NETROADSHOW INFORMATION SECURITY

Security is a top priority at NetRoadshow. We have been the Market Standard and trusted global leader in hosting online roadshows for the global banking community since 1997.

SECURE BY DESIGN

The core tenets of NetRoadshow's security program are to safeguard customer data and to maintain customer trust.

NetRoadshow uses a defense-in-depth approach to implement layers of security throughout our organization. We're passionate about defining new security controls and continuously refining our existing ones.

Our security program is driven not only by compliance and regulatory requirements, but also by industry best practices like the OWASP Top 10, CIS Critical Security Controls and threat intelligence.

SECURITY CULTURE

All NetRoadshow employees and contractors undergo background checks prior to employment. The consequences of problematic background check results may range from a limitation of security privileges to revocation of employment offers. Our background checks cover: County, State, and Federal criminal search histories, Sex offender search, employment history, and credit history.

We have security policies for ensuring the integrity, confidentiality, and availability of all customer data and protecting that data against any unauthorized or unlawful access, use disclosure or destruction.

PRIVACY AND PROTECTION

NetRoadshow works hard to maintain the privacy of data you entrust with us. We put our security program in place to protect your data, and use it only as permitted in our Terms of Service and Privacy Policy. We never share your data across customers and never sell it. NetRoadshow is committed to ongoing GDPR compliance and will work with clients to execute Standard Contractual Clauses and Data Protection Agreements to document how NetRoadshow uses and protects Personal Data.

DISASTER RECOVERY AND BUSINESS CONTINUITY

NetRoadshow services are hosted in AWS and are configured to withstand long-term outages to an AWS Availability Zone. We have a fully redundant system across AWS regions in US-EAST-1 and EU-WEST-1 to maintain the availability of our applications to our clients.

There are no critical servers and no client data stored in any of our offices and on our corporate network. In the event that any of our offices suddenly becomes inaccessible, employees will find alternative, remote work places, potentially coordinating to physically co-work in order to optimize productivity.

If any disaster occurs, whether a fire, weather related, political or pandemic, causing NetRoadshow's physical offices to be affected, local authorities would be contacted for assistance to ensure the safety and security of our employees.

SECURE SINGLE SIGN-ON AND DEVICE VERIFICATION

NetRoadshow can integrate with industry standard SAML 2.0 single sign-on (SSO) solution so that team members can log in to NetRoadshow using their SSO credentials. This eliminates the need for your users to have separate NetRoadshow credentials, ensuring only the right users have access to your data, and enables you to apply the same authentication policies to NetRoadshow as you do with your other enterprise applications. Session inactivity accounts are set for each application so that no forgotten sessions are lingering open on employee devices.

ENCRYPTION IN-MOTION

NetRoadshow's policy is that all TLS endpoints accessed exclusively by NetRoadshow employees support TLS 1.2 and 1.3.

ENCRYPTION AT-REST

All persistent data is encrypted at rest using AWS/KMS, which encrypts all data using AES-256 ciphers. This is managed in AWS, whose security practice implementation has successfully earned SSAE-16 compliant SOC 1, SOC 2, and SOC 3 certifications.

SOFTWARE DEVELOPMENT AND MONITORING

NetRoadshow practices secure coding according to the recommendations of the OWASP Project and CIS.

Source code and configuration files are stored in private git-based repositories. These tools support code attribution and code reviews. Reviewers check for compliance with NetRoadshow's conventions and style, potential bugs, potential performance issues, and that the deploy is bound to only its intended purpose.. Multiple scanning tools in the CI pipelines also perform static analysis and automated tests for quality, security, and unit validation.

Secrets, such as password and encryption keys are not stored in the repository. All secrets are stored in AWS Secrets Manager or AWS CloudHSM devices in the case of TLS secret keys.

Once integrated for deployment, code is scanned with the OWASP Zap tool to find unit and integration vulnerabilities. All vulnerabilities are fixed prior to any release being pushed into production.

All major components of incorporated open-source software libraries and tools are reviewed for robustness, stability, performance, security, and maintainability. The security and development teams establish and adhere to a formal software release process.

CODE REVIEWS AND PRODUCTION SIGN-OFF

All changes to NetRoadshow source code destined for production systems are subject to pre-commit code reviews by a qualified development peer that includes security, performance, and potential-for-abuse analysis.

Prior to updating production services, all contributors to the updated software version are required to approve that their changes are working as intended on staging servers. All changes are required to adhere to the document change management process.

SECURITY TRAINING

The security team maintains a company-wide, computer-based security awareness program delivered to NetRoadshow employees upon hire and annually thereafter. The program covers security awareness, policies, processes, privacy, and training to ensure that employees are sufficiently informed to meet their obligations.

Development employees receive additional mandatory quarterly training which focuses specifically on software and development security topics.

EMPLOYEE ACCESS

NetRoadshow follows the principle of least privilege when it comes to server access, writing software, diagnosing and resolving problems, and supporting customers. Employees are only granted enough access to meet the task at hand, and no more. Access control reviews are conducted on a quarterly basis to ensure that least privilege is maintained throughout the organization and employees do not have access beyond what is required to do their job.

We use AWS IAM to verify employee account identity and require two-factor authentication for all internal applications without exception. Administrative permissions are enforced where applicable and all administrative access is logged and auditable from traditional web server logs and CloudWatch/CloudTrail.

PHYSICAL SECURITY

We leverage AWS data centers to provide infrastructure and hosting services for our applications. Amazon AWS exceeds all industry standards for physical security, including 24/7 surveillance and biometrics. All data is hosted within their secure data centers. AWS undergoes various third-party independent audits on a regular basis and can provide verification of compliance controls for its data centers, infrastructure, and operations. This includes, but is not limited to, SOC 1, 2, and 3 certifications, as well as ISO 27001 certification.

