Security and Data Protection Overview

January 2022

MARCH networks

Contents

Contents

Contents

1. Introduction

Over the past several years, data protection, privacy, and cybersecurity have moved from behind-the-scenes activities to front page news, emerging as a strategic priority for every company that handles personal customer data.

March Networks has a long history of delivering secure products. Since 2000, we've developed enterprise-class networked video solutions for organizations that demand only the highest cybersecurity standards from their vendors. From day one, the principle of privacy-by-design has guided our product development, and we've incorporated features that limit unauthorized access to our devices. We continue to work closely with our customers, partners and legal counsel to understand and address varying data protection requirements around the world.

March Networks is constantly evaluating and enhancing our business policies and practices, and the security of our products.

March Networks is committed to building a secure digital environment that allows business activities to be safe and to prosper and to protect customers' information and networks. Our risk-based cybersecurity approach is focused on protecting the company's employees, assets and customers' information. All reasonable efforts are made to assure integrity, confidentiality & availability of our products, networks, systems and data.

March Networks is taking a strategic and proactive approach to manage cyber risks. This document outlines the practices we take to be able to adapt to continually evolving threats. With objectives covering a combination of innovative cybersecurity technology, security compliance processes and security aware employees, this risk-based strategy enables March Networks to be resilient and put in place the proper actions to respond to eventual attacks. Our main goals are:

1. Develop secure software/hardware products and protect customers.
2. Increase security of our company's networks, systems and data.
3. Develop a cyber-aware workforce.
4. Continuous improvement of cybersecurity posture.

The majority of our policies, processes and procedures contain confidential information, proprietary to March Networks, and may not be distributed outside the organization. We have therefore prepared this document to identify and give a brief overview of the security practices in place at March Networks.

2. High Level Security Summary

- Designing inherently secure, data-protected solutions is part of March Networks' DNA, tracing back to our deep roots in information technology and networking. Our holistic approach to cybersecurity involves a 360° view of all aspects of our business, encompassing our products, the people who build them, and the processes that guide us. We're also committed to helping our customers understand and address cybersecurity and data protection as it relates to video surveillance and video-based business intelligence.

People

- Deep heritage in information technology and networking
- Background checks on developers working with product code in the company's Canadian R&D Center of Excellence
- Secure, access-restricted Network Operations Center (NOC)
- Corporate offices and R&D labs access card protected
- All employees participate in annual cyber security training

Products

- Extensive list of product features and capabilities to support video data authentication, anonymization, encryption and anti-tampering, flexible retention, multi-video streaming and configurable resolution
- Solutions already compliant with the European Union's previous data protection directive 95/46/EC
- Interactive Security Audit tool via our free GURU Smartphone App
- Product hardening guide

Processes

- Follow security-by-design principles in our product development and business systems
- Participate in extensive security audits with Fortune 500 customers
- Operate an extensive Security Updates and Advisories program; proactive, transparent and available to all customers and partners via our website
- Conduct annual penetration testing of internal business systems
- Cyber Essentials Canada certified, designating March Networks a cybersecure business

- March Networks products are designed with cybersecurity in mind. Our network video recorders (NVRs) and IP cameras pass rigorous IT testing, including ethical hacks to assess and resolve potential cyber weaknesses. The Linux-based operating systems in our NVRs are custom-built to help safeguard against vulnerabilities, and March Networks products use a sophisticated one-time password mechanism.
- Because cybersecurity is a joint effort, March Networks also develops tools to help our partners ensure the security of their video surveillance installations. Our industry-first GURU Smartphone App helps our partners by analyzing how secure the configuration of installed March Networks recorders is against a list of potential weaknesses. It then recommends ways to harden the system, such as changing a default password.

- March Networks takes a proactive approach to cybersecurity communications. We have a dedicated team who monitors our products for vulnerabilities and communicates all necessary information through our Security Updates and Advisories program. With this program, we are committed to: 1) assessing a vulnerability once we've been alerted to it, to determine if it affects our products; 2) addressing the vulnerability via a patch or software release, if required; and 3) communicating with our partners.
- March Networks is taking a proactive approach leveraging the NIST Framework to effectively mitigate the cyber risks we are exposed to. The NIST Cyber Security Framework integrates industry standards and best practices to help organizations manage their cybersecurity risks. We have put in place and continuously improve access control and intrusion prevention processes and technologies. However, we also recognize successful attacks may occur and we're prepared to detect and respond.
- March Networks is CyberSecure Canada certified. CyberSecure Canada is a certification program developed by the Canadian government in collaboration with Innovation, Science and Economic Development (ISED) and the Communications Security Establishment (CSE). The accreditation is a formal, independent and demanding process that ensures certified organizations like March Networks are able to meet security control standards and demonstrate their technical competency in handling cybersecurity.
- Because data breaches can occur anywhere in an organization, March Networks employees constitute the first line of defense against cyber threats. All March Networks employees undertake mandatory cybersecurity training. Training is completed annually, and covers best practices for Internet security and maintaining data privacy and integrity.

