domotz

White Paper

Why the Domotz Cloud is a Safe Place for Services

IT departments are challenged with how they should manage the security of their networks.

As an integrator or MSP (Managed Service Provider), your clients will question the security aspects of what you are installing. This paper should give you some guidance on how to address the question of Cloud vs On-Premise solutions and to discuss the security aspects of those solutions.

There is still debate about the security of Cloud solutions vs On-Premise solutions especially when it comes to critical applications like Remote Monitoring and Management solutions (RMM). As for any change on the infrastructure and management of a network, the security managers of your clients will definitely weight the pros and cons of implementing an RMM solution on the cloud.

This white paper presents practical considerations for choosing an RMM hosted on the cloud, addressing most of security topics which affect cloud solutions.

What are the options?

On-Premise Solutions have been the standard way to manage networked systems for many years. An on-premise solution generally consists of a server running management software, often accessed by multiple users. These servers are typically “keyed” to allow a limited number of users access to the management tool. In many cases where users need remote access to the server, a Virtual Private Network (VPN) is created to allow secure access. Use of VPN’s is a common practice; however, these have to be maintained regularly to ensure security and integrity.

Any on premise software solution should work as expected the day it is installed. The problem is that as the software and server that this solution is running on ages, vulnerabilities start to be exposed. Older versions of the operating system, lack of maintenance updates to applications and potential changes to the network all create potential holes in the system. On premise solutions require a dedicated manager to ensure that these vulnerabilities are dealt with appropriately. It’s important to recognize that the security of the system is only as good as the efforts put into managing it.

Cloud Solutions are becoming a standard for many software companies as they allow faster, better scalability and centralized software updates. The best part of a cloud-based solution is that they can be accessed securely from anywhere. Users of the cloud solution can typically be added and removed easily, giving greater flexibility to the solution administrator. Perhaps even more importantly, cloud solutions are designed to

work on many different platforms and are usually browser-based providing businesses with more flexibility when selecting hardware and operating systems.

Moreover, many organizations already have several enterprise solutions in the cloud. Services such as email and voicemail, CRM tools, human resources and accountability systems, or even data storage are already implemented in the cloud. A very similar trend has been reported on the adoption of Network Remote Monitoring and Management solution on the cloud. This is due to the inherent benefits of a cloud-based RMM solution.

A cloud-based solution requires connectivity between the client and the cloud. To ensure connectivity, standard protocols and robust security must be implemented. These protocols and security measures must remain up-to-date to keep the integrity of the cloud in place. It is up to the manufacturer and the cloud hosting service to ensure that proper maintenance is always in place. A cloud service user relies on the vendor or the manufacturer to keep the cloud-based solution updated with the latest software and security measures. This is a major benefit to using a cloud service.

There are additional benefits to cloud solutions that go beyond maintenance. Cloud hosted services have built in redundancy which ensures that data stored and the configuration of these services are backed up on a continuous basis. This should give peace of mind to customers that maintenance is current and downtime is minimized.

A cloud solution will leverage standard browser technology or a web application that allows a user to connect to the service from anywhere. Use of standard web browsers make it easier for the manufacturer to develop and maintain infrastructure changes to the cloud.

Hybrid Models are a combination of both cloud and on-premise solutions with the intent of optimizing workflows. These hybrid models are often used where real-time data gathering and aggregation are a lower priority allowing information to be stored locally and then synchronized with the cloud during off-peak times. Hybrid solution users must manage both the on-premise portion of their network as well as the cloud-based portion, often increasing maintenance overhead and total cost of ownership.

How Domotz Pro keeps your business and your client's business secure

Domotz Pro is a cloud-based service that provides a business with remote monitoring and management tools for their on-premise location. There are three components to the Domotz Pro services that all have unique security features: 1) the Domotz Pro agent which resides on the Local Area Network, 2) the Domotz Pro Cloud, which is hosted by Amazon Web Services, and 3) the Domotz Pro application, which can be web-based or installed on a mobile or desktop client. The communications between these components always passes through the Domotz Pro cloud. Any communications that occur between these components are encrypted and unique to the component. It is an important part of the Domotz Pro design, that each component has a unique, secure channel.

