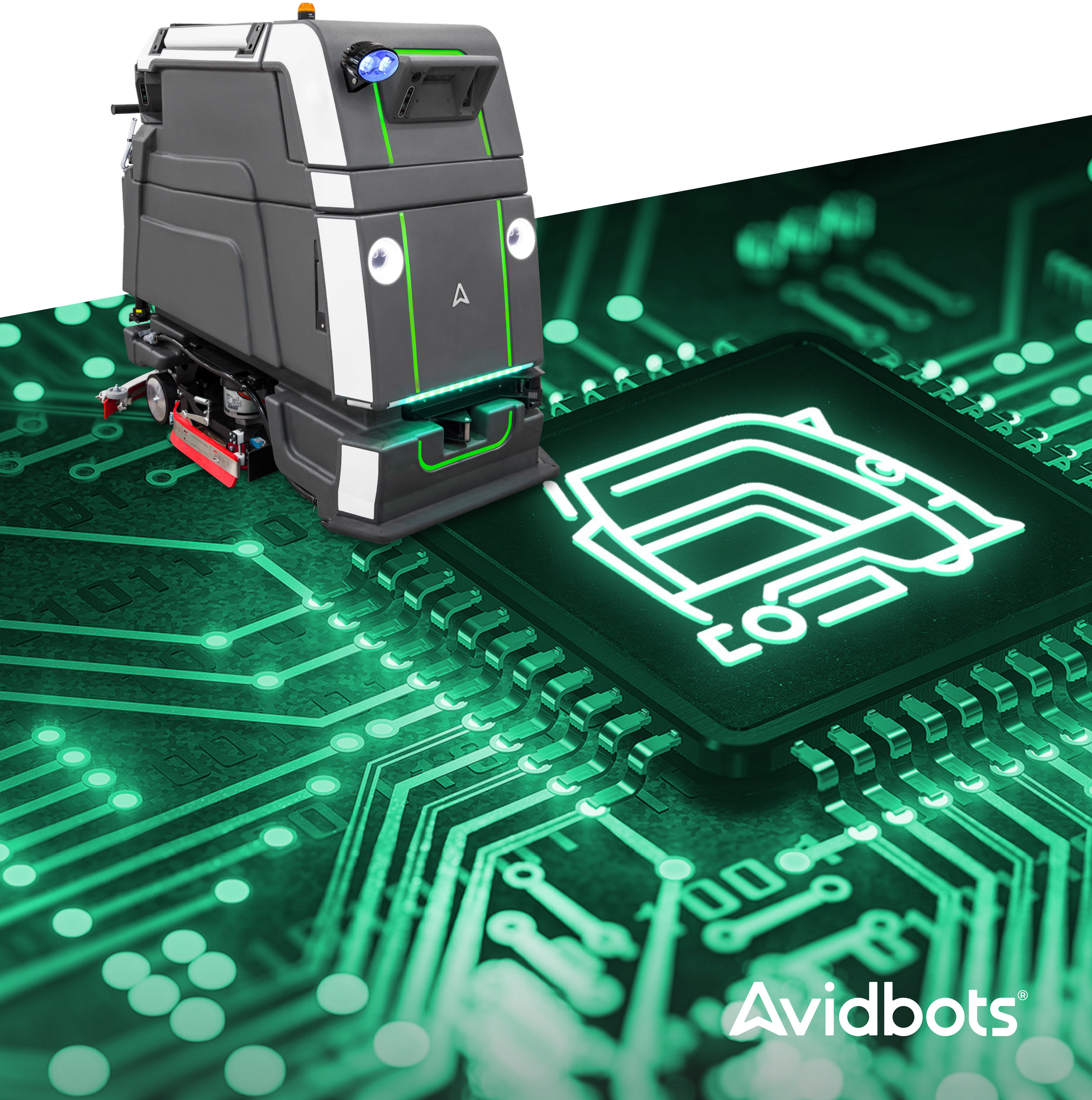
Neo by Avidbots® | Security information



Avidbots®

Avidbots is committed to the highest levels of security

➤ Neo is secure

Avidbots is committed to a secure operation, employing the most advanced security methods available. We work with third-party experts to ensure that our tools, systems, settings and configurations are working in concert sufficiently to prevent cyber attacks and meet compliance and regulatory requirements.

