Security at WorkWave

SUMMARY

WorkWave's mission is to provide secure solutions to companies in the Field Service, Workforce Management, and Fleet Management industries. Our applications automate, predict, digitize, and optimize business processes and tasks across the enterprise. Security is a key component in all our offerings and is reflected in our people, processes, and products. We're committed to being transparent about our security practices and want to help you understand our approach. This white paper outlines the security practices, policies, and infrastructure in place for our solutions and services.

INTRODUCTION

Our customers count on WorkWave for reliable and secure SaaS (Software as a Service) products that safeguard the reliability of our operations; protect customers' data; and security of our systems, products, services, and facilities. Our security measures ensure that business operations are highly available and customer data is protected from loss due to operational failures or security events.

OPERATIONAL SECURITY

Operational Security represents our security and risk management processes to prevent sensitive information from getting into the wrong hands. Further, it ensures all operations are running securely, ensuring the confidentiality of our customers' information.

Security Operations

WorkWave actively monitors our systems from external and internal threats at the application, server and network levels through a dedicated security operations team. Employee access to critical servers is restricted based on their role and requires multi-factor authentication with a strong password. Customer data backups are retained both on-cloud and off-cloud. We maintain logging and immutable audit trails of system activity for optimal system performance and to ensure accountability.

Incident Response

WorkWave has established policies and procedures to handle and respond to any potential security incidents that can directly or indirectly affect our infrastructure and services. We maintain and execute Security Incident Response Procedures in response to a wide variety of threats and work closely with our Engineering and external Security teams to identify and remediate vulnerabilities. Our incident response procedures are tested and updated on an annual basis or when a major change in infrastructure takes place. We respond to the security or privacy incidents reported to us through security@workwave.com, with high priority.

Vulnerability Management

WorkWave performs security audits on internal and external environments. Audits are performed by our in-house security team and credentialled third-party security vendors using certified vulnerability scanning tools and manual penetration test methods. Audit results are reviewed by WorkWave's Security Committee. Reported vulnerabilities are prioritized, tracked and resolved to eliminate the risk of known vulnerabilities.

Furthermore, our security team actively reviews inbound security reports and monitors public mailing lists, blog posts and wikis to spot security incidents that could affect the company's infrastructure.

Responsible Disclosure Program

We are committed to working with the community to verify, reproduce, respond to legitimate security issues, and implement appropriate solutions for the reported vulnerabilities. If you discover a vulnerability in our systems, products, or network infrastructure, WorkWave appreciates your help in disclosing it to our company in a responsible manner. Please submit any potential security issues at security@workwave.com. Note that WorkWave does not permit actively auditing our infrastructure without prior approval.

Secure Development Lifecycle

WorkWave has introduced 'Privacy By Design' and 'Secure-By-Design' methodology into our product development lifecycle. We use an agile development process that includes independent validation steps run by an independent quality team. A requirement of this process is to produce a validation report that includes security as a required signatory to the release process. Our Software Development Life Cycle (SDLC) mandates adherence to secure coding guidelines, as well as screening of code changes for potential security issues with our code analyzer tools, vulnerability scanners and manual review processes.

User privacy and security are evaluated during each stage of the development process to ensure only necessary data is collected to perform an application's task. Security measures are continually considered and deployed through new product releases and updates as deemed advisable as part of the product development/engineering process to keep pace with evolving security threats. Environment changes are reviewed and approved in advance to ensure system integrity.

TECHNOLOGY INFRASTRUCTURE SECURITY

Technology infrastructure security is the process of securing the network of electronic systems and devices that are configured, operated and maintained by WorkWave to provide various internal and external functions and services.

Cloud and Network Security

We employ rigorous safeguards and security measures to provide a secure environment for you and your customers. We employ a defense-in-depth strategy utilizing web application firewalls, multi-factor authentication, intrusion detection systems, intrusion prevention systems, audit and logging systems, restricted access controls, and encrypted access tools. Our systems are segmented into separate networks to protect sensitive data. Systems supporting testing and development activities are hosted in a separate network from systems supporting the production infrastructure.

