Compliance

- NDAA-compliant
- CyberSecure Canada Certified
- Committed to European Union General Data Protection Regulation (EU GDPR)
- Lifecycle Policy

Data Protection

- End-to-end encryption
- Linux-based OS for NVRs

Network Security

- 802.1x Certificate Management
- X.509 Certificate Monitoring
- Server Name Identification (SNI)

Access Management

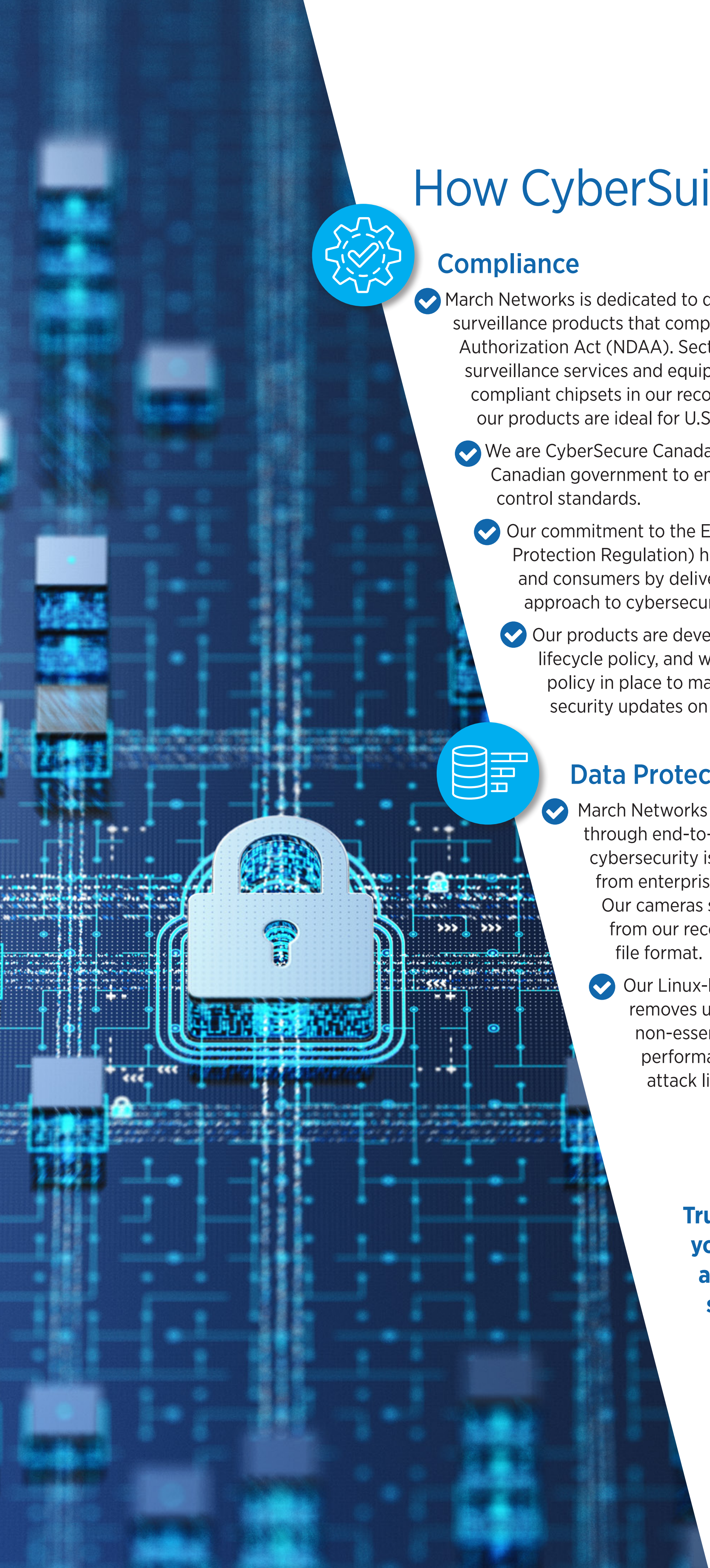
- Single Sign-On (SSO)
- Two-Factor Authentication (2FA)
- Active Directory (AD)
- CyberArk

March Networks CyberSuite

Introducing the March Networks CyberSuite, a comprehensive cybersecurity and data protection solution. Our CyberSuite is designed to ensure your operations remain secure, efficient, and compliant with stringent industry standards. It encompasses robust data protection measures, advanced network security protocols, streamlined access management, and adherence to global regulations. The March Networks CyberSuite safeguards your network against unauthorized access and cyber threats. Discover how our cutting-edge solutions can help you build a secure and trustworthy network environment.

Leading the Future of Intelligent Video Solutions

MARCH® networks
A Delta Group Company



How CyberSuite Works for You

Compliance

- March Networks is dedicated to delivering secure, highly reliable IP video surveillance products that comply with the John S. McCain National Defense Authorization Act (NDAA). Section 889 of the act prohibits certain video surveillance services and equipment from specific vendors. By using NDAA-compliant chipsets in our recorders, cameras and edge devices, we ensure our products are ideal for U.S. installations subject to the NDAA.
- We are CyberSecure Canada certified, a program developed by the Canadian government to ensure organizations meet stringent security control standards.
- Our commitment to the EU GDPR (European Union General Data Protection Regulation) helps safeguard the personal data of individuals and consumers by delivering products developed with a complete approach to cybersecurity.
- Our products are developed following a strict software development lifecycle policy, and we have a security vulnerability and support policy in place to manage new issues in the field, providing security updates on our Partner Portal and public website.

