Naverisk

Technology Management Solutions

Security Summary

April 2018

Contents

Introduction....3
1.0 Protection of Communication Channels....3
1.1 Website....3
1.2 Remote Control....3
2.0 Naverisk Network Protocol (NNP) Connections....4
3.0 Data Protection....4
4.0 Application Security....5
4.1 User Authentication....5
5.0 EU General Data Protection Regulation (GDPR)....5

Introduction

This document's purpose is to give an overview of technologies and models used to provide a secure environment for Device Management.
Security covers:

- Protection of communication channels, to prevent sensitive data being obtained by third parties, and to prevent third parties from being able to gain control over part or all of the Naverisk system or the Devices it manages.
- Protection of data, to avoid data loss.

1.0 Protection of Communication Channels

All channels used within Naverisk are designed to be protected from external interference.

1.1 Website

The Naverisk website is published with a valid SSL certificate, i.e. using HTTPS. This makes it difficult to intercept the data flow between the User Interface and the Web Server which provides Naverisk services.

1.2 Remote Control

Naverisk Remote Control services are provided by a standard VNC Server deployed on monitored machines. Security is obtained by setting this VNC Server only to listen on the internal loopback network interface (e.g. 127.0.0.1). This prevents connections being made to this VNC Server from any other computer, even one on the same LAN.

Traffic between the Proxy Server (Site Controller) and the VNC Server on the monitored Device is further encrypted with 56bit DES encryption. The command channel is the regular Agent – NC – SC channel. The connection via Remote Control and the Naverisk Site Controller (acting as a Proxy between the Device and the controlling Naverisk user) is opened by the Remote Control package. The Agent itself only opens listen sockets for intra-machine communications (i.e. only listens on the loopback/127.0.0.1 interface), making it invulnerable to network based attacks.

The viewers used for Remote Control are Java based. The viewers are only able to open connections to the Remote Control Listen Port provided by the Naverisk Site Controller. They do not open a connection to any other server, which provides a good degree of protection, in that it is difficult to mislead the viewer into connecting to the wrong system.
In general, Remote Control is secure, as to initiate a connection (i.e. enable access to the monitored Device's VNC server) a user must be logged into the Naverisk website. The Naverisk Remote Control viewer cannot

connect unless the connection is expected by the Site Controller, and the VNC server on the monitored Device is not externally accessible as it will only connect to the Site Controller when triggered by an impending Remote Control session.

Additional Remote Control systems are optionally provided from within Naverisk. These Remote Control options do not pass over Naverisk Network connections and are secured entirely by the vendor who provides the Remote Control system.

2.0 Naverisk Network Protocol (NNP) Connections

Naverisk Network Protocol (NNP) connections are used to allow communication between remote components of Naverisk, regardless of platform, e.g. Agent to Network Controller, Network Controller to Site Controller.

All NNP connections provide a high level of security.

1. Connections are only ever made upstream, i.e. the Agent will only connect to its Network Controller, and the Network Controller will only connect to its Site Controller. Agents use no external Listen Ports; they can never accept incoming connections, so they are invulnerable to external attacks. Network Controllers only listen for Agents; the Site Controller can never initiate a connection to a Network Controller.
2. AES 256-bit encryption is used on all NNP connections.

3.0 Data Protection

Naverisk provides methods for safe transfer of data between system entities. An example of this data is the historical performance data recorded by Advanced Agents. This recorded data should be recorded and available to complete the data set, even if failures which prevent the data being transmitted occur.

Safe data transfer services are provided by the FileSocket system of NNP, inheriting the security benefits of NNP. This provides a managed channel for the Agent to send data to its Site Controller. Even if networking is disrupted, or parts of the system are non-functional, data can still be delivered. This is achieved by a Data Reception Verification Process; it is not assumed that any data has been sent successfully until the receiving entity explicitly notifies the sending entity that the data has arrived safely.

All High priority messages from the Agents expect an acknowledgement from the Site Controller. Should that acknowledgement not happen the message will be resent until it is acknowledged. In this way Naverisk can be sure that priority messages will get passed through to the Site Controllers.

4.0 Application Security

4.1 User Authentication

Naverisk offers three user authentication methods.

1. Password Authentication - Users can specify the password that is to be used for accessing Naverisk.
2. AuthAnvil 2 Factor Authentication – Adds an extra of authentication to access Naverisk services via soft token.
3. Google 2 Factor Authentication – Gives Naverisk the ability to generate a Google 2FA key that can be sent to any Smart Phone or Tablet.

Note: for more information on 2 Factor Authentication please refer to the Configuration documents in Naverisk Help.

5.0 EU General Data Protection Regulation (GDPR)

The European General Data Protection Regulation (GDPR) is enforceable from May 25th 2018. This legislation changes the landscape of regulated data protection law and the way that companies collect and use personal data.

As per the GDPR website **www.eugdpr.org** "The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy."

The GDPR not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location

Is Naverisk Complaint? Yes! All Naverisk services comply with this Regulation and we have taken steps to protect the personal data of our partners, including but not limited to:

- Naverisk SaaS offerings are provided using well established and industry-leading cloud services platforms. These providers have stated their commitment to compliance with GDPR.

- Naverisk SaaS offerings are localized in the region where our partners are located unless the partner specifically designates another locality.
- Naverisk maintains and administers a security policy with safeguards designed to protect the security, integrity and confidentiality of customer data.

Naverisk's hosted solutions may be used for the collection, processing, and storage of personal data by Partners. In such cases, Naverisk acts as data 'processor'. Naverisk Partners generally act as the data 'controller' determining what data to collect, how long it is stored and how it is used. Since each business is unique, Naverisk recommends that each Partner perform their own GDPR gap assessment.

This information does not provide, does not constitute, and should not be construed as, legal advice on GDPR. Naverisk partners should seek advice from their legal counsel to determine their legal obligations.

For further questions on Naverisk privacy and security, please see our website https://naverisk.com/privacy/ or contact security@naverisk.com