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 Information
- Card and Payment Data
- Employee Credentials
- Insider Threats
- Supply Chain Security

How The Breach Occurred:
1. Hackers stole login credentials
2. Accessed Okta customer support portal
3. Downloaded HTTP archive (HAR) file containing:
   - Credentials
   - Cookies
   - Device identifiers
4. Impersonated users with stolen credentials

Essential Security Capabilities for Customer Support:
- Granular access controls: 60% of data breaches involve stolen credentials
- Encryption of data in transit and at rest
- Activity logging and auditing
- Consolidation onto a single platform
- Security certifications such as ISO 27001, ISO 27017, and ISO 27020, FedRAMP, and others

Kiteworks Governs and Protects Sensitive Customer Support Data:
- Secure cloud platform: data encryption
- Automated access: improved security
- 40+ 195-195 encryption, including double encryption, protects sensitive data
- Secure, secure, and more secure: we know where data is

Schedule a custom demo of Kiteworks for secure customer support.

Kiteworks