Domotz Security Standards

This white paper outlines how Domotz protects *Security*, *Availability* and *Privacy* for you and your clients.

March 2021

domotz

Contents

Abstract

Security and reliability of the offered service are our top priority in everything we do at Domotz.

If you are reading this document you are probably a Network Administrator, a Technology Service Provider or a Managed Service Provider and the security of the networks you manage is, likely, your first concerns. Our philosophy is the same, and for this reason, we adopt the best processes, technologies and controls to guarantee the best security, availability and privacy in the tools we make for you.

In this white paper we will give you an overview on the three matters that, like you, we most care of:

- **Security**. This section is a walk-through our security framework and compliance programs, and provides you an overview of the main actions we take to keep your data safe and to continuously improve security
- **Availability**. Domotz is devoted to making sure the service is always up & running all the time, even in case of unexpected events or major disaster. In this section we describe the processes and best practice we follow
- **Privacy**. Domotz has always been proactive in maintaining the privacy and data of its users, even before major regulations, such as GDPR came to force. In this section we describe how all data processed by Domotz are treated.

Finally, we have decided to add, at the end of this document an **Appendix: How Domotz can improve the security of your networks**. We want to remark that Domotz is a remote network monitoring and management system and not a security product. Nevertheless, we have developed a number of features that can help users increasing the defenses of their networks. In this section, a quick overview of such features.

Security

Domotz Security Principles and Standards

Defense in Depth (DiD) and Defense in Breadth

We believe that no organization can be fully protected by single layers of security. To protect systems and data in the Domotz cloud, we adopt the "Defense in Depth" principle, which focuses on implementing several layers of security to guard against cyber threats or, in the unfortunate case of a cyber compromise, to quickly detect and mitigate its effects.

A layered approach to security is applied to all levels of our IT systems and organization. A good way of representing this is show in the following diagram.

> Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack. Defense in Depth is commonly referred to as the "castle approach" because it mirrors the layered defenses of a medieval castle. Before you can penetrate a castle, you are faced with the moat, ramparts, drawbridge, towers, battlements and so on.

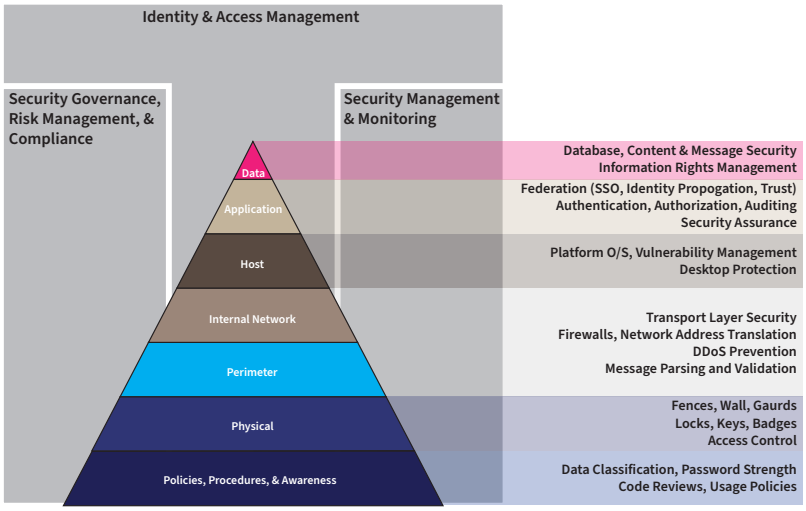

Figure 1 - Layered Security to Defense in Depth

The horizontal layers represent the different levels of protections of the systems. The vertical bands represent tools and processes to be applied at each level of the networks.

In the following subsections we describe all the elements of our secure architecture.

Security Standards and Practices

SOC 2 (Systems and Organizations Controls 2)

SOC 2 is a set of compliance requirements and audit procedures for technology-based service organizations that store customer data in the cloud. Developed by the American Institute of CPAs (AICPA), SOC 2 defines criteria for managing customer data based on five "trust service principles"—security, availability, processing integrity, confidentiality and privacy. Regular audits ensure the effectiveness of controls in place.

Domotz continuously enforces, improves and audits all its controls relevant to security to ensure compliancy with SOC 2. Controls include physical and logical access, control environment and activities, risk assessment and mitigations, system operations, change management, communications and information. Independent auditing firms perform regular audits and issue periodic reports. Our customers can reach privacy@domotz.com to obtain the latest available SOC 2 report.

CIS Controls®

Domotz has adopted CIS Controls® as effective and formal framework for implementing all Security best practices.

CIS Controls® is a global standard and a set of recognized best practices for securing IT systems and data against the most pervasive attacks and threats. These proven guidelines are continuously refined and verified by a volunteer, global community of leading security experts and IT professionals.

CIS® (Center for Internet Security, Inc.) is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. CIS® is home to both the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center™ (EI-ISAC®), which supports the cybersecurity needs of U.S. State, Local and Territorial elections offices.

