WORKING GROUP TWO

Approach to **Security**

Introduction

Working Group Two's (WG2) mission is to provide a more useful and relevant mobile subscription through a programmable network core that operators can leverage to create innovative solutions.

Organizational Security

Building an industry-leading security program based on the concept of defense in depth with securing our organization and your data at every layer. Our security program aligns our work towards industry standards and best practices.

WG2 employees security engineers who's responsible for implementing our security program. Here we focus on Cloud and On-Premise Security Architecture, Product Security, Security Engineering and Operations, Detection and Response, Risk and Compliance, and Telecommunications Security. Company-wide developer and management security training is administered on a yearly basis.

Protecting Customer Data

Dedicated security personnel ensure that security is implemented in every stage of software development lifecycle to ensure the prevention of unauthorized access to customer data. Partnering with product teams across the company allows us to take exhaustive steps to identify and mitigate risks, implement best practices and constantly develop ways to improve our security.

Secure by design

WG2 has built a robust and secure development lifecycle, which identifies security threats early in the development process to ensure our APIs and services are secure. We use security threat modeling, a powerful analysis tool, as well as automated processes to identify vulnerabilities within our code and network misconfigurations that impact the security or privacy of our resources.

Encryption in Transit

All data transmitted between WG2 clients and our operator services is done using strong encryption protocols. WG2 supports the latest recommended secure cipher suites to encrypt all external traffic in transit, including TLSv1.x protocols, IPsec with AES128 encryption, and ECDHE ciphers.

Network Security and Server Hardening

WG2 divides its systems into separate networks to better protect sensitive data. Systems supporting testing and development activities are hosted in a separate network from systems supporting WG2's production infrastructure. All servers within our production infrastructure are hardened (e.g. removing default passwords, disabling unnecessary ports, etc.) and have a base configuration image applied to ensure consistency across the environment. Automatic security updates are applied on a regular basis.

Network access to WG2's production environment requires multi-factor authentication. A network-based intrusion detection system has been deployed across all environments to identify and alert on network anomalies such as data leakage, trojans, unauthorized access, backdoors, and brute forcing.

Endpoint Security

All endpoint hard drives are encrypted at rest. Phones are managed and company data can be wiped remotely if the phone is lost or stolen.

Access Control

Provisioning

To minimize the risk of data exposure, WG2 adheres to the principles of least privilege and role-based permissions when provisioning access. Employees are only authorized to access data that they reasonably must handle in order to fulfil their current job responsibilities. All production access is reviewed on a quarterly base.

Authentication

To further reduce the risk of unauthorized access to data, WG2 employs multi-factor authentication for all access to production web application portals and infrastructure systems, which could include highly classified data..

Password Management

WG2 requires personnel to use an approved password manager. Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks.

System and Network Monitoring, Logging, and Alerting

WG2 maintains an extensive, centralized logging infrastructure in its production environment which contains information pertaining to security metrics and system monitoring, availability and access. These logs are analyzed for security events via automated monitoring software, overseen by the security and on-call engineer.

Data Retention

Customer data, CDRs, is removed immediately upon deletion requests by the operator or upon the automated expiration of 21 days.

Disaster Recovery and Business Continuity Plan

WG2 utilizes services deployed by its hosting provider to distribute production operations across two separate physical locations. These two locations are within one geographic region, but protect WG2's service from loss of connectivity, power infrastructure, and other common location-specific failures. WG2 retains a full backup copy of production data in a remote location. Full backups are saved to this remote location every 24 hours with limited access.

Responding to Security Incidents

WG2 has an extensive 24/7 oncall program to quickly identify and remediate operational and security incidents. Dedicated security playbooks have been established to facilitate the proper handling of all security incidents. In the event of a security incident, all affected parties will be informed within 72 hours. Incident response procedures are tested and updated at least annually.

Penetration Testing

Internal penetration testing is performed on every new feature or service that impacts the security or privacy of our systems. This includes but not limited to APIs, web applications, and or network configurations.

Conclusion

Security is at the heart of WG2's engineering culture. Every person, team, and organization deserves and expects their data to be secure and confidential. We continue to work hard to ensure the safeguarding of this data. Please contact us at security@wgtwo.com if you have any questions or concerns.

WORKING GROUP TWO

wgtwo.com/**security**