3. Physical Security

March Networks implements commercially reasonable security practices and procedures that meet or exceed standard industry practices. March Networks headquarters is a secured facility, requiring an employee access card to enter the premises. Physical security measures in place include:

- Access to March Networks facilities is controlled. Employees are only issued appropriate access devices to gain entry to areas where they perform their job duties.
- Sensitive areas like the Network Operations Center (NOC) have restricted access and extra security measures, including biometric and video monitoring.
- Video surveillance cameras are throughout the facility, including at all entrances and restricted areas.
- All visitors are required to sign a visitor log and must be escorted by a March Networks employee.
- Entry/visitor logs are reviewed regularly and stored for one year.
- Documented processes and procedures related to the prevention, detection, investigation and reporting of actual or potential physical security incidents.
- A program for the identification, logging, tracking, escalation, and management of all physical security incidents in order to properly respond to and manage incidents, as well as identify potential trends that may indicate that new or enhanced controls are required.
- Annual security awareness and training program includes physical security topics such as, prevention of tailgating/piggybacking, reporting suspicious persons/activities, etc.
- Communication of physical security best practices to employees through online training and/or email updates.
- Server rooms are armed with high temperature, water (leaks) and breach alarms, as well as video surveillance cameras. Documented processes are in place when outside access (for maintenance) is required.

4. Network Security

March Networks has a Network Security Policy to protect our information assets, employees, customers, and partners from external threats inherent in network usage. The documented corporate security policies, procedures, frameworks, and guidelines are used to protect our corporate assets, safeguard the confidentiality, integrity of availability of our information assets, to ensure continuity of services, and to provide the highest level of protection for our internal clients, as well as the customer base which purchases our products or subscribes to our services.

The documented corporate security policies, procedures, frameworks, and guidelines are used to protect our corporate assets, safeguard the confidentiality, integrity of availability of our information assets, to ensure continuity of services.

4.1 Critical Assets

- March Networks identifies and continuously updates a list of critical networks, systems, and data.
- Based on their categorization, critical assets benefit from different appropriate levels of protection.
- Data protection processes are based on our Data Classification Policy. Customer data benefits from the highest confidentiality level.

4.2 Network Protection

4.2.1 Network Access Control

- March Networks has implemented network logical access control solutions including proper users' identification, authentication and authorization components.
- Access is provisioned based on a least privilege approach.
- Critical assets benefit from reinforced access controls including VPN and multi-factor authentication.
- March Networks has a documented policy in place that governs elevated access rights of admins of the various systems at the company. All admin transactions are logged.

4.2.2 Firewall

- All March Networks offices are protected behind a network of redundant firewalls.
- Our public cloud presence benefits from the same level of firewall protection.
- Firewall configurations and rules changes are managed through a formal process.
- All Internet access from the March Networks network is via a March Networks IT-approved path that passes through a firewall.
- Inbound and outbound traffic is prohibited by default until there is a specific firewall rule to allow it.

4.2.3 Antivirus

- All March Networks on-premise servers, cloud servers and end-point devices are protected by an antivirus solution.
- Virus definitions are automatically updated using a cloud-based solution. End-point devices are updated as soon as they connect to the Internet.

4.2.4 Patch Management

- March Networks has a proactive approach to patch management. Where possible, patches are applied automatically to our systems and network devices.
- Patch management for systems and network devices that require special attention is done regularly following a pre-defined schedule for each system and device.
- Vulnerability scans are conducted on a regular basis and vulnerabilities are addressed in a timely manner.

4.3 Security Audits

- March Networks hires a third-party security consulting firm to conduct network security audits on an annual basis. We also conduct a comprehensive penetration test against all Internet facing assets at least on an annual basis.
- Recommendations from security audits and penetration tests are reviewed and remediated in a timely manner based on relevance and levels of importance and urgency.

