Nx Witness
VIDEO MANAGEMENT SYSTEM

Cyber Security

“IoT without security = Internet of Threats”

- Stephane Nappo, Global Chief Information Security Officer at Société Générale International Banking

Network Optix designs our software products to provide high levels of protection against both external and internal cyber security threats. In this document we outline the most common types of cyber security threats, the technologies and process methods we use to secure Powered-by-Nx systems, and some of the proactive environmental approaches our customers can take to prevent the most common types of cyber threats.

What is a Cyber Attack?

A cyber attack is a malicious and deliberate attempt by an individual or organization to breach the information system of anotherindividual or organization.

Why do people / organizations launch Cyber Attacks?

According to Cisco cyber attacks are most often used for ransom - with 53% of cyber attacks resulted in damages of $500,000 or more. Cyber attacks are also sometimes initiated as a form of “hacktivism” with a goal of disrupting normal business operations. In the IP Video world cyber attacks are often executed in an effort to cover up criminal behavior that has been captured.

Common Types of Cyber Attacks

There are many types of cyber attacks that exist - below we outline the most common.

MALWARE

Malicious software that installs on computers through a vulnerability in an operating system or a piece of software.

Malware could potentially be used to intercept user credentials and video streams, or cause the user’s Nx Witness System to function poorly due to interruption in system or network resources caused by the Malware.

PHISHING

Phishing is a method of sending fraudulent communications - usually email - which mimic a reputable source in order to obtain login credentials.

Nx Witness’ Secure Password Reset functionality ensures passwords are able to be reset / recovered quickly in such an instance.

MAN-IN-THE-MIDDLE

This type of attack occurs when the attackers insert themselves into the middle of communications between two parties in order to intercept sensitive data. Typically this is accomplished by monitoring network traffic or through the use of Malware.

Nx Witness secure communications capabilities - including OpenSSL connections, HTTPS communications, and encrypted video traffic - were engineered to address this type of attack.

SQL INJECTION

SQL injection occurs when a malicious actor inserts code into a server running an SQL database that forces the server to reveal information.

Nx Witness utilizes the OWASP standard for prevention of SQL injection attacks and employs additional obfuscation techniques.

ZERO DAY EXPLOITS

A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented.

Nx Witness monitors market news regularly and updates our customers about Zero Day vulnerabilities as they emerge, are documented, and are addressed.

USER ENUMERATION

In password-based attacks, hackers use software and brute force attacks to access secure accounts.

Nx Witness has minimum password standards, an invalid login timeout, and a secure password reset / recovery method for Nx Cloud connected Systems.

DISTRIBUTED DENIAL OF SERVICE

This type of attack is designed to flood systems, servers, or networks with traffic to exhaust resources, effectively killing the system’s ability to perform normally.

Nx Witness’ secure communications (SSL, HTTPS, Cloud Proxy, Secure Connections, and Encrypted Video) help to prevent DDOS attacks and server health monitoring provides the ability for operators to diagnose DDOS attacks in real-time.

SOCIAL ENGINEERING

The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Nx Witness allows for fast reset / recovery of passwords in the case of theft of credentials.

Nx Witness’ Audit Trail feature allows administrators to review all operator actions.

Nx Witness
VIDEO MANAGEMENT SYSTEM

Cyber Security

Cyber Security Protections

Nx Witness VMS is continually improved to address the cyber security threats listed above by using a combination of secure technology and process measures outlined below.

USER RIGHTS MANAGEMENT

Nx Witness has advanced User Rights capabilities that allow Administrators to implement strict controls over what operators are able to accomplish in the system and which resources they are allowed to configure and interact with.

USER RIGHTS

Single system owner with super user rights
Customizable user rights & roles

AUDIT TRAIL

All user actions are logged for review by System Administrators

PASSWORD PROTECTIONS

Nx Witness requires a minimum level of security when creating passwords.

PASSWORD SECURITY

Minimum password strength during account creation
Secure password reset via Nx Cloud
Complex Multi-Level Salted/Hash password storag
Two Factor Authentication (Cloud only)

USER ENUMERATION DETECTION

Nx Witness Server and Cloud applications detect and prevent user enumeration (brute force attacks, guess and confirm attacks) through the use of timeouts.

INTEGRATION WITH LDAP

Integration with LDAP enables centralized management / reset of IT credentials by IT administrators.

> “A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted.”
>
> - Kevin Mitnick, Mitnick Security Consulting

DATA INTEGRITY CHECKS

Nx Witness includes many protections for system communications over both secure (e.g. LAN/WAN/VPN) and unsecure (e.g. Internet) networks.

OPEN SSL FOR NETWORK CONNECTIONS

By default deprecated and insecure protocols are disabled in lieu of TLS v1+. The Transport Layer Security protocol aims primarily to provide privacy and data integrity between two communicating computer applications.

- Server -> Client (Mobile, Desktop, Web) Communications -HTTPS
  HTTPS is used by default for all connections.
- Email - TLS / SSL
  TLS is the default option for the Email Server.

ENCRYPTED CLIENT-SERVER COMMUNICATIONS

System administrators can choose to encrypt VMS communications with the “allow only secure connections” option in System Administration settings.

ENCRYPTED VIDEO TRAFFIC & ARCHIVES

System administrators can choose to encrypt all video traffic between Clients and Servers with the “encrypt video traffic” option and encrypt archives (128 AES).

CUSTOM SSL CERTIFICATES

Nx Witness supports the use of Custom SSL certificates.

CLOUD CONNECTION PROXY

Nx Cloud securely proxies remote connections to systems, removing the need to open or forward ports on secure networks.

RISK PREVENTION METHODS

Network Optix also institutes processes to ensure threat assessment and resolution is part of our core culture. These steps include:

EXTENSIVE QUALITY ASSURANCE TESTING

Nx Witness VMS undergoes rigorous Quality Assurance testing prior to release to identify and remedy vulnerabilities.

EXTERNAL SECURITY AUDITING

Nx Witness VMS undergoes regular external security testing and auditing.

ONLINE SUPPORT PORTAL

Network Optix maintains a global support presence with an active support portal and community forum at http://support.networkoptix.com. Customers and partners are encouraged to report issues and work with proactive support team members who are able to remotely assist customers with any issue.

REGULAR PATCHES

Nx Witness provides regular monthly patches at http://my.networkoptix.com which address emerging security threats and reported bugs.