

Contact Center Integration Security Checklist

AVOID HIDDEN RISKS. SECURE YOUR CX STACK.

Why This Matters

According to McKinsey, organizations take an average of 73 days to contain a breach, despite increasing cybersecurity spending to \$200 billion in 2024. The high costs stem from securing complex distributed cloud systems and third-party integrations, particularly in contact centers reliant on various technologies. Each connection poses a potential attack surface, especially as vendors transition from public to private cloud, introducing new vulnerabilities.

Checklist

- ☐ Audit all existing integrations to identify outdated or unused connections
- ☐ Remove deprecated APIs and inactive tools to reduce unnecessary exposure.
- ☐ Disable unused accounts and verify that active users require current permissions.
- ☐ Implement Role-Based Access Control (RBAC)
- ☐ Implement Single Sign-On (SSO) or federated identity management
- ☐ Enable Multi-Factor Authentication (MFA) across all CX systems
- ☐ Automate token and credential rotation to eliminate hardcoded or expired secrets.
- ☐ Monitor for anomalies to detect off-hours access, unusual activity, or large data exports.
- ☐ Scan for and remove shadow integrations created outside of official IT processes.
- ☐ Ensure backup and recovery processes are tested for any systems tied to core integrations.
- ☐ Work with InfoSec to vet all new integrations and ensure vendors meet security and compliance standards.
- ☐ Assign an internal owner for each integration to maintain accountability and lifecycle visibility.

"WE START ALL OF OUR SALES ENGAGEMENTS WITH A DISCUSSION OF SECURITY AND WE KEEP TALKING ABOUT SECURITY THROUGHOUT THE LIFECYCLE—BLUEPRINTING, ARCHITECTURAL DIAGRAMS, AND REVIEW BOARDS TO ADDRESS EVERY INTEGRATION POINT."

NEED HELP?

800.390.4866

CONTACT@AMCTECHNOLOGY.COM

AMCTECHNOLOGY.COM



FAQs

HOW FREQUENTLY SHOULD THE ACCESS CONTROLS BE REVIEWED AND UPDATED?

Access controls should be reviewed quarterly and updated immediately after role changes like promotions or departures. High-turnover environments may require monthly audits. Use IAM tools to automate provisioning and de-provisioning for efficiency.

WHAT STEPS SHOULD BE TAKEN IF A BREACH IS DETECTED THROUGH MONITORING?

First, contain the threat by disabling compromised accounts and revoking API keys. Next, investigate logs to determine scope, then notify stakeholders, including compliance teams if customer data is impacted. Remediate by patching vulnerabilities and rotating credentials. Finally, run a post-mortem to improve defenses.