5. Data Protection

5.1 Data Governance

March Networks has defined a data governance process to support the protection of company and customers' data. Data is a vital company asset and our policies and practices are designed to ensure it is used securely, efficiently, and legally.

- Our practices are based on the concept of Need to Know. No information will be disclosed to any person who does not have a legitimate and demonstrable business requirement to have access to the information.
- Data management roles and responsibilities have been clearly defined and divided among data owners, data custodians, and uses.
- Data is classified based on confidentiality category and potential impacts levels.

5.2 Encryption

- A variety of latest encryption technologies and protocols such as: HTTPS, TLS 1.3, SFTP, SSH, etc., are leveraged in order to protect company and customers' data from malicious interception.
- Highly sensitive company and customers' data is encrypted at rest.
- All devices deployed to our employees benefit from hard disk encryption at rest.

5.3 Secure Data Destruction

- All decommissioned hard drives, USB drives, or any other hardware that contains company or clients' confidential information are destroyed rendering the data completely unrecoverable.

6. Incident Response Plan

Our incident response plan is focused on timely and efficient response management to incidents compromising the confidentiality, integrity or availability of our critical networks, systems and data.

March Networks has a formally documented incident response plan outlining detailed guidelines for managing information security incidents.

March Networks has a formally documented incident response plan outlining detailed guidelines for managing information security incidents. Our plan is structured in three phases:

Phase 1: Prevent, Plan, Prepare, Detect, Analyze and Contain

- **Prevent:** Even though it is impossible to completely eliminate cyber risk exposure, preventing attacks from happening remains the best incident response possible. We leverage a set of physical and logical security measures and technologies to prevent incidents from happening (access controls, firewalls, antivirus, patch management, security awareness training, security audits, etc.)
- **Plan & Prepare:** We've identified the individuals involved in our Incident Response team and clearly defined their roles and responsibilities.
- **Detect, Analyze & Contain:** Our IT/Security team uses a set of modern technologies and practices to detect and analyze potential incidents including (but not limited to) systems availability, performance monitoring, logs analysis, etc. Analysis is based on the potential business/functional impacts, type of compromised data, and recoverability. In the case of an incident, we take immediate actions to stop the unauthorized practice, isolate the impacted areas and revoke compromised access.

Phase 2: Communicate

- **Communicate:** We've documented communication requirements as part of our regional-based privacy breach policies. In case of an incident, we have established the list of internal and external stakeholders to be notified.

Phase 3: Eradicate & Recover

- **Eradicate:** Containment work will evolve into eradication by doing additional area isolation, reducing access privileges, network and systems scanning and patching, clean-up, and proceeding to systems and data restoration.
- **Recover:** Once the root causes of the incident have been eliminated and extra measures have been taken to protect from future threats, the Incident Response team will work on restoring affected systems and networks to their normal operations and enabling customers and business groups to safely gain access to their systems and data.

