TechIDManager
by Ruffian Software

TechIDManager Agents

Installing yet another agent on my system?!

It is a valid concern, MSPs should know what is going on with their machines, and it is always a valid question to ask what an agent does. This is an easily addressed concern when it comes to TechIDManager and here is why.

Unique accounts are required by insurance and cybersecurity frameworks. TechIDManager facilitates meeting these requirements while ensuring a path with the least security risk.

Having random code executing on any computer can be a problem, especially ones that have high levels of access and permission. RMMs do it, remote connection tools do it, TechIDManager does not do it. The RMM agent is a higher vulnerability, higher target, higher risk; so by installing a TechIDManager agent, there is no more risk than a client is already taking.

TechIDManager made very specific security decisions to not do any remote code execution to keep the use of the TechIDManager agent secure. This leads to also not doing automatic updates. We only do what we do. We don't allow any incoming commands, TechIDManager only reaches out to our servers to guarantee that the actions they are performing are coming from the right place. This is important security that is architected into the product, and allows you to vet all agents before deploying. The reason behind this is similar to patch management; it can be verified right before pushing it out. When agent executables are vetted, it shows that TechIDManager only does as intended, and security risks are minimized.

Self hosting is also an option that creates an environment where only the MSP has access to all data hosted within TechIDManager. This includes the clients' data as it relates to privileged accounts and credential storage. This includes all data in transit and all data at rest.

TechIDManager
by Ruffian Software

Encryption of Credentials System Overview

All information stored in the cloud is stored on an encrypted disk in accordance with best vendor security practices.

All credential information that is stored is further encrypted with the specific RSA key of the tech who owns each account. The ManagementConsole does not store, or ever have access to, the Private Key of the asymmetric key pairs that encrypt the credentials. In this way, no one, not TechIDManager devs, not production staff, not support, not hackers, nor anyone else with access to the data stored in the ManagementConsole can decrypt any credentials. The private keys needed to decrypt a set of credentials only exist on the tech's computer who owns the account. This is an important aspect of the Zero-Visibility architecture that underpins all of TechIDManager.