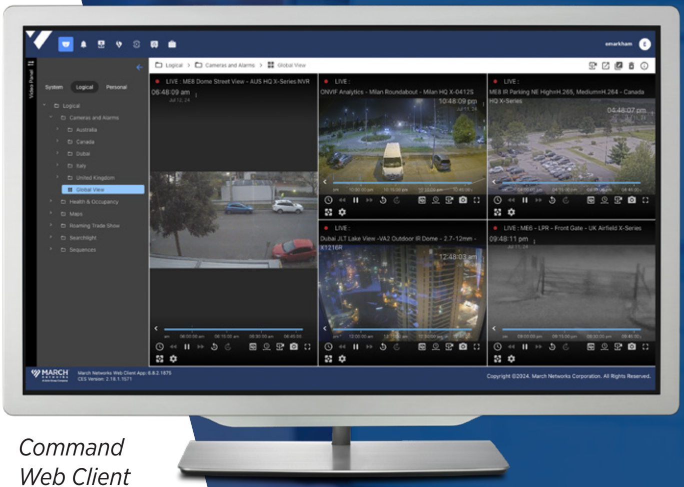
Data Protection

- March Networks ensures the highest level of data protection through end-to-end encryption, preventing potential cybersecurity issues from camera streams to recorders and from enterprise management systems to client software. Our cameras support RTP/RTSP over HTTPS, and media from our recorders is exported in a custom encrypted file format.
- Our Linux-based OS on all March Networks recorders removes unnecessary services and applications, locks non-essential network ports, and optimizes system performance to minimize defects and reduce attack likelihood.

Trust our advanced tools to protect your network against unauthorized access and cyber threats while simplifying user management and enhancing operational efficiency.

Network Security

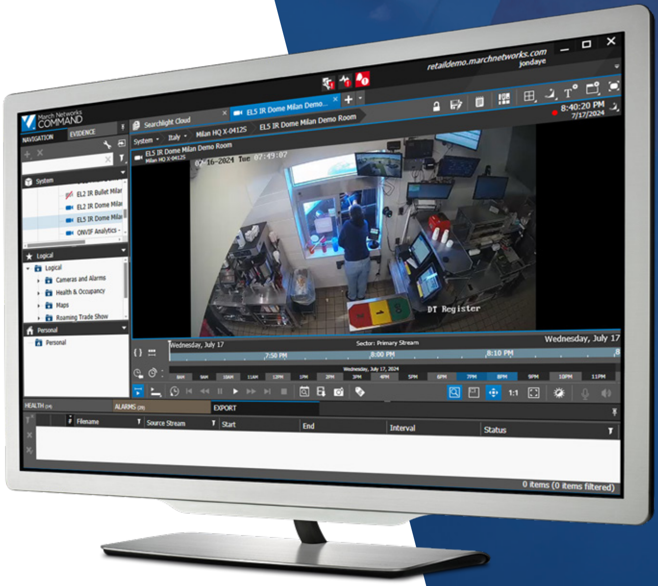
- The 802.1x Certificate Manager, thanks to a user-configurable certification authority (CA), allows convenient certificate management through our Command Enterprise Software (CES), which controls access to switches, allowing only authorized devices and monitoring and renewing certificates as they expire.
- Thanks to a user-configurable certification authority (CA), the X. 509 Certificate Monitoring allows convenient management of certificates that enable HTTPS through our CES, monitoring and renewing certificates as they expire.
- The Server Name Identification (SNI) certificate is used for secure communication with our Web Client. Without this certificate, accessing the Command Web Client results in a “not secure” message. Adding the certificate makes it a secure and trusted website.



Command Web Client

Access Management

- Single Sign-On (SSO) is compatible with Command Enterprise Software (CES). SSO allows users to sign in once and access multiple applications with the same credentials without repeated logins. SAML 2.0 is the protocol used for communication between our enterprise management system and identity providers like OKTA and Sailpoint.
- CES implements Two-Factor Authentication (2FA), which is a security method requiring two forms of identification to access resources and data, enhancing identity and access management. Our 2FA uses standard time-based one-time passwords and is compatible with apps like Google Authenticator and Microsoft Authenticator.
- Active Directory (AD) lists users and permissions to network resources, simplifying user management by allowing the addition of users as groups in CES while IT manages group memberships. CES communicates with a customer’s AD over the LDAP protocol, primarily for on-premise systems and allowing external access through SAML 2.0 and Single Sign-on (SSO). LDAP is the industry-standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol network.
- CyberArk, an enterprise service that controls and frequently changes system credentials, integrates with CES and audits use and access to other systems, such as databases and LDAP directories.



Command Enterprise Software

CyberSuite

Scan Here to Learn More

MARCH networks®
A Delta Group Company

060-3509-00-A

marchnetworks.com