Endpoint Security

All application endpoints employ network firewalls, web application firewalls, intrusion detection systems, DDOS mitigation, HTTPS TLS 1.2+ encryption and fully authenticated sessions to ensure the security of our applications. Sensitive servers and systems are deployed to private networks, behind load balancers, network firewalls and proxy servers to reduce our security footprint.

All workstations issued to WorkWave employees run up-to-date OS versions and are configured with anti-virus software and firewall. They are configured according to our formal corporate security standards. Workstations are secure by default to encrypt data at rest, have strong passwords, and get locked when idle.

Monitoring and Threat Detection

We employ advanced logging and monitoring of network, system, OS, application, database and cloud events. Logs are stored separately from production systems to ensure their integrity. We log more than a billion events each day to ensure the performance and security of our systems. Our anomaly-based intrusion detection and prevention systems receive regular updates from external threat intelligence sources and scan data against blacklisted signatures and malicious patterns to keep our infrastructure secure.

Identity and Access Control

WorkWave has established strict rules and processes around user access provisioning to minimize the risk of data exposure. WorkWave follows principles of least-privilege and role-based permissions when provisioning access. We employ technical access controls and internal policies to prohibit employees from arbitrarily accessing user data. Only designated and authorized WorkWave employees are allowed access to production systems and customer data. We restrict our employees' access to our environments to only those who have a need to access each specific application/function. We use role-based identity and access management to restrict low-level access. As an example, access to our cloud and network infrastructure is restricted to our production operations team (DNS, IP addresses, access to Amazon, etc). Every employee has specific login credentials and individual access rights.

User access audits are performed by the WorkWave Security team at regular intervals. Employees are required to use strong passwords with multi-factor authentication and SSO.

Reliability

WorkWave builds its products from the ground up with redundancy in place to protect against many failure scenarios. We employ farms of web and application servers to minimize the risk of single points of failure. Databases utilize real-time replication to allow immediate restoration of service in the event of failures. WorkWave leverages AWS services, including Availability Zones, Route53, Application Load Balancers, Auto-Scaling Groups, etc. to mitigate against the risk of partial service failures and to effortlessly scale as application volume increases. In the event of a disaster, WorkWave maintains a robust disaster recovery plan to resume operations in alternative AWS Regions with minimal data loss and within reasonable recovery time periods. By offering our SaaS products through the cloud we deliver cost-effective, highly secure, highly scalable and robust storage solutions for businesses looking to achieve efficiency and scalability.

Physical Security

WorkWave controls access to its physical resources including buildings, infrastructure and facilities. We provide employees, contractors, vendors and visitors with different access cards that only allow access strictly specific to the purpose of presence on the premises. WorkWave office building security monitors all entry and exit movements throughout our premises in all our business centers through CCTV cameras, deployed according to local regulations. Physical security of data centers is managed by data center location providers like AWS, Google and others.

DATA SECURITY

Data security focuses on protecting WorkWave and our customers' information against unauthorized access or use, and operational failures that could result in exposure, deletion, or corruption of that data. Data security exercises ensure we practice caution while handling sensitive data that passes through our systems. Our backup service provider maintains active SOC-1 Type II and ISO 27001-audited data centers to ensure the reliability and consistency of the data.

Availability and Disaster Recovery

All WorkWave systems are highly available, employing redundant systems and networking to ensure continuous service in the event of failures. We maintain multiple redundant backups of data across multiple cloud providers and different geographic locations. Customer databases are replicated to failover nodes with a typical latency of seconds to protect against failures in primary systems. Additionally, customer databases are backed up daily to allow data restoration in the event of a larger application or environment issue that causes data loss. WorkWave also maintains multiple production environments and the ability to create additional production environments, which allows WorkWave to rebuild an environment from scratch to ensure system availability. In the event of a recovery event, WorkWave has defined DR plans to ensure a coordinated and quick response.

Data Protection and Encryption

All databases are backed up and stored in four separate and encrypted physical locations to provide the highest resiliency against data corruption and ransomware threats. Document storage is backed by Amazon's S3 service to provide the highest levels of security, resiliency and availability.

WorkWave utilizes encrypted communications systems for its products and for sensitive customer communications (Virtru). WorkWave leverages Multi-Factor Authentication (MFA) to secure access to production systems and employee productivity tools and systems.

