Kiteworks

www.kiteworks.com

Safeguarding Customer Support Communications

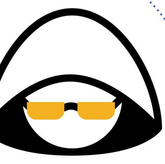
Takeaways From the Okta Customer Support Breach

The Okta customer support breach demonstrates the security risk exposure of customer service platforms

Key Risks

- Personal Customer Data Exposure
- IP and Source Code Theft
- Employee Credential Compromise
- Internal Data Leakage
- System Access Enabling Breaches

How the Breach Occurred



1. Hackers stole login credentials
2. Accessed Okta customer support portal
3. Downloaded HTTP archive (HAR) files containing:
   - Session cookies
   - API keys
   - Usernames/passwords
   - PII
   - Application code
   - Strategic documents
4. Impersonated users with stolen credentials

Essential Security Capabilities for Customer Support

1. Granular access controls
   60% of data breaches involve stolen credentials[1]
2. Encryption of data in transit and at rest
3. Activity logging and auditing
4. Consolidation onto a single platform
5. Security certifications such as SOC 2 Type II, ISO 27001, ISO 27017, and ISO 27018, FedRAMP, and others

[1] "2023 Data Breach Investigations Report," Verizon, March 2023.

Kiteworks Governs and Protects Sensitive Customer Support Data

- Zero-trust policy management limits data exposure
- Hardened virtual appliance provides layered security
- Consolidated content communications with comprehensive tracking and control
- Rigorous third-party audits and certifications of technology
- AES-256 encryption, including double encryption, protects breached data
- Granular access policies enforce zero-trust privilege
- AI-enabled anomaly detection identifies malicious activity proactively
- Detailed activity audit logs detect threats and demonstrate compliance with data privacy regulations

Schedule a custom demo of Kiteworks for secure customer support.

SCHEDULE NOW

Kiteworks