Our engineers and security specialists work closely with our customer’s IT teams to ensure our robots always operate within corporate network security policies. Platform flexibility and our collaborative approach to deployment enables Neo(s) to clean high-security facilities such as airports, hospitals and nuclear power stations. Avidbots has established IT policies and procedures including ISO 27001 certification and is currently working towards SOC2.

Neo leverages data to deliver advanced performance reporting, cleaning map optimizations and **24/7/365 Real-Time Monitoring** and **Remote Assistance**. Together, these important features keep Neo performing at its best while cleaning your facility.

Data security

How data is captured and used

An industry-leading suite of lidar and 3D cameras/sensors provides Avidbots Autonomy with a constant stream of information and data that is analyzed, enabling the robot to make informed decisions on a continuous basis. Camera imagery is used solely to monitor and tune the performance of cleaning plans only. The angle of the cameras, their low resolution and their programming do not allow us to identify individuals or materials. Data is used for cleaning plan creation/updates, obstacle avoidance, product development, troubleshooting and remote assistance. In addition to providing the robot with this data, the sensors share the data with our Customer Success Team who leverage it to work directly with our customers and optimize their cleaning operation.

No sensitive personal data is captured or used by Avidbots. Names, email addresses and contact details collected are only used to communicate with customers regarding the performance of their robot. Ground staff and cleaning operators can be made anonymous and contact details limited to corporate contact details only.

Keeping data private

Unidentified data captured in video streams is not used for personal identification. All video is of low quality and no processing of images for personal identification takes place. It is not possible to identify individuals based on the data captured and there is no plan to add such functionality. Video files are not shared outside of Avidbots.

Data transmission

Neo is equipped with an industry-standard network gateway supporting Wi-Fi, 3G and 4G LTE network support connections. Wi-Fi network connections are recommended for optimal reliability, with cellular data connections optionally supported for network failover in Wi-Fi cold spots. An Ethernet port, reserved for diagnostic support, is also included. Avidbots is committed to supporting the highest levels of network security. All communications originate from the robot, securing the customer's network. In addition, Neo robots are protected by a firewall, with a minimum number of ports open for authorized connections. This ensures that no data is unintentionally exposed and no unauthorized connections can be made.

The network gateways equipped on Neo robots support WPA2-enterprise encryption. All data transmitted between Neo and Avidbots secure servers is encrypted using modern TLS 1.2, or SSH encryption protocols using Advanced Encryption Standard (AES). Data at rest is encrypted using AES-256 (Advanced Encryption Standard), the same standard used by the U.S. Government to protect classified information. In transit, secure TLS encryption protects against data eavesdropping.

Network communication

Avidbots Neo robots are firewalled and only allow white-listed ports to open connections. This ensures that no data is unintentionally exposed, and no unauthorized connections can be made. The ports it allows connection on are: 22 (via SSH), 323 and 123 (via NTP) and 1194 (via OpenVPN).

All network-communicated data between the robot's computers and Amazon Web Services (AWS) and between the Avidbots Command Center and the robots/AWS is encrypted using modern TLS, SSH or OpenVPN encryption protocols. All of these encryption protocols are standard security protocols used in everyday environments (e.g. HTTPS is based on TLS).

Data storage location

Video and performance data is stored both on the robot's internal hard drives and on our Avidbots Command Center servers, located at a CJIS compliant storage provider in Virginia, USA. However, we are happy to discuss alternative options, if desired, to conform with corporate IT policies or regional regulatory requirements.

How long data is stored

All video data recorded by Neo is stored remotely on Avidbots Command Center for 90 days before automatic deletion. Only text data is recorded locally on the robot and kept for up to 32 hours on a rolling basis. No video or images are stored locally on the robot. We keep the recorded data for a short time to allow historic review of specific cleaning operations, in case of a performance or safety issue. Performance reports are stored indefinitely on our servers to provide cumulative, historic productivity analysis for customers.

Secure hardware and software

Software installation and updates

The robots are configured to run only software specifically approved and installed by Avidbots and are otherwise locked down entirely. Software updates are delivered using TLS encrypted channels from servers that are managed by Avidbots. There is no facility to add, remove or modify any of the programs or data on the robot except by Avidbots.

