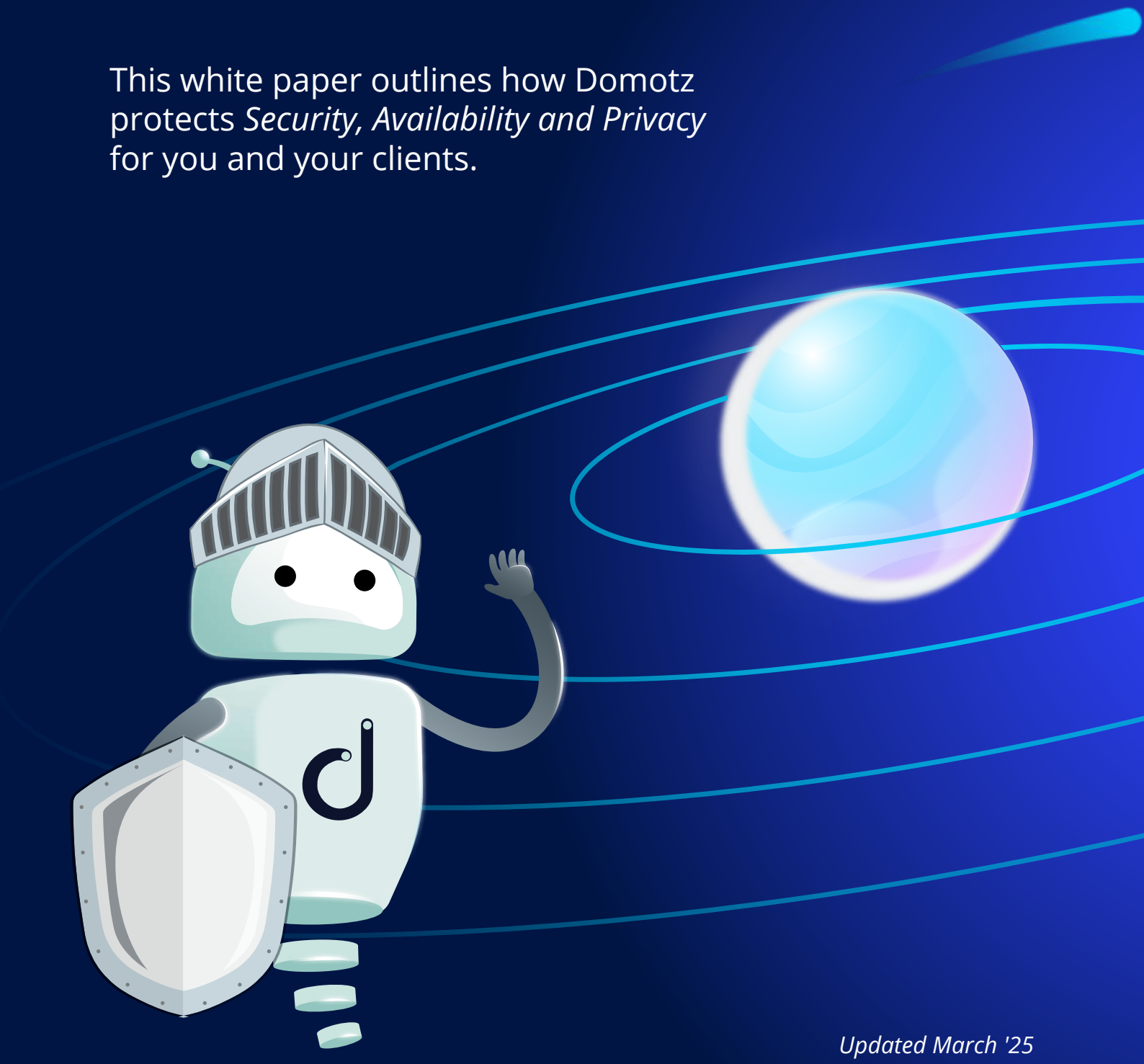
domotz

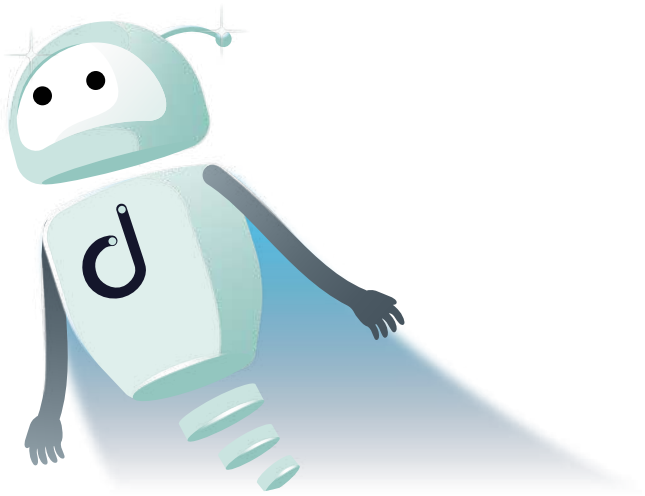
Domotz Security Standards

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



Updated March '25

Contents



domotz

Abstract

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

If you read this document, you are probably a Network Administrator, a Technology Service Provider, or a Managed Service Provider. The security of the networks you manage is your first concern, too. And the tools you use must guarantee the best security, availability, and privacy care you deserve.