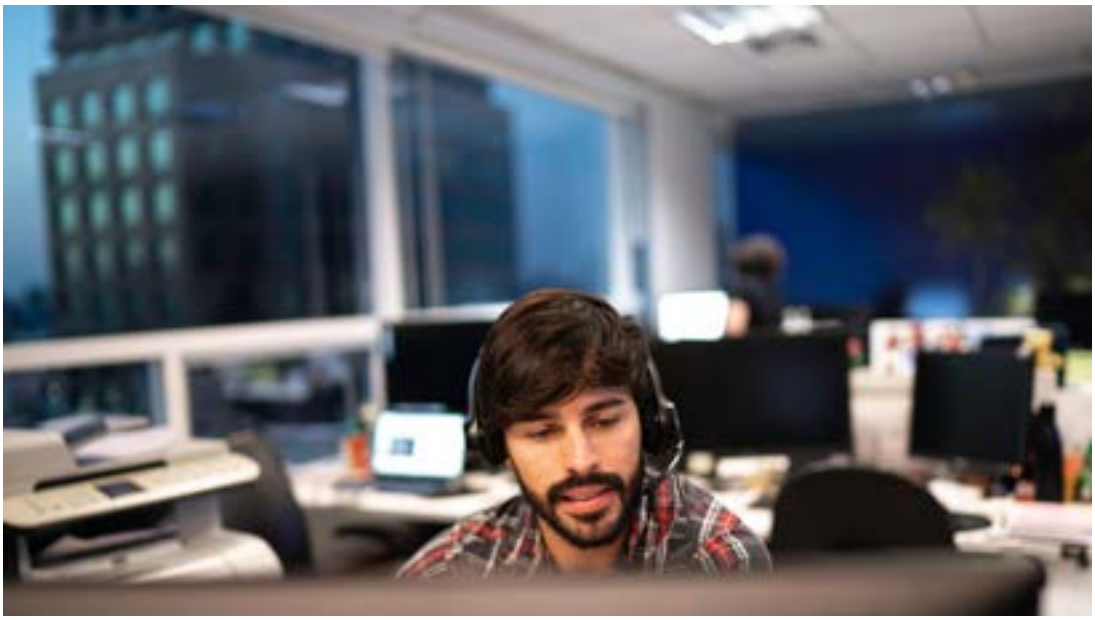
7. Change Management

7.1 IT Change Management

- March Networks has a documented IT Change Management Process to ensure the effective management of changes while reducing risk. Key components include:
  - Formal, defined Change Management Process
  - Accurate documentation
  - Consistent test planning and execution
  - Continuous oversight
- March Networks Change Management Process and Procedures cover a multitude of activities including identifying and obtaining business authorization for change requests, user testing, management approval, deployment of the change into the production environment, and monitoring.
- Established change control procedures are followed to ensure only authorized changes are moved into production. All security updates and patches are installed in a timely manner and require proper testing and preparation of a backup plan prior to implementation.

7.2 Emergency Changes

- The Emergency IT Change Management Procedure may be used for critical priority issues that require immediate attention.
- The Emergency IT Change Management Procedure document details the procedure that will be followed to effect all emergency changes in the IT Business Application and Infrastructure environment at March Networks. The procedure is used when a system outage or issue is impacting business flow and there is a critical and immediate need to resolve the problem.
- The procedure has been established with best practice approach to General Computing Controls surrounding effecting emergency actions to restore system functionality.
- In the event that an emergency change is required, post-change monitoring and oversight must be employed, which can also act as the testing and approval.
- Documentation of the control points for the emergency change must be retained.



8. Back-Up And Disaster Recovery

Back-ups are an organization's last line of defense in defending data integrity.

- March Networks back-up strategy has been designed to protect corporate data and the intellectual property of the company, and to preserve data integrity.
- The strategy and documented Back-up Policy will allow the company to restore any data that has been accidentally deleted, or destroyed due to system error or corruption.
- Back-ups are completed based on a pre-defined schedule that varies from hourly to daily depending on business needs and data sensitivity.
- Regular verification and integrity checks are conducted.
- All business critical systems are backed up and stored offsite.
- Data is retained based on standard information retention best practices and has several layers of protection built into our strategy.
- All March Networks' customers data, company data and business systems and configuration are backed-up multiple times per day into our Disaster Recovery solution. The Disaster Recovery solution is based on a combination of cloud-based components for extremely fast recovery of critical systems and data and an off-site solution for the remainder of the systems and data.

All March Networks' customers data, company data and business systems and configuration are backed-up multiple times per day into our Disaster Recovery solution.

9. Product Features And Development

9.1 User Access Logs

March Networks Command Enterprise is capable of generating audit reports detailing user access history including all actions.

9.2 Customer Security Controls

- The security of a Video Surveillance network is dependent on the entire ecosystem, including device manufacturers, integrators, service providers, as well as the end user organization. Following industry best practices and March Networks' recommendations associated with device configuration can decrease the risk associated with security vulnerabilities. The March Networks' Product Hardening Guide is a specific document that explains how to improve the strength of your March Networks solution. The document helps to identify security vulnerability exposures associated with the configuration of March Networks products. The Product Hardening Guide provides recommendations for technicians and system administrators installing March Networks products within a customer's network to help ensure security.
- In addition to the **March Networks' Product Hardening Guide** we recommend customers also adopt the practices suggested in our *Data Protection and Privacy Application Note*, which describes how March Networks products should be deployed and configured to address data protection and privacy concerns.

When we learn of potential vulnerabilities, our team conducts immediate, in-depth investigations across our product lines.