Physical

It is possible (as with any unattended object) that a malicious person with unrestricted physical access to the device could modify the robot to affect its functionality (e.g. tampering with sensors, cutting wires, etc.). This vulnerability is present on any device and is not unique to Neo.

Security recommendations for customers

We recommend that you keep the key for Neo in a secure location that only your trusted staff can get to or that it remains with trusted individuals at all times. It is also recommended that staff who operate Neo have passcodes that are difficult to guess. As noted below, safeguards are in place to ensure passwords are strong.

Our team would be pleased to discuss the technical details of Neo's advanced security protection and our experience partnering with corporate IT teams across a wide variety of industries.

Avidbots Command Center

Avidbots is vigilant about protecting your data, so we employ the most advanced security methods available, including: encryption of data at rest and data in transit, minimum password complexity requirements and mobile phone two-factor authentication.

Encryption

At rest

Data at rest is encrypted using AES-256 in Amazon RDS (Relational Database Services).

In transit

Data in transit is encrypted using TLS.

Authentication

Passwords

Passwords are never stored in plain text. Avidbots uses the bcrypt adaptive password hashing function. Passwords are salted and hashed before being stored. This ensures passwords are resistant to brute-force search attacks and maximizes data access security. As an Avidbots Command Center user, you set your own password. This password must contain at least eight characters, cannot be part of your username, and cannot be part of a database of over 30,000 common and easily guessable passwords.

Mobile phone two-factor authentication

For users who want additional layers of security, Avidbots Command Center supports mobile two-factor authentication using the Google Authenticator™ app that is available on Android™ and iOS™. By using this authentication method, even if someone were to maliciously guess or steal your password, they would not have access to your Avidbots account unless they also had access to the code generated by the Google Authenticator™ app on your mobile device.

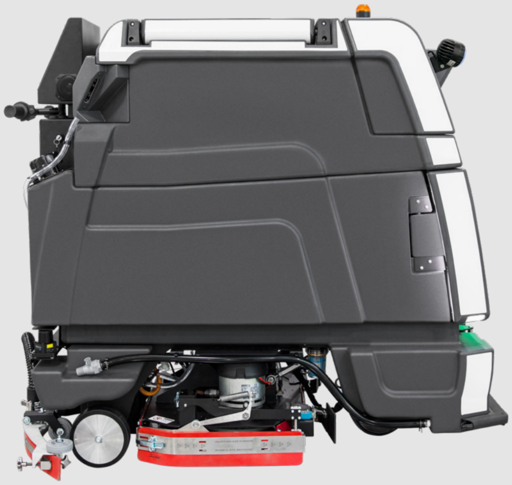
Data center security

Amazon Web Services

The Avidbots Command Center is hosted through Amazon Web Services (AWS). Read about their ISO 27001 certification here: https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf. The following whitepaper contains more details about their security: https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf.

Why Avidbots?

Buying an Avidbots Neo isn't just buying a floor scrubber. It's investing in a technological future that can redefine your cleaning function, making it more productive, more cost effective and easier to run. More importantly, our robotics and AI technology open up new opportunities to make your business even more successful. We realize this isn't just about buying a product, or a technology, or even a business proposition. You want to buy into a trusted partner who can take you into the future of automated operations using cutting edge robotics. At Avidbots, we work side-by-side with our customers to earn that trust and realize all the benefits that robotics can bring them.



About us

Avidbots is a robotics company with a vision to make robots ubiquitous to unlock humanity's potential with a hyperfocus on autonomous cleaning. Our groundbreaking product, the Neo fully autonomous floor scrubbing robot, is deployed around the world and trusted by leading facilities and building service companies. Headquartered in Kitchener, ON, Canada, Avidbots is offering comprehensive service and support to customers on 5 continents.

Contact us

Learn more about Neo.

✉ sales@avidbots.com

☎ +1.855.928.4326

avidbots.com

Avidbots Corp
45 Washburn Drive
Kitchener, ON N2R 1S1
Canada

Avidbots Chicago
5400 Newport Drive STE 7
Rolling Meadows, IL 60008
United States of America

Avidbots®