We don't allow sensitive personally identifiable information (such as social security numbers or credit cards) in our databases. Sensitive customer information, such as passwords, is encrypted at the database level and in some products stored as one-way salted hashes.

We support and enforce (via HTTP-to-HTTPS redirect) TLS to encrypt all data transmissions from web browsers to our servers and to our external partners, ensuring no man-in-the-middle interceptions of data. We utilize network firewalls to control access to our network and applications. In addition, all user and API sessions are authenticated to ensure security is maintained during transactional events at a system level.

PRIVACY AND COMPLIANCE

Data privacy and compliance programs at WorkWave are focused on how personal information and data are collected, used, shared and processed, consistent with the expectations of the individual and applicable laws, regulations, professional practice requirements and contractual obligations. Every year WorkWave is rigorously audited by independent third-party companies to ensure that we comply with various global and regional standards governing information security.

Privacy

WorkWave makes every effort to preserve the privacy of our users and customers. Our detailed privacy statement can be found **here.**

Governance, Risk and Compliance

All production changes undergo rigorous and SOC-1 certified change management processes. Further, changes are reviewed regularly by the WorkWave security team. We frequently conduct vulnerability scans and penetration tests to improve the security of our cloud environments. Our accreditors are experts in their respective fields with a deep understanding of the different global and regional laws and standards that must be complied with. They thoroughly assess WorkWave's processes and controls against these standards, verifying that they are met or exceeded at all times. When the audit reports are complete, we make them available to customers by request.

We follow ISO 27001, GDPR, PCI DSS and SOC-1 guidelines for risk management, change management, data privacy and security. WorkWave engages with a third-party ASV to conduct quarterly un-credentialed network scans. Reports are reviewed and issues remediated based on priority and complexity. WorkWave also engages with the same third party to conduct credentialed manual penetration tests against applications in PCI DSS scope.

Compliance Certifications

WorkWave works with leading audit firms to certify our adherence to industry-standard compliance programs and regulations so you can have confidence that your company and customer data is secure and compliant.

Certifications: PCI DSS, SOC-1 Type 2, SOC-2 Type 2, Privacy Shield, GDPR

EMPLOYEE AND PARTNER SECURITY

WorkWave follows strict guidelines while onboarding new vendors, employees and contractors to ensure our customers are in safe hands. Further, we ensure our employees have the knowledge and skills to perform their roles effectively while protecting security. This helps WorkWave to prevent and mitigate user and partner risk.

Training & Certification

WorkWave has created a culture of security that covers all employees. All employees are required to take privacy and security awareness training on a regular basis. Engineering and operations employees receive additional job/function-specific training and certification to be informed, adaptable and responsive to whatever risks may arise. Furthermore, we evaluate their understanding through tests and quizzes to determine where they need further training.

Background Verification

Each WorkWave employee undergoes a process of background verification. We hire reputable external agencies to perform this check on our behalf. Subject to per-country restrictions, we verify criminal records, citizen status, previous employment records if any, and educational background. Until this check is performed, the employee is not onboarded or assigned tasks that may pose risks to customers. Failure to pass these tests will result in either mandatory disqualification from the employment process or a further follow-up investigation.

All employees and contractors are required to sign a non-disclosure agreement and review and confirm their understanding of the WorkWave Employee Handbook and Ethics policy along with the Acceptable Use Policy. This confirmation is recorded electronically.

Vendor Security

WorkWave utilizes third-party technology vendors to provide additional functionalities and software integrations. We take appropriate steps to ensure our security requirements are maintained by vendors at all times, using our vendor management policy. We onboard new vendors after understanding their processes for delivering us service and performing risk assessments. We take appropriate steps to ensure our security stance is maintained by establishing agreements that require the vendors to adhere to confidentiality, availability and integrity commitments we have made to our customers.

All of our products are hosted at top-tier cloud hosting and data center vendors such as Amazon Web Services, Microsoft Azure, and Edgeconnex, and accordingly are protected by the rigorous security standards and mechanisms of those hosting providers as well, such as automated security scans to identify malware, suspicious or malicious traffic or other types of security incidents. WorkWave evaluates vendor security at least annually.

For information related to WorkWave's offerings and how they may differ, please contact your WorkWave account representative.