9.3 Security Vulnerability Assessment & Incident Management

9.3.1 Product Vulnerability Scanning and Monitoring

- March Networks is committed to ensuring the ongoing security and reliability of its products. We strive to proactively address security threats as they are reported by the US Computer Emergency Readiness Team (US-CERT). When we learn of potential vulnerabilities, our team conducts immediate, in-depth investigations across our product lines. If appropriate and required, immediate action is taken to prepare software/firmware updates. These alerts are sent out through the security email distribution list.
- Our documented Security Vulnerability Assessment Procedure outlines the internal process to be followed with the goal of maintaining the security of March Networks supported Products and Software Releases.
- Various sources of information, including the Common Vulnerabilities and Exposures (CVE) reports, are used to monitor for reported security vulnerabilities in software employed in our products.
- As part of standard practice, March Networks maintains and executes vulnerability scans with tools in our labs prior to releasing new software for customer use.
- Products are monitored for potential vulnerability threats based on a number of methods, including but not limited to:
  - Static Application Security Testing (SAST)
  - Dynamic Application Security Testing (DAST)
  - National Vulnerability Database (NVD) Monitoring
  - Potential vulnerabilities identified and reported by Independent Security Professionals or Customers
  - External Penetration Testing
- Identified vulnerabilities are individually reviewed and assessed to analyze the issue and determine appropriate action. If necessary, mitigation strategies and remediation plans are developed.
- If March Networks determines that a security vulnerability ranked with a severity of high or critical, as identified by the NVD CVSS (Common Vulnerability Scoring System), affects it's supported products, a patch or security fix is released to address such vulnerability in a timely manner.
- Previous security updates impacting March Networks products are listed on our security advisories page, along with the corresponding software versions in which the vulnerability was addressed. Online subscription is available to receive March Networks Security Updates and Advisories email alerts.

9.3.2 External Audits

On a periodic basis, March Networks evaluates the opportunity to employ a third-party vendor to conduct penetration testing on specific products. These third-party vendor audits of critical security controls are performed to identify vulnerabilities, risks and gaps.

9.3.3 Guru-Security Audit Tool

- The March Networks GURU application for smartphones and tablets has a Security Audit feature to help system integrators improve the security of their video surveillance installations. The audit capability available in GURU automatically analyzes and rates how secure the configuration of installed March Networks recorders is against a list of potential vulnerabilities. It then provides guidance on how to make the configuration more secure with a list of recommendations on ways to harden the system, such as changing a password or closing ports.
- The GURU Security Audit is a configuration hardening tool to help identify security vulnerability exposures associated with the configuration of March Networks NVRs. A failure to follow March Networks recommendations or industry-best practices associated with device configuration may increase the risk associated with security vulnerabilities. The security of a video surveillance network is dependent on the entire ecosystem, including device manufacturers, integrators and service providers, as well as the end user organization.

9.4 Software Development Practices

March Networks uses Agile/Scrum Software Development Methodologies. All software changes follow a strict code review policy. Testing and validation is done using a set of manual and automated Unit, System, Regression, Integration and Acceptance tests. Impact analysis is performed for changes and changes are ported to affected releases.

9.5 Software Development Change Management Process

All software changes follow a Configuration Management (CM) process. Changes are identified and tracked through a CM tool, linking the reason/description of change, affected releases and source changes together. All changes follow a workflow throughout the process ensuring that designated stakeholders review and approve.

10. SaaS Application Security

The infrastructure environments we use to host our Software-as-a-Service (SaaS) applications and hosted services benefit from the same security measures as our internal networks and systems. Our security approach is based on risks, critical systems and sensitivity of data. Customer data benefits from high levels of protection. On top of the network and infrastructure level security measures, we've taken additional actions to protect our SaaS applications and services:

10.1 Application Level Identity Management And Access Controls

All March Networks hosted applications include user level user name/password access controls. This includes the Insight Service, hosted Command Enterprise Software (CES), Searchlight for Retail as a Service, Health Compliance Solution, and Evidence Vault. In addition:

- Our Insight Monitoring and Resolution Service uses two-factor authentication, which provides secure oversight of access to the application, data, and reporting.
- Searchlight for Retail as a Service and hosted CES recently added security health alerts that warn when there are too many login attempts using incorrect passwords. This safeguards against Denial of Service (DoS) attacks.

10.2 Data Transfer Encryption/Protection

All March Networks hosted applications ensure that data transfer is encrypted and secure. Communication to hosted applications is through either secure web interfaces (HTTPS) and standard encrypted socket communication protocols (TLS, DTLS) that ensure protection and integrity of data.

10.3 Secure Apps Development Lifecycle

March Networks creates and verifies all our hosted applications using documented and monitored development processes. For example, our Insight Service is based on a highly secure third-party applications development platform that includes regular security updates. The platform benefits from very robust security practices evaluated within ISO27001 certification and SOC 1/2/3 audits. Development activities are conducted within this secure framework.

