Inscene Company B.V. / Networkapp

IT Security Statement

Content

IT Security

Last update 2 July 2018

We take the security of your data very seriously at Networkapp. We aim to be as clear and open as we can about the way we handle security. If you have additional questions regarding security, we are happy to answer them. Please write to info@networkapp.eu and we will respond as quickly as we can.

1.1 User Security

[1] Passwords: Best practices are in place for storage of user application passwords. User application passwords have minimum complexity requirements. Passwords are individually salted and hashed.

[2] Data Portability: Networkapp enables you to export your data from our system in excel format so that you can back it up, or use it with other applications.

[3] Privacy: We have a comprehensive privacy policy (see https://networkapp.eu/en/disclaimer/) that provides a very transparent view of how we handle your data, including how we use your data, who we share it with, and how long we retain it.

[4] Data Residency: All Networkapp user data, is stored on servers located in Frankfurt, Germany and Zürich, Switzerland.

[5] Encryption in Transit: All communications with the Networkapp website, systems and third party suppliers are sent over TLS connections, which protects communications by using both server authentication and data encryption. This ensures that user data in transit is safe, secure, and available only to intended recipients. Our application endpoints are TLS only and score an "A" rating on SSL Labs' tests.

1.2 Network Security

[1]Server protection: The environment that hosts the Networkapp services maintains multiple certifications for its data centers, including ISO 27001 compliance, PCI Certification, and SOC reports. For more information about their certification and compliance, please visit the AWS Security website and the AWS Compliance website.

[2]Firewalls: Firewalls are configured according to industry best practices and unnecessary ports are blocked by configuration with AWS Security Groups.

[3] Access Control: Access to Networkapp servers is based upon pub/private key authorization and limited with IP.

1.3 Availability

[1] incident management: We understand that you rely on the Networkapp services to work. We're committed to making Networkapp a highly-available service that you can count on. Our infrastructure runs on systems that are fault tolerant, for failures of individual servers or even entire data centers. Our operations team tests disaster-recovery measures regularly and staffs an around-the-clock on-call team to quickly resolve unexpected incidents.

[2]Uptime: We perform continuous uptime monitoring, with immediate escalation to Networkapp staff for any downtime.

[3] Backup Frequency: Backups occur daily at multiple geographically disparate sites.

1.4 Organizational & Administrative Security

[1] Personnel Practices: Employees receive security briefing during onboarding as well as on an ongoing basis. All employees are required to read our security policy en internal procedures. All of our employees and contract personnel are bound to our policies regarding Customer Data (security and confidentiality).

[2] Information Security Policies: We maintain internal information security policies, including incident response plans and password policies and regularly quarterly review and update them.

[3] Service Providers: We screen our service providers and check if they have the appropriate confidentiality and security measurements in place if they deal with any user data.

[4] Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis.

[5] Internal procedures are in place for storage of personal data that belongs to our clients and is not actively used in the Networkapp platform.

1.5 Vulnerability Management

[1] Patching: Latest security patches are applied to all operating systems, and network infrastructure to mitigate exposure to vulnerabilities.

[2] Bug Bounty: We take the security of our platform very seriously! Networkapp runs a private bug bounty program to ensure our applications are continuously reviewed for vulnerabilities.

[3] Penetration Testing: Starting from January 1st 2017 external organizations will be invited to perform penetration tests at least annually.

[4] Third Party Scans: Our environments are continuously scanned using security tools. These tools are configured to perform application and network vulnerability assessments, which test for patch status and basic misconfigurations of systems and sites.

1.6 Software Development Practices

[1] Stack: We code in Python and run on MySQL and Ubuntu.

[2] Coding Practices: Our engineers use best practices and industry-standard secure coding guidelines which align with the OWASP Top 10.

[3] Deployment: We frequently deploy code, giving us the ability to react quickly in the event a bug or vulnerability is discovered within our code.

1.7 Responsible Disclosure

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if Inscene Company / Networkapp learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with Dutch government guidelines.

1.8 Your Responsibilities

Keeping your data secure also depends on you ensuring that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems, to keep any data you download to your own computer away from prying eyes.

If you wish to keep the information shared at your event as private as possible, we advise you not to share the event code on your website, twitter or other internet medium. Or choose the option to send out personal login codes for each of your guests.