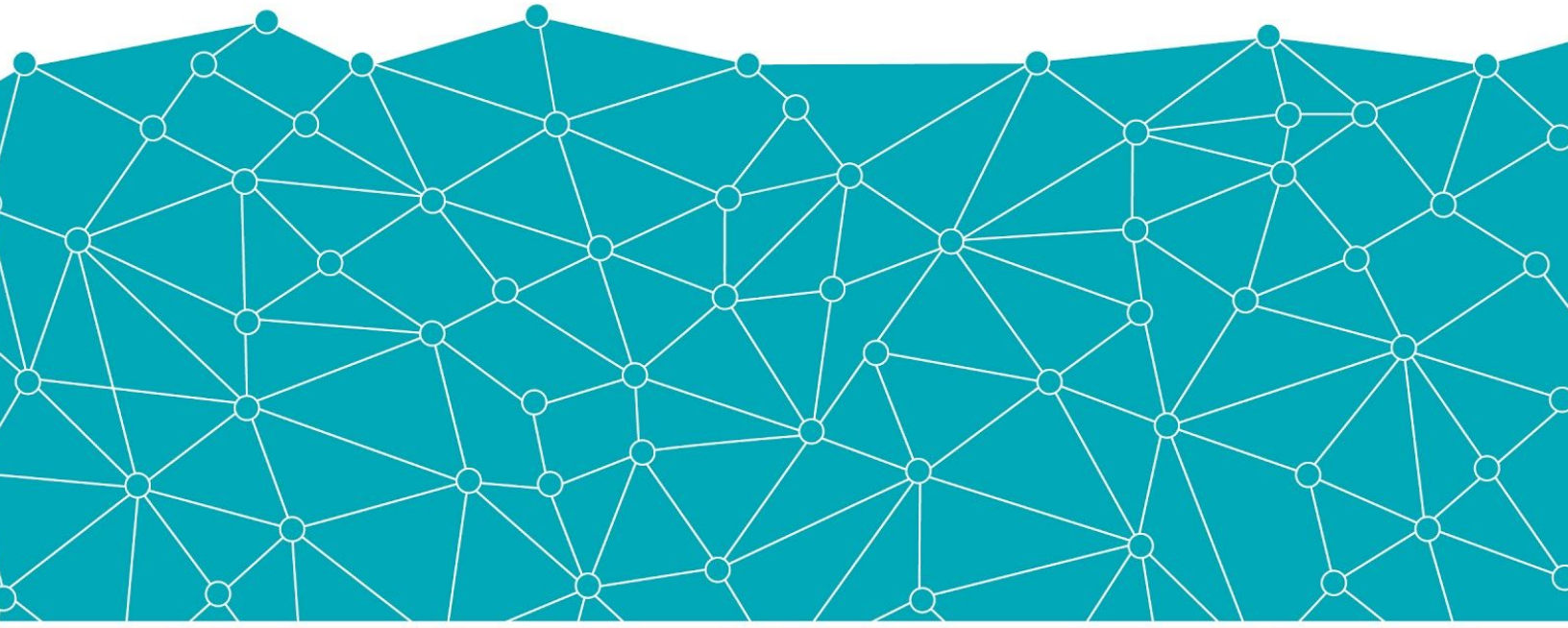
NeuraLegion

Futurae Ex Machina

NexPloit FAQ



Q.
WHERE IS NEXPLOIT DEPLOYED?

A.
NexPloit is comprised of two main parts:

The first part is a cloud service that holds our Machine Learning algorithm and does the heavy lifting of communicating with the target, learning it's architecture, creating new attacks and understanding the implications of these attacks.

The second and optional part, is a local agent which sits on the tested environment and gathers machine-specific data. The gathered data includes no sensitive information, only system resources, which gives NexPloit the ability to detect anomalous behaviour of the tested application.

With this revolutionary 2 part solution NexPloit is able to track down any local application's vulnerabilities more accurately and swiftly with no false positives.

Q.
DO I HAVE TO INSTALL A LOCAL AGENT?

A.
No, NexPloit can scan for vulnerabilities using a complete "Black-Box" mode without relying on an Agent. However, in order to perform a more in-depth analysis of the target, a local agent is recommended as it significantly enhances the discovery of issues.

Q.
HOW DOES NEXPLOIT ENSURE DATA SECURITY AND PRIVACY?

A.
We at NeuraLegion place the security and privacy of our customers as our top priority, after all, we are a cyber-security company. Our cloud ML engine does not collect or store any customer specific information after the scan. Any user data that are necessary during the scan are stored in-memory only, and are deleted as soon as the scan ends. In addition we employ the industry's best practices in handling data, including encryption, access regulations, and data separation in all of NexPloit's parts.

Q.
WHAT ON PREMISES DATA IS GATHERED?

A.
When using our local Agent, the only data we collect are machine-specific resources such as cpu and memory consumption. This is only general data about the machine on which our agent is running. No information regarding the network or the file system is gathered.

Q.
WHAT KIND OF ENCRYPTION IS APPLIED TO DATA IN FLIGHT?

Q.
We use the latest versions of the most secure ciphers available, currently TLS 1.3.

Q.
WHAT KIND OF SECURITY PRACTICES ARE IN PLACE?

A.
NexPloit follows the industry's best practices In security and privacy assurance.

Both the infrastructure and application are secured and hardened. Software development is subject to regular security code reviews, and security tests are included during every release cycle.

Q.
CAN NEXPLOIT'S BACKEND BE DEPLOYED ON PREMISE?

A.
No, currently our solution is only available from the cloud. We believe this is for the best for several reasons: First, our ML engine constantly learns from each scan, so all our customers enjoy the shared improvement of our ML model. Second, any improvements and updates to the ML engine are deployed on the cloud and are instantly incorporated in our customers versions of the product with no requirements for updates. Third, scaling NexPloit engines is easy and flexible for any needs of our customers.