10.4 Threat Management

- All March Networks hosted applications execute on systems protected by a multi-layered threat management solution, including an Intrusion Prevention System (IPS) and malware and antivirus detection. Our threat management solution is updated automatically with the most recent virus and intrusion definitions.
- Antivirus and intrusion protection databases are dynamically updated on a continuous basis.

All March Networks hosted applications execute on systems protected by a multi-layered threat management solution.

10.5 Data Back-Up / Redundancy / Disaster Recovery

- Full back-ups of all hosted application data are automated to occur on a daily basis.
- Our hosted applications are cloud-based and are deployed with internal processes that include standby redundancy and disaster recovery (if required).

11. Human Resource Management

11.1 Employee Recruitment

- March Networks recruitment process is conducted in accordance with the local employment, labor, and human rights legislation.
- Reference checks are conducted to verify references and accomplishments (i.e. education, experience, certificate verifications).
- For certain positions more extensive verifications, including background checks and/or criminal record checks, are conducted, where permitted by law. Criminal background checks are conducted on all Sales Engineers, Technical Support Personnel, and Software Developers.

11.2 Employee Termination

When employees/contractors leave the organization and/or employment is terminated, all access rights are promptly removed. March Networks Human Resources notifies IT of all employee terminations and access is removed on the date of termination.

11.3 Security Awareness Training Program

- March Networks has implemented a consistent, comprehensive Security Awareness Training program with Internet security training, strict adherence to compliance regarding knowledge of Network Acceptable Use policies, and ongoing simulated attacks to test effectiveness of the training.
- All staff complete a review of relevant security policies upon hire and periodically when a policy is updated. All employees and contractors are provided with and accept the Network Acceptable Use Policy, Privacy Policy, and are required to sign a confidentiality agreement.
- Ongoing testing such as directed phishing and spear phishing attacks are performed by the IT department. Senior Management is informed of testing results on an ongoing basis. Anyone failing these tests at any point after taking the initial training is required to re-take the training as mandated in the Network Acceptable Use Policy.

12. Privacy

March Networks respects the privacy of its customers and understands the need for appropriate protections of personal information.

- March Networks uses Personal Information (information collected about its affiliates, customers, consultants, users, channel partners, strategic partners, resellers, suppliers, contractors, and distributers (including their employees)) in order to manage its relationships, provide information about products and services, to deliver products and services to customers, and to meet any legal or regulatory requirement.
- March Networks endeavours to maintain appropriate physical, procedural, and technical security with respect to its offices and information storage facilities to prevent any loss, misuse, unauthorized access, disclosure, or modification of Personal Information.
- Personal Information is further protected by restricting access to it to those employees that need to know the information in order that March Networks may provide its products, services, or information.
- Our Public Privacy Policy can be found at www.marchnetworks.com/public-privacy-policy/.

13. Insurance

March Networks maintains errors & omissions insurance covering liability for technology-related security incidents with extended Cyber Liability coverage. Upon written request, March Networks can provide a certificate of insurance evidencing coverage and limits. March Networks will deliver notice of cancellation or modification of such policy coverages and limits to its customer(s) in accordance with its insurance policy provisions and contractual obligations.

14. CyberSecure Canada Certification

March Networks has achieved CyberSecure Canada certification, developed by the Canadian Centre for Cyber Security, Canada's authority on cyber security. In order to become certified, an organization must effectively put into place the requirements of the 13 security control areas developed by the Centre. Examples of these control areas include developing an incident response plan, using strong user authentication, providing employee training, and backing up and encrypting all data. After implementing all of the 13 requirements, an organization must go through a thorough audit by an accredited certification body. March Networks is pleased to have been successful in the implementation of these stringent requirements.

Associated Documents

- March Networks' Product Hardening Guide
- Data Protection and Privacy Application Note
- March Networks Public Privacy Policy

Revision History

Version	Date	Revision Details
1	August 6, 2020	Initial release of document
2	January 2022	Update to document

Questions? Contact Us

Should you have additional questions about any of our products, please contact your March Networks sales representative, call us at +1 613 591 8181 or email us at info@marchnetworks.com.

Document Release Date: August 6, 2020
Document Revision Date: January, 2022

North America 1 800 563 5564
Latin America . . . . . +5255 5259 9511
Europe . . . . . +39 0362 17935
Asia . . . . . +65 6818 0963
Australia and New Zealand . . . . . +61 1300 089 419
Middle East and Africa . . . . . +971 4 399 5525