INFORMATION SECURITY PRACTICES

NetRoadshow practices infosec in depth, combining the recommendations of SOC2 CIS and a wide variety of tools to protect our systems and customer data. Our approach is SOC2 Type 1 certified and approved by infosec reviewers at all of the 10 largest international banks.

Some of the solutions we leverage include:

INTRUSION DETECTION AND PREVENTION

NetRoadshow uses two tiers of IDS/IPS systems to detect and prevent intrusions at the device level and at a per-request, application level.

We employ Crowdstrike IPS in all cloud environments to provide protection to every server and containerized device. This offers broad and dynamic attack detection and reaction with visibility across all cloud endpoints. We also utilize the ModSecurity IDS/IPS inside ingress and egress point to prevent intrusions that might attempt to hide in valid requests. All detections are logged to a centralized log system and sent to an distribution group for review.

For Conference system steams, we employ Fortinet’s Fortiguard for IDS/IPS.

ENDPOINT SECURITY AND ENCRYPTION

We deploy a Mobile Device Management (MDM) system called WorkSpace ONE. WorkSpace ONE is loaded on all corporate laptops and desktops and is centrally monitored. Monitoring capabilities include remote wipe in the event a corporate device is lost or stolen. WorkSpace ONE ensures that USB ports on all corporate devices are blocked from being used as writable devices on the machines.

All laptop hard drives have Bitlocker encryption, which is installed via WorkSpace ONE. Bitlocker encrypts data stored on the hard drive with an AES 256-bit key. All corporate laptops also have Crowdstrike anti-virus installed. Crowdstrike is locked from being disabled by all end users.

All corporate and personal mobile devices that have access to corporate email and data must have VMWareOne (IntelligentHub) installed on it. IntelligentHub containerizes all corporate information (including email) on each person’s mobile device. Those containers are segmented from the rest of the phone and can be remote wiped in the event a device is lost or stolen. All devices are managed through compliance and configuration policies.

EMAIL DLP

We use Mimecast as our internal Data-Loss Prevention (DLP) tool to monitor email. All outbound emails are scanned based on a set up reference dictionary which incorporates rules from GDPR, CCPA, GLBA, PCI, etc. Suspect emails are quarantined for review prior to being released. Mimecast is also used as our web filtering tool to block employee access to non-approved sites on all corporate devices.

PENETRATION TESTING

All NetRoadshow applications are pentested via a third-party company on an annual basis. Information about any security vulnerabilities successfully exploited through penetration testing is used to set mitigation and remediation priorities. Results and findings are properly documented and presented to the management team for each application upon completion. All critical issues identified during testing are addressed within 45 calendar days of the date the issue is identified. All issues identified during testing are ranked based on the risk to the organization. Each issue is tracked from initiation to completion by a member of the Information Security Team.

NetRoadshow will provide a summary of penetration test findings to customers upon request.

VULNERABILITY SCANNING

We run Nessus scans on a weekly basis to test for both vulnerabilities and compliance, which includes software version rules. Upon completion of a scan, a member of the Information Security Team reviews and ranks the vulnerabilities and presents those findings to the DevOps team for remediation.

APPLICATION EXTERNAL CV

We use DigiCert as our certificate authority for SSL certificates for our applications' web sites. DigiCert is one of the most trusted certificate authorities in the market today.

AUDITING AND LOGGING

We maintain audit logs on all systems. These logs provide an account of what personal has accessed which systems. Access to our logs are restricted. Security events are logged, monitored, and addressed by our Information Security team. Network components, workstations, applications and any monitoring tools are enabled to monitor user activity. Organizational responsibilities for responding to events are defined in our Incident Response Policy. Security events that record critical system configuration changes and administrators are alerted at the time of change. Retention schedules for logs are defined in our Information Security Policy.

CONTINUOUS MONITORING

We utilize both internal and external services to perform continuous scanning and monitoring of our network and applications. We conduct weekly vulnerability scans, annual risk assessments and penetration testing.

ANTI-VIRUS/ANTI-MALWARE

Crowdstrike is installed on all user endpoints and servers as our Anti-Virus/Anti-Malware solution. It has centralized configuration and logging. Signature updates happen automatically every 24-48 hours. CrowdStrike analyzes and neutralizes any potential threats in real time.

SECURE SOFTWARE DEVELOPMENT

We have in place Secure Coding Standards that are tailored to addressing the standard OWASP vulnerabilities. We leverage industry standard front-end frameworks such as VueJS and AngularJS to help provide standard protection against common vulnerabilities. In addition, our Secure Software Development Process involves several layers of defense to address these sorts of vulnerabilities including STRIDE/DREAD threat analysis, peer code reviews, security testing, and dynamic scanning of our application for every major release, as well as external penetration testing.

SECURITY POLICIES

NetRoadshow maintains an internal set of security policies, which are reviewed at least annually. Our security policies cover a wide array of security related topics ranging from general standards with which every employee must comply, such as account, data, and physical security, to more specialized security standards covering application and network security and information systems. For copies of these polices for review, please contact our Information Security Department.

NetRoadshow maintains an Information Security Policy, Acceptable Use Policy and Code of Conduct that defines employee's responsibilities and acceptable use of information system resources. The organization receives signed acknowledgement from users indicating that they have read, understand and agree to abide by the rules of behavior.

If you or any member of your team have any questions or would like further information detailing into one or all of these security controls, please email security@netroadshow.com and one of our InfoSec team members will be in touch.