OWASP

The Open Web Application Security Project (OWASP) is a non-profit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

Domotz is part of the OWASP community and uses a number of OWASP tools and resources, as well as OWASP's education and training materials.

Data Security

Security Architecture

Domotz has adopted administrative, physical, and technical industry-standards (including encryption, firewalls and SSL) to safeguard the security of our services and to protect the confidentiality of personally identifiable information. Domotz's solution relies on very strict perimeter security policies. Only the required standard communication ports are open to the public, while we use a different communication channel for the management services.

Encryption

Domotz implements strict requirements for cryptographic encryption and for the management of cryptographic keys, in order to protect the confidentiality, integrity, authenticity and non-repudiation of information.

Our Encryption Policy applies to:

- all systems, equipment, facilities and information within the scope of the organization's information security program.
- all data in transit across Domotz's cloud boundaries.
- personal identification and other sensitive data at rest.

Domotz uses strong cryptography and security protocols based on National Institute of Standards and Technology ("NIST") standards for encryption. Specifically:

Type of data/system	Cryptographic Tool	Encryption Algorithm	Key Size
Data at rest	Python/pycryptodome	AES-256 CBC	256-bit key
Data in transit	SSL v3 or better	AES or CHACHA20	128-bit or 256-bit
User Credentials	OpenLDAP/others	SHA256+salt	256-bit
VPN	OpenConnect VPN Server over TLS1.2	AES-256 GCM	256-bit key

Cryptographic keys are managed, secured, restricted and rotated according to the NIST SP 800-57 Part 1 Recommendation for the management of encryption keys.

Client Communication with Domotz Cloud

All the communications between the Domotz App (either the Mobile App, the Desktop App or Portal-WebApp) are established over a secure HTTPS channel (Hypertext Transfer Protocol over Secure Socket Layer). As you can see from your Web Browser when connecting to the Domotz Portal or WebApp, there is a Green Lock near the URL, which means that the connection is certified to be secure.

The entire communication between the Domotz App and the Cloud is over a secure channel (encrypted). Your account password is only transmitted over this secure channel to monitor and act on your network (or your client's networks).

You and your team are the only users that can interact with your network, unless you "Invite a guest" or a Support Team to manage that network. You are always entitled to revoke this invitation in any moment you want, so that the invited guest cannot act any more on your monitored network. Only the owner (or the delegated Team Member) of a specific agent (network) can invite or revoke guests on that network.

Agent Communication with Domotz Cloud

All the commands to the Domotz Agent are sent over a secure channel (AMQPS - Advanced Message Queuing Protocol over Secure Socket Layer). Each agent/network has its own private channel, and this channel can only be accessed by that specific agent (the credentials to access to this channel are created at the moment of the Agent configuration, and it is only stored on premise within your Domotz device - e.g., Raspberry Pi, NAS, your own Server or the Domotz Box).

Similar to the Client Communication channel, we do not store the Agent password in the clear on our cloud. Information from the Agent to the Cloud are also sent over HTTPS channel, with the same Agent credentials.

It is important to note here that the Domotz solution does not increase the possible attack surface of your network, since all the communications are established from within the network out to the cloud. Therefore, no additional ports are opened by Domotz on the WAN side of the network.

Remote Connect functionality

One of the key features of Domotz is the direct remote connection (HTTP or HTTPS, SSH or Telnet, RDP or VNC). When a connection is created, Domotz establishes a secure channel (Encrypted Overlay Network) between the remote network and our cloud, as well as an HTTPS channel between the App (either Mobile App or WebApp). The entire communication from the App to the Agent is encrypted, such that nobody can “sniff” the content of it.

Please note that if you look at the URL when opening a Remote Connection through the WebApp, and you copy and paste that URL on a different PC/Client, you will not be able to reach the end-device. This has been designed in order to guarantee additional security in case you are accessing Domotz Pro from a non-secure location - e.g., in a public place, over a non-secure WiFi.

Note that with Domotz, you do not need to open any external port on the router to reach your local devices. The Domotz solution for Remote Connectivity guarantees an additional level of security, given that all the supported protocols are encrypted when the data is exposed on the public network. Therefore, even the data associated with Telnet and Http Remote Connections, which are inherently unencrypted), with the Domotz solution are secured on the public network by the Domotz encrypted channels.

Moreover, we have also provided a very secure way to connect to remote devices through a non-directly supported protocol - e.g., FTP, VNC and, in general, any proprietary TCP protocol. Even though the Open TCP Tunnel functionality does not guarantee the same level of encryption as the direct Remote Connectivity, we have protected the end–point of the secure channel allowing only connections coming from the specific calling public IP (which is the public IP of the client initializing the Remote Connection).

Similar mechanisms are in place for the VPN on Demand feature. With the additional layer of security offered by the fact that only the Domotz App requesting to start a new VPN on Demand session will receive the OpenVPN configuration file required to start the session. Additionally, that configuration file contains a one-time key to connect to the OpenVPN server started on the fly, via the Domotz Agent.