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

Security. This section is a walk-through of our security framework and provides an overview of the main actions we take to keep your data safe and continuously improve security.
Availability. Domotz is devoted to ensuring the service is always up & running, even in unexpected events or significant disasters. In this section, we describe the processes and best practices 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 into force. In this section, we describe how all data processed by Domotz are treated.

Finally, at the end of this document, we have decided to add an **Appendix: How Domotz can improve the security of your networks**. Domotz is a remote network monitoring and management system, not a security product. Nevertheless, we have developed several features that can help users increase 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 organizations 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 organisation. 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.

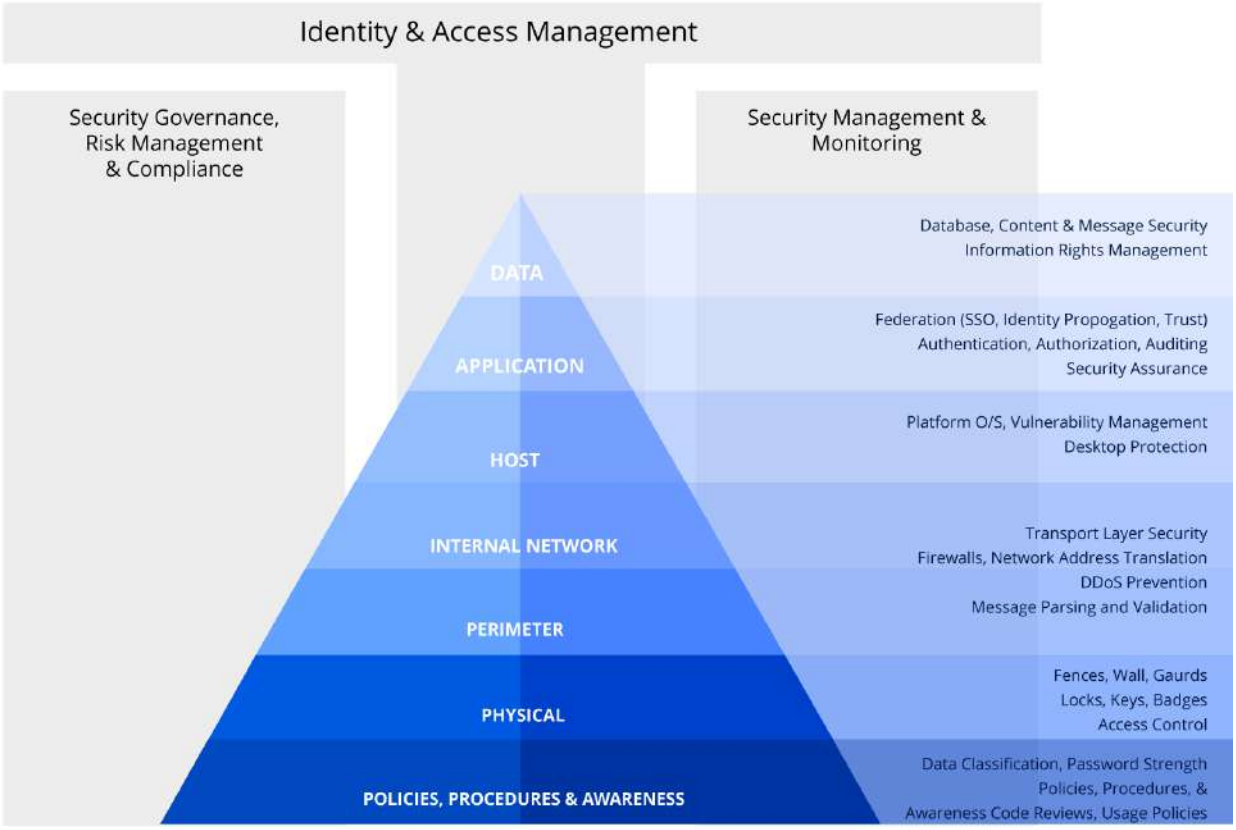


Figure 1 - Layered Security to Defence in Depth

The horizontal layers represent the different levels of protection 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.

ISO/IEC 27001

ISO/IEC 27001 is the world's best-known standard that outlines best practices for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It provides a systematic approach to managing sensitive company and customer information, incorporating processes, people, and technology to protect data confidentiality, integrity, and availability. By adopting the ISO/IEC 27001 framework, organizations adhere to a comprehensive set of security controls that address risks and ensure ongoing compliance through regular internal and external audits.

Domotz is certified under the standard ISO/IEC 27001:2022. Independent certification bodies conduct periodic audits and verify Domotz’s adherence to the standard, ensuring that best practices are rigorously followed.

CIS Controls®

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

CIS Controls® is a global standard and recognized best practices for securing IT systems and data against the most pervasive attacks and threats. These proven guidelines are continuously refined & 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 office.