For example, as a cloud-based service, Domotz Pro does not require inbound ports to be opened. Opening a static port on a firewall to inbound traffic poses a security risk and creates an attack surface opportunity. Instead, anytime Domotz Pro needs

to communicate with the cloud, a request comes from the locally installed Domotz Pro agent and is sent outbound to the Domotz Pro cloud. Any transaction that occurs between the Domotz Pro agent and the Domotz Pro cloud is fully encrypted and secure. Data is always encrypted with the latest technology available.

Domotz Pro offers additional security benefits at the individual user level. Often the weakest part of any online transaction is due to simple passwords. Domotz Pro leverages strength measurements to help ensure that individual account passwords are secure. Two-factor authentication can also be enabled and is recommended for all Domotz Pro accounts. By leveraging strong passwords and two-factor authentication, your client's systems are further protected.

If you are the Domotz Pro service account admin, or Team Master, you have the ability to limit your employees' access to your clients. If you have special clients, where you want to limit exposure to a small number of employees, you can do this by taking advantage of the team hierarchy within the Domotz Pro application.

Given that Domotz Pro has been built with solid principles around the security of our cloud service, we are proud to share those principles, and how they are applied on our infrastructure. More information on Domotz Security Standards can be found at:

https://www.domotz.com/pro-security-standards.pdf

Moreover, Domotz Pro, being the primary service provider for large enterprises, has been put under multiple due diligence with regard to security and privacy policies. These enterprises have put Domotz Pro under intense scrutiny and security assessments, which has brought (and will continue to bring) additional improvements from the security point of view. This due diligence performs and periodically repeats the exercise of a Penetration Test against all the components of our infrastructure (Agent, Cloud and App). Every Domotz Pro user benefits from this relationship with these large enterprises: any security improvement coming from this relationships will be made available to all the users.

When it comes to the Domotz Pro agent and its security, a secure Linux operating system (OS) called Ubuntu Core has been implemented. This operating system has be designed with IOT (Internet of Things) devices in mind. This Linux OS has the ability to update an installed application, the OS and even the kernel in real-time and in a completely transactional way. This means that the Domotz Pro software agent can be updated without the need for user intervention or a hardware reboot. If at any time a vulnerability is exposed in the operating system, it can be patched promptly. This ensures that your client's networks are maintained and up-to-date with all the latest security code and features.

Additional details about the security of the Ubuntu Core OS can be found in:

https://developer.ubuntu.com/static/resources/ubuntu-core-security-whitepaper.pdf

A cloud-based remote monitoring and management tool like Domotz Pro is a viable solution for your customer

To recap, if your clients are concerned about security of their network, they should consider the adoption of a cloud-based RMM solution for the following benefits:

- **Ensure an always updated system**
  Domotz takes advantage of the latest patches in security. A cloud service is typically updated with the latest cybersecurity patches, which helps mitigate the risk against most common attacks. An on-premise solution forces your company to keep constant upgrades on all the remote installations.

- **Keep access to the system under control**
  Ensure that only the authorized and updated list of the members of your team has access to the tool. An on-premise solution forces your company to keep constant maintenance of the Access Control List (ACL) systems on all remote installations.

- **Provide access from anywhere without compromising security**
  Ensure that the members of your team have remote monitoring and access to client's networks without creating unnecessary cybersecurity holes on those. An on-premise solution forces your members to create Virtual Private Networks (VPNs), Port Forwards or NAT on the networks to have remote access to the on-premise solutions.

- **Reduce the cost of ownership**
  Domotz Pro allows companies to save money, due to the lower total cost of ownership. A cloud-based RMM solution requires a very minimal upfront investment, because all the effort required to secure the service is on the cloud solution provider. An on-premise solution forces your clients to acquire expensive hardware and ensure that all the servers adopted in the solution are hardened from a cybersecurity point of view.

- **Innovation and scalability**
  Domotz provides you with the latest and most evolved technologies. With the adoption of a cloud-based RMM solution, your clients will leverage leading-edge innovation that provide mobile access, easier maintenance, easier deployment and scalability, but more important higher standard of security.