Device credentials and configuration data of network devices

In order to allow our users to remotely control their devices, Domotz may require providing, through the app, the related username/password to act on that specific device. The username/password is transmitted to our Cloud over a secure channel (HTTPS) and from our Cloud to the Agent over a secure channel (AMQPS).

All the credentials and configuration data of network devices shared with Domotz are sent to the cloud and stored there using AES-256 encryption, and furthermore protected by the user password. In this way, nobody will be able to decrypt the password, even in the remote possibility of a hacker getting access to our database.

Credit Card numbers

Domotz does not store your credit card numbers in our infrastructure. We rely on secure third-party services which are certified to PCI Service Provider Level 1. This is the most stringent level of certification available in the payments industry.

Application Security

Secure Coding

Domotz developers are trained and adopt the best security methodologies. As part of our software development cycle process, every piece of code is peer-reviewed and tested against the Top 10 OWASP vulnerabilities.

Security and Penetration Testing

Domotz adopts the best and most advanced technique to deeply test its features from a Security point of view.

We examine applications from the inside as part of our Static Application Security Testing (SAST) , a white-box testing methodology, that includes searching our code for conditions that indicate that a security vulnerability might be present.

Domotz has also implemented Dynamic Application Security Testing (DAST), that is a black-box security testing methodology, in which we perform web application penetration testing and try to hack it just like an attacker would.

Software Change Control

Domotz policies define specific requirements to ensure that changes to systems and applications are properly planned, evaluated, reviewed, approved, communicated, implemented, documented, and reviewed, thereby ensuring the greatest probability of success.

Where changes are not successful, Domotz has mechanisms for conducting post-implementation reviews such that future mistakes and errors can be prevented.

Agile/Scrum methodology, a high-level of automated testing, and a wide adoption of real-time system monitoring, are the main frameworks adopted to reduce the possibility that unwanted changes and faults are introduced into the Domotz solution and to minimize disruption of our 24/7 service.

Host and Internal Network Security

The host layer of security focuses on keeping any computer and server secure. Security at this layer can be very challenging, as these devices are often designed to multitask and interact with multiple applications and services simultaneously. The following actions are a list of practices followed by Domotz.

Host Hardening

All Domotz hosts are hardened. Hardening is the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions. To decrease the surface of vulnerability all the Domotz servers are strictly configured for running only the specific service they implement. Unused and unnecessary services, software, user accounts and file-systems are removed.

Docker security

Domotz uses a docker-based virtualization technology quite extensively. The deployment of software components uses a containerized approach. Domotz uses the same virtualization technology also to configure constraints on the usage of resources for any single piece of the application (also known as a micro-services approach).

System resources (such as CPUs, memory and access to filesystems) are some of the parameters configured for each container through docker. Domotz also monitors and analyzes behaviors of processes started within each container so that they cannot perform privilege escalation in the hosting environment.

Patch and Security Update Management

Domotz hosts are always kept up to date on all security related patches and updates. The most commonly exploited security vulnerabilities are widely known and Domotz applies readily available patches and updates to address them.

Continuous Vulnerability Management

All our servers are periodically and frequently scanned to detect system-level vulnerabilities including incorrect file permissions, registry permissions, and software configuration errors.

We have also involved third-party experts to perform vulnerability testing (external and internal) at least once a year.

Principle of Least Privilege

Principle of least privilege (POLP) is adopted at all levels of our organization. We limit access rights for users to the bare minimum permissions they need to perform their work.

Access Control and Authentication

Host-based access control grants or denies access depending on the IP address of the machine that requested access. This system is the least intrusive to users because access is granted on the basis of the machine address. User authentication allows access control on an individual user basis by utilizing username and password lists to provide the necessary authentication. Moreover, multi-factor authentication is enforced to all personnel accessing Domotz systems.

Firewalls and Port Control

Domotz makes sure that all its hosts do not have unnecessary ports open. Each Domotz host within our cloud, has host-based firewalls to control incoming and outgoing network traffic on individual hosts. The firewalls check each packet's source, destination address, port, type, etc., and then determines whether to allow them into the machine.

Anti-Virus and Anti-Malware Protection

Anti-virus protection is enforced on all employee computers and are centrally managed to ensure that updates to the required signature files for addressing new forms of malware are delivered as soon as possible. A signature file contains information that anti-virus programs use to detect malware during a scan. Signature files are designed to be regularly updated by the anti-virus application vendors and downloaded to the client computer.

Logging and Auditing

Critical host activities are logged, and the logs are audited for any unusual activity.

Perimeter Security

Minimal attack surface

Only the required standard communication ports are open to the public, while we use a different communication channel, with multiple levels of protection, for the management features. We have implemented multiple levels of firewalls, keeping completely segregated the front-end servers (with no-data) from the back-end servers (managing customer data).

Vulnerability Scan and Pen Testing

We continuously monitor vulnerabilities and do periodic penetration testing of our perimeter. Moreover, we have engaged independent third parties to perform Vulnerability assessments and penetration testing.