OSWAP

The Open Web Application Security Project (OWASP) is a non-profit foundation that works to improve software security. 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 many 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 protect the confidentiality of personally identifiable information. Domotz's solution relies on very strict perimete security policies. Only the required standard communication ports are open to the public, while we use a different communication channel for the management.

Encryption

Domotz implements strict requirements for cryptographic encryption and the management of cryptographic keys to protect the confidentiality, integrity, authenticity, & 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 cloud's 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

Name of System/Type of Information	Cryptographic Tool	Encryption Algorithm	Key Size
Data at rest	Python/pycryptodome	AES-256 CBC	256-bit key
Data in transit across boundaries	TLS1.2 or better	AES-256/128 or CHACHA20 (*)	128-bit or 256-bit
User credentials	OpenLDAP/other	Hashed SHA512+salt	N/A (hashed)
Virtual Private Network (VPN on Demand for customer usage)	OpenVPN	AES-256 CBC	256-bit key
Virtual Private Network (VPN for internal usage)	OpenConnect VPN Server over TLS1.2	AES-256 GCM or cipher suites that offer a security level 192-bit or more (*)	192-bit or 256-bit key

Table 1: Cryptographic Controls
(*) The used ciphers are negotiated with the clients (e.g., client browser).

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

Client Communication with Domotz Cloud

This means that 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 at any moment, so the invited guest cannot act anymore on your monitored network. Only the owner (or the delegated Team Member) of a specific collector (network) can invite or revoke guests on his network.

Collector Communication with Domotz Cloud

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

As said before, we do not store the Collector password in clear on our cloud for the Client Communication channel. Sensible information from the Collector to the Cloud is also sent to the HTTPS channel with the same Collector credentials.

Finally, the Domotz solution does not increase the possible attack surface of your network since all the communications are established from within the network toward the cloud. Therefore, no additional ports are opened by Domotz to the external interfaces of your firewall or router.

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 and an HTTPS channel between the App (either Mobile App or WebApp). So, the entire communication from the App to the Collector is encrypted.

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 to guarantee additional security if you are accessing Domotz Pro from a non-secure location, e.g., in a public place, over a non-secure WiFi.

Important to 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 additional security, given that all the supported protocols are encrypted when the data is exposed on the public network. Therefore, even the data for the Telnet and HTTP Remote Connection (which, by default, are not encrypted) with the Domotz solution are secured on the public network by these 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 endpoint 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. The additional layer of security is offered by only the Domotz App requesting to start a new VPN on Demand session will receive the OpenVPN configuration file required to start the session. As a matter of fact, the co figuration file contains the one-time key to connect to the Open-VPN server created on-the-fly for the Domotz Collector.

Device credentials and configuration data of network device

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

All the credentials and configuration data of network devices shared with Domotz are sent to the cloud, stored there using AES-256 encryption rotated annually. In this way, nobody can decrypt the password, even in the remote possibility of a hacker accessing 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 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 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), 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 ar 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 to prevent future mistakes and errors.

Adopting Agile/Scrum methodology, a high level of automated testing, and 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 minimize disruption of our 24/7 service.

Automated tools implement and monitor change process controls that report any exceptions to the managed security team.

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 sometimes, are 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 secures a system by reducing its surface vulnerability, which is larger when it 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 an 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 also uses the same virtualization technology to configure constraints on the usage of resources for any single piece of the application (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 the behavior 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 updated on all security-related patches and updates. The most commonly exploited security vulnerabilities are widely known and already have patches and updates which 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 error

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

Principle of Least Privilege

The 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 machine's IP address that requested access. This system is the least intrusive to users because access is granted based on the machine address. User authentication allows access control on an individual user basis by utilizing user and password lists to provide the necessary authentication.

Moreover, multi-Factor authentication is enforced for all personnel accessing the Domotz systems.

Firewalls and Port Control

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

Anti-Virus and Anti-Malware Protection

Anti-virus protection is enforced on all employee computers and 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 on anti-virus programs that detect malware during a scan. Signature files are designed to be regularly updated by the anti-virus application vendors and downloaded to the client's computer.

A remote monitoring tool is used to ensure that all workstations comply with security configuration requirements, including but not limited to: disk encryption, automatic screen lock, and disabled remote desktop access.

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 management. We have implemented multiple firewall levels, keeping the front-end servers (with no data) completely segregated from the back-end servers (managing customer data).

Vulnerability Scan and Pen Testing

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

Sometimes, we have arranged penetration testing sessions performed by some of our largest customers. Penetration testing from our customers is very welcome and 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 an unauthorized data from leaving the app. It does this by adhering to policies that help determine which traffic is malicious and which is safe. Just as a proxy server acts as an intermediary to protect client's identity, a WAF operates in a similar fashion but in reverse-called a reverse proxy-acting as an intermediary that protects the web app server from a potentially malicious client.

DoS/DDoS Protection

Domotz has implemented several measures at different levels of its architecture to protect from denial of-service attacks. By means of self-diagnostic heuristics, it determines when the system is under excessive stