you what's configured correctly, what's drifted, and what an attacker could reach. Findings arrive with the specific account, policy, or role attached, so your team acts on evidence instead of assumptions.

REAL-WORLD USE CASES

Compliance and Audit Readiness

Audit and compliance evidence lives across multiple consoles, and pulling it together manually takes weeks. Accelerynt Security Platform maps your Microsoft configuration state to NIST CSF 2.0, NIST 800-53, MITRE ATT&CK, CISA SCuBA, HIPAA, PCI-DSS v4.0, ISO 27001:2022, and the CIS benchmark family, fifteen frameworks from one scan. Evidence that used to take weeks is ready in minutes.

Attack Path Analysis

Your external exposure and internal misconfigurations live in separate consoles and separate reports. Accelerynt Security Platform combines them into one view, showing the path an attacker would follow from initial access to your data.

Change Management You Can Trust

Settings change. Microsoft ships updates, team members adjust policies, configurations drift. You see exactly what changed, who changed it, and when, compared against your approved baseline. Unauthorized deviations become auditable records.

Service Connection Oversight

Apps, automations, and service accounts across your Microsoft environment accumulate permissions faster than any team can manually track. The platform inventories and risk-scores them so you can find and revoke over-privileged or dormant connections before they become a liability.

Partner and MSP Access

Your partners and MSPs hold delegated admin privileges in your tenant. Accelerynt Security Platform audits GDAP roles so you see who has access, at what scope, and whether it's still justified.

Code Pipeline Validation

Your code pipeline is part of your attack surface. Accelerynt Security Platform evaluates Azure DevOps and GitHub against CIS Benchmarks so pipeline risk is validated alongside the rest of your Microsoft environment.

HOW IT WORKS

1 → 2 → 3 → 4

Scan in minutes

Connect once, hit scan, review findings in one place.

See your top risks

Findings name the specific account, policy, or role.

See the attacker's path

Findings connect into the paths an attacker would follow.

See what changed

Changes go on the record: what, who, and when.

CONTROL VALIDATION COVERAGE

Configuration state, attack paths, baseline drift, and compliance evidence across your Microsoft environment.

IDENTITY

- Conditional Access Policies
- Identity Controls & MFA
- Privileged Identity (PIM)
- Non-Human Identities

COLLABORATION & DATA

- Teams & Collaboration
- Data Loss Prevention
- Exchange Online

DEVICE & APPS

- Intune Management
- SharePoint & OneDrive
- App Registrations

CODE & PIPELINE

- GitHub (CIS Benchmarks)
- Azure DevOps (CIS Benchmarks)

EXTERNAL ATTACK SURFACE

- DNS & Domains (DMARC, SPF, DKIM)
- Asset Timeline
- Shadow Tenants

DEFENDER & PLATFORM

- Defender XDR
- Power Platform
- Microsoft Secure Score
- Copilot & AI

CLOUD PLATFORMS

Azure Foundations · AWS Foundations · GCP Foundations · Google Workspace

Connect your tenant. See your evidence.

Read-only access. First findings from your live environment in minutes.