In addition, we have penetration testing sessions performed by some of our largest customers. Penetration testing from our customers is very welcome and just requires some previous arrangement.

Web Application Firewall (WAF)

Domotz has enabled the usage of WAF to protect our web application by filtering, monitoring, and blocking any malicious HTTPS traffic traveling to our cloud applications, and to prevent any unauthorized data from leaving the app. The WAF does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe. Just as a proxy server acts as an intermediary to protect the identity of a client, a WAF operates in similar fashion but in the reverse—called a reverse proxy—acting as an intermediary that protects the web app server from a potentially malicious client.

DoS/DDoS Protection

To protect from denial-of-service attacks, Domotz has implemented a number of measures at different levels of its architecture. Through self-diagnostic heuristics, Domotz determines when the system is under excessive stress and rejects requests until the application can serve new ones. Suspicious host IP Addresses are blacklisted.

Physical Security

Domotz is hosted on Amazon Web Services (AWS).

AWS and Domotz implements what is defined a Shared Security Responsibility Model.

Basically, AWS is responsible for securing the underlying infrastructure that supports the cloud, and Domotz is responsible for anything we put on the cloud or connect to the cloud. The schema below, provided by Amazon, clearly depicts this model.

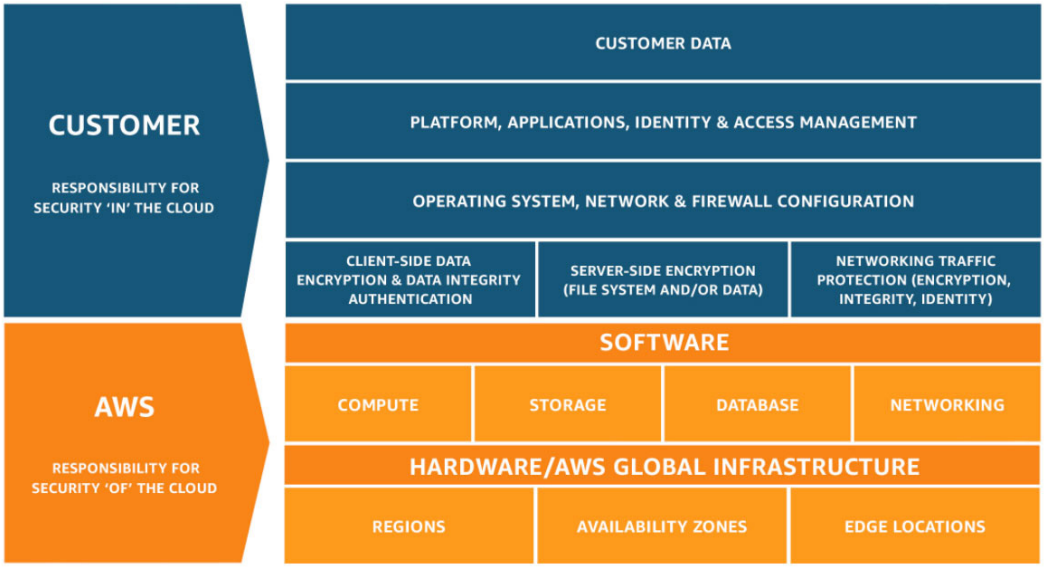

Figure 2 AWS Shared Security Model

AWS data center physical security begins at the Physical Perimeter Layer. This Layer includes number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures, as described here: https://aws.amazon.com/compliance/data-center/perimeter-layer/

Amazon's physical and operational security processes are also documented in Amazon Web Services: Overview of Security Processes, which outlines AWS data center controls such as:

- Physical and environmental security
- Fire detection and suppression
- Power
- Climate and temperature
- Storage device decommissioning
- Amazon's fault-tolerant infrastructure design
- Certifications

AWS holds numerous security certifications, which can be reviewed here: https://aws.amazon.com/compliance/.

Furthermore, CUECs (Complementary User Entity Controls) given by AWS are followed to correctly leverage AWS' security standards (for an explanation of what CUECs are: https://www.venminder.com/blog/importance-complementary-user-entity-controls-vendor-relationships)

Security Controls

Security Organization, Processes and Awareness

The Domotz policies are built under the framework of SOC 2 compliance, so that we have established processes and practices with required levels of oversight across the organization.

Every Domotz employee and any third parties providing service to Domotz must follow our Code of Business Conduct and Ethics and all Policies and Procedures, including, but not limited to:

- IT Security
- Acceptable Use
- Access Onboarding and Termination
- Remote Access
- Data Protectiown
- Encryption
- Disposal of Information Technology
- Risk Assessment
- System Change
- Security Incident Response
- Disaster Recovery

All our employees are accurately selected and follow periodic training and assessment on Data Privacy and Security awareness. Our Engineering teams follow special training programs for security best practices and security coding.

Identity and Access Management

Identity management is a foundational security measure to help ensure users have the access they need, and that systems, data, and applications are inaccessible to unauthorized users.

In particular:

- **Multi-Factor authentication** is enforced on all systems used by Domotz and imposed at every level of the Domotz organization.
- **Single Sign On (SSO)** is enforced on a number of subsystems used by Domotz employees access and login system that allows users to authenticate themselves once and then grants them access to all the software, systems, and data they need without having to log into each of those areas individually.
- **Privileged Access Management** methodologies are established to provide the access employees need to perform their roles and to ensure that Domotz personnel have only access to certain resources (applications, databases, networks, etc.) based on their role and within the correct context.

Risk Assessment and Mitigation

Domotz has a formal risk management process to identify, assess and mitigate threats that may affect the platform and the services provided to our customers. Risk assessment includes, but it is not limited to, the evaluation of infrastructure, people, procedures, software, safeguarding of data, third parties and the potential for fraud. The risk identified are formally identified, documented, assessed, and given a risk score. Risks are then mapped to mitigating factors, and action plans are deployed to mitigate those risks.
Risks are closely monitored and frequently re-assessed.

Domotz understands that particular risks exist when engaging vendors. To mitigate these risks, Domotz has decided not to use any external contractor for the developments of core features and for operating production platforms and data. Whenever third-party services are needed, we deploy a number of measures to effectively assess their compliance levels.

Whenever third-party services are needed, we deploy a number of measures to effectively assess their compliance levels. When a vendor provides Complementary User Entity Controls (CUECs), Domotz follows those policies to fully leverage the vendor's security controls. In this way, we are not only checking that the vendor follows the right compliances, but we follow their suggestions on how to use their services in the most secure way.

Change Management

Domotz reviews, prioritizes and assigns change requests to change iterations that are launched in two-week sprints. Domotz uses project management tools to define, develop and track system changes through the software development lifecycle.

We maintain separate environments for development, testing, staging and production. As changes are identified, they are prioritized and assigned to sprints. Engineers check out code from the code repository and develop changes in an isolated development environment. After development has been completed, the software is fully retested and the code is peer reviewed before the change is marked as completed. All changes are then fully tested in a separate testing environment before being deployed to the staging environment. Also, a continuous integration environment has been configured to fully automatically test every single part of the solution. Once the new software is available in Staging environment, and again peer reviewed by the rest of the team, the software is then approved to be released in production. The release is then deployed in Production by a release management team member. Deployment of changes to production is strictly controlled and need multiple levels of authorization.

System Monitoring

Monitoring is a fundamental part of the Security process. All the key activities within the security layers are logged and monitored: accesses, errors, configuration changes, WAF, resource consumptions, and more. Alerts are generated when anomalies or unexpected events occur.

Alerts are dispatched in real-time to the personnel in charge of the specific controls so that we can guarantee a prompt response to security threats. The Incident Response Team is responsible for putting the plan into action by executing an Incident Response Procedure, which is established to provide a quick, effective and orderly response to security incidents.

Process Control, Monitoring and Continuous Improvement

Monitoring is a critical aspect in evaluating whether Security control are operated as intended and whether they are modified as appropriate for changing conditions.

Domotz management has instituted mechanisms to determine that any potential problem within the organization is immediately identified and resolved. All controls are periodically assessed and internally audited to make sure they meet the trust services criteria and operate effectively to maintain and improve the security of the Domotz platform.

The whole organization is devoted, and allocates time, to continuously improve our security processes. Senior management members meet regularly to discuss internal controls, operations, risks and strategy. Action plans are developed, tracked and prioritized.

Availability

Uptime and Service Availability

Domotz monitors its infrastructure, applications and service usage, to guarantee a safe environment both in terms of security (e.g., access, usage monitoring, etc.) and reliability (e.g., service uptime, server failure, trigger of cold backup procedures, etc.).

Domotz publicly report the overall results of its availability monitoring of the Domotz platform, website and underlying infrastructure. The Status of Domotz Services can be monitored by the users anytime at this URL: https://status.domotz.com/

Domotz actively monitors the operational status of the production environment for key performance parameters, by generating alerts when certain thresholds are exceeded. This allows for prompt response actions to be taken by the team.

Our Hot/Hot configurations ensure that services are never down for planned maintenance and upgrades.

In Q4 2020, Domotz had an uptime of 99.991% including the downtime due to planned maintenance.

> A Hot/Hot type of architecture is required to implement a High Availability (HA) configuration of “high nines.” This requires that there be two (at a minimum) identically configured systems that are up and running and available to users, as well as a separate Disaster Recovery platform.

Change Controls

In order to prevent disruption to services, faults into the system and unwanted or unnecessary changes, Domotz has implemented robust Software Change Control and Infrastructure Change Control processes.

These processes ensure that changes to systems and applications are properly planned, evaluated, reviewed, approved, communicated, implemented, documented, and tested, thereby ensuring the greatest probability of success.

Adoption of Agile/Scrum methodologies, a high-level of automated testing, a wide adoption of real-time system monitoring, together with post-implementation reviews, retrospective analysis and customer feedback, are the main frameworks adopted by Domotz to reduce the possibility that unwanted changes and faults are introduced into the Domotz solution and to continuously improve availability of our 24/7 service.

Capacity Planning

Being a fast-growing company, Domotz continuously monitors processing capacity and use of system components to manage capacity demand and proactively implement additional capacity to prevent failures. Automatic mechanisms are in place to allow the self-scaling of resources in the case of an unexpected increase of requests occurs.

Backup, Recovery, Disaster Recovery

Domotz has implemented procedures to recover its cloud infrastructure and all its services within set deadlines, in the case of a disaster or other disruptive incident. The objective of this plan is to complete the recovery of IT infrastructure and IT services within a set Recovery Time Objective (RTO) and Recovering Point Objective (RPO).

This policy includes all resources and processes necessary for service and data recovery and covers all information security aspects of business continuity management.

RTO (Recovery Time Objective) - the duration of time and service level for critical business processes to be restored after a disaster or other disruptive event.

RPO (Recovery Point Objective) - it is the maximum targeted period in which data might be lost from an IT service due to a major incident.

Persistent Data Backup

Configuration data are used to build the infrastructure and to keep relationships between different parts of that infrastructure. All these types of data are retained at level code, committed on distributed repositories and all changes are tracked. Periodic backups are performed and retained on different datacenters.

Dynamic Data Backup

Dynamic data are strictly related to Domotz users.

All Data (relational and non-relational/historical) are backed up in a continuous way to standby instances in a different AWS Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable.

In case of an infrastructure failure, Amazon performs an automatic failover to the standby so that database operations can be resumed as soon as the failover is complete and without the need for manual administrative intervention. In case of an infrastructure failure, the maximum targeted period for Recovery, or RPO, is less than 30 min.

In addition to the real-time backup on standby instances, Domotz also performs periodic backups that are exported outside the datacenter over a secure channel to a different datacenter. All the transfer of backups is ensured on a secure and encrypted channel.

Incident Recovery

All the nodes which do not rely on any dynamic data, are balanced and offer a high-availability solution, which in case of failure for the primary node will automatically recover the status.

Nodes relying on dynamic data, are replicated with cold backup instances. In case of failure of the primary node, backup instances are provisioned with the latest snapshot of dynamic data and started. The target for recovery of these critical business processes, or RTO, is less than 30 min.

Disaster Recovery

For Disaster Recovery (DR) purposes, all the Dynamic Data are also exported outside the primary datacenters (over an encrypted channel) and stored on different AWS regions.

In case of a catastrophic disaster event hitting an AWS datacenter, Domotz is able to re-build the entire infrastructure in a different datacenter (AWS region) and provision the nodes requiring Dynamic data. In this worst-case disaster scenario, the RTO is less than one day.

Privacy

GDPR Compliance

What is GDPR?

The General Data Protection Regulation ("GDPR") is a European Union privacy regulation that went into effect within the European Union on May 25, 2018. The GDPR aims to strengthen the security and protection of personal data in the EU and unify all EU member states' approaches to data regulation, ensuring all data protection laws are applied identically in every country within the EU.

Who does the GDPR affect?

The GDPR applies to all organizations operating in the EU and processing "personal identifiable data" of EU residents. Even if the organizations are based outside the EU, the GDPR will still apply to them so long as they're dealing with data belonging to EU residents. Personal data is any information relating to an identified or identifiable natural person.

What implications does GDPR have for companies processing the personal data of EU citizens?

One of the key aspects of the GDPR is that it creates consistency across EU member states on how personal data can be processed, used, and exchanged securely. Organizations will need to demonstrate the security of the data they are processing and their compliance with GDPR on a continual basis, by implementing and regularly reviewing robust technical and organizational measures, as well as compliance policies.

Is Domotz GDPR compliant?

Domotz is fully compliant with the GDPR regulation. Our customers,

- Can be made aware of where their data is being held
- Have the right to view, amend, export or delete any information we hold on their behalf
- Express their consent while signing up and can withdraw it at any time

We ensure that we have a high level of protection against unauthorized access to customers' data; any personal data breach would be reported to the data protection authority and to affected data subjects, where feasible, within 72 hours of having become aware of it.

For more details, please consult our privacy policy https://www.domotz.com/product-privacy-policy.php

I am a business using Domotz to serve my customers. How can Domotz support me in being compliant with GDPR?

We encourage you to review your privacy and data security processes and policies, as Data Controllers are primarily responsible for GDPR Compliance. Here at Domotz we can support you ensuring that we have in place robust processes and security standards and our product provides you with all the features needed to comply with data subject rights (the right to view, amend, export or delete any information that we hold on your behalf, including anything held by 3rd party services).

Do you provide documentation about data processing you perform as Data Processor?

Yes, each Data Controller using Domotz can ask us to receive the Data Processing Agreement ("DPA"), submitting their request to privacy@domotz.com.

What Information does Domotz Collect?

Domotz only collects minimal data that are strictly necessary for the provision of its services, such as Name, Address, telephone and email contact of its users. All personal data are stored securely and encrypted using AES-256 encryption.

Domotz also collects:

- **Credentials and configuration data of network devices.** All the credentials and configuration data of network devices shared with Domotz are sent to the cloud and stored there using AES-256 encryption. This data is decrypted and made available to the system only as needed for delivering product features.
- **Geo-location of the networks.** Domotz may collect approximate location where our products and services are installed to provide our services and to assist you in case of troubleshooting. Geolocation is encrypted in the Domotz database.
- **Technical and Diagnostic information from networks and devices.** Domotz collects technical and diagnostic information about the devices in the network. For instance, the MAC address, maker name and model of devices, device status, operating system version, unique device identifiers and the related software. Domotz also collects real-time operating status of your network and its connected devices (e.g., network speed, IP addresses, device event information such as disconnections, system activity, hardware settings, the date and time of your requests) and the related diagnostics information. Domotz may process information from your devices so that we can send you alerts when something happens. Since all personal information is encrypted, no one entering the Domotz database can relate technical information to the owner of the network.
- **Remote connections audit.** One of the features of Domotz is to provide you, or people enabled by you, to remotely connect to your networks via secure sessions. For example, you (or others you allow) could be accessing a PC remotely via our Remote Desktop feature or you could login remotely into the configuration page of a router. **Domotz does not see any traffic content. Domotz only logs, for the benefit of our customers, the date and time these operations are performed by you or your employees.**

Where is data stored?

Domotz users residing in North America have their data stored in servers located in the United States of America. Domotz users residing in Europe and the rest of the world have their data stored in servers based in the European Union.

In what circumstances does Domotz share my data?

Domotz, proudly, does not use any external contractor for developing and managing our Cloud services. All our cloud is managed by Domotz full-time, trusted and screened employees.

No external contractors or third parties have access to the Domotz Cloud.

Nevertheless, for certain activities, we need to rely on third parties and we have to pass them some information. In such cases, third parties will only receive information on a strictly need-to-know basis, and only in order to performs tasks on our behalf and in compliance with our privacy policy and GDPR, but will never have access to the Domotz Cloud.

Trusted partners working for Domotz: Domotz may occasionally use certain third-party service providers to help us provide, improve, protect, and promote our services and to perform functions on our behalf. Examples include fulfilling orders, delivering packages, sending postal mail and e-mail, providing marketing assistance, processing credit card payments.

Domotz partners and third-party developers: We may share de-identified data for research, statistical, and business purposes. Additionally, to improve their software, hardware and services designed for use with our products and services, Domotz may provide any such partner or third-party developer with information that is relevant to that partner's or developer's software, hardware and/or services, as long as the diagnostic information is in a form that does not personally identify you.

How does Domotz keep my information secure?

We take security seriously and care about the integrity of your data. We use administrative, physical, and technical safeguards to protect the confidentiality of personally identifiable information, including encryption, firewalls and SSL (Secure Sockets Layer). The first part of this document explains the Security measures we have in place. We remind our customers that no system can be 100% secure, so we cannot guarantee the absolute security of your information.

We remind our customers that no system can be 100% secure.

One of the major causes of security incidents is poor credential management, such as weak or reused passwords. Hence the reason we only accept strong passwords and we do not accept passwords involved in acknowledged data leaks. Our recommendation is to enforce the usage of two-factor authentication or to rely on an Identity Provider that supports SAML for accessing Domotz.

How long does Domotz save my data and how can I delete it?

Network Data

Domotz stores data related to the networks you monitor on Domotz's cloud servers for as long as the Domotz Agent is configured in the system. You can view and edit all network agents as long as the agent is in the system and you are paying for it. You can delete an agent at any time from the Domotz User Portal. All related information will be immediately removed from the system.

Customer Data

Domotz stores data related to its customers as long as they remain Domotz customers in order to provide them with Domotz Services and products and for legal compliance purposes. Customers can view and edit their information on the Domotz web or mobile applications. Customers can delete their personal data at any time by terminating their account and writing to us at privacy@domotz.com. Accounts and all their data will be removed within one working day. We may retain some de-identified data in the system.

Appendix

How Domotz can improve the security of your networks

Alerting on Unexpected Devices

To protect your network, you must understand all the devices on your network. Establishing which devices are critical, necessary and important to the functioning of all the systems on the network must be done in order to ensure a functioning network and business. When unnecessary devices are placed onto a network, vulnerabilities can be exposed. A Domotz agent continuously scans the network, looking for changes to devices and can alert you when new devices show up on the network. It is up to you then to decide if that device should be blocked, removed or marked as acceptable. This monitoring feature is a great way to ensure that your networks remain secure an in your control.

Hardware Asset Inventory

When Domotz scans your network, it returns a list of devices that are on that network. Information such as MAC Address, IP Address, manufacturer, make, model and type are returned about those devices. The MAC address is a unique number that associates to each individual device on the network. This MAC address can be associated to an Asset Management System, giving you a living document on the status of your equipment. You can know when these Assets are on the network and when they leave the network. Keeping control and an understanding of where your assets are is an important part of security in a system.

Monitoring Open Ports

The Domotz service can be configured to monitor ports being opened on the WAN side of your network. While the Domotz service is not a firewall, it is bringing awareness to you that a WAN-side port may be open to your network, exposing it to potential hackers. If this port points to a device on the network that is using default, or commonly used credentials, then this network is completely exposed. Domotz continuously checks for ports that are opened and alerts you to this potential vulnerability. It is up to you to then take action, by accessing the router/firewall and closing the port, or to accept the port as a known vulnerability. If you reject the vulnerability within Domotz, but do not fix the issue, Domotz will alert you again on the next scan. This continuous monitoring helps mitigate WAN-side security vulnerabilities.

UPnP Port Forward Checking

In addition to looking for WAN-side ports being open, the Domotz service also look for UPnP port forwards enabled by the router. Universal Plug and Play, commonly known as UPnP, is a legacy technology that allows devices on a network to gain access to external services. This technology was developed to make it easy for systems and services to be deployed on a network. The problem with UPnP is that it is not as secure as it should be. While Domotz recommends that UPnP Management should be disabled on your network, there are some cases where it may be required. Domotz looks at which devices are receiving open ports from the UPnP server and alerts you to these devices and the ports they have open. You can be alerted to this information and then can accept or reject this potential vulnerability. As with Open Port Monitoring, if you reject the vulnerability within Domotz and this issue reappears, Domotz will alert you again at the next scan.

Device IP Address Monitoring

While Domotz primarily scans networks at a Layer-2 level (Data Link/MAC Addressing), it also can look for information on Layer-3 (Network / IP Addressing). When a network is being configured, often system integrators will use fixed, or reserved, IP addressing schemes to maintain their systems. DHCP may still be used, but in a known range of addresses. You can use Domotz to alert you when a device with a fixed/reserved IP address changes unexpectedly. This feature is beneficial for security in two ways, 1) it allows you to know when network changes are occurring, and 2) it can be the sign of a potential spoofed MAC address. Leveraging this Domotz monitoring feature, helps ensure that your network schema is solid and resilient.

Centralized Access and Auditing of Remote Accessibility of Client's Networks

Accessibility to your client's networks should be minimized as much as possible. The more accessibility points you have, the more difficult it is to maintain security. You can use the Domotz service as a single point of entry into your client's networks. Features such as VPN on Demand and TCP Tunnel, give you complete access and control of systems on the network and the ability to leverage 3rd Party Tools as appropriate. Furthermore, the Domotz service logs each and every team member/field operator that remotely accesses your client's networks. A date and time stamp is made for each individual, as well as what device was remotely accessed. This feature provides you, as a service provider to your clients, a historical record of what you and your employees have accessed within your client's network. The date and time stamping allows you associate events within the network to your team's accessibility of that network. In addition, access can be easily controlled through your Domotz portal, in case of team members leaving your company or role changes.

This ability to log access helps show your customer how you, as their service provider, has continued to maintain their network and systems as described by any Service Level Agreement (SLA) you have in place.

Configuration Monitoring of Network Infrastructure Devices

Critical to network security is the configuration associated with the network devices, such as managed switches, wireless access points, routers and firewalls. Domotz can alert you when the configuration files associated with these critical network devices change. It is essential that you configure these devices correctly in the first place, but once a configuration is locked down and ready, Domotz can alert you when the device configuration file have been updated or modified. This feature allows you to stay on top of these critical components, see what has been modified and revert to known configuration files as appropriate.

Firmware Upgrades and Patch Management

Management of network devices not only means ensuring proper configuration of the systems and devices, but also making sure that they have the latest firmware and security updates associated with them. It is imperative that you, as a service provider, safeguard your client's networks by keeping devices and systems you install up to date. When a system update is made available by a manufacturer, Domotz makes it easy for you to remotely, and securely, connect to that system and issue the update. Leveraging features like VPN on Demand make it easy to connect to multiple devices simultaneously and issue updates, whether this is through direct connectivity to one or more devices, or by using a 3rd-Party tool associated with that manufacturer and device(s).

Monitoring of Physical Security Systems

Part of maintaining any companies Security Standards is making sure that there is also a physical security system in place. While all business will have locks on the doors, most business will not have access-controlled doors, locks and gates, along with security cameras and video recorders. Today's systems are network controlled and operated. While these systems are often on a separate VLAN, they should still be monitored for online/offline status. In fact, these security systems are extremely important to the operation of any business and therefore should be treated as critically important networks. Domotz tells you immediately when one of these systems go offline, allowing you to take action quickly on these critical systems. Furthermore, Domotz allows you to capture a snapshot from security cameras, so you know that not only is the IP security camera online, but it is also functioning as expected, including pointed in the direction it should be and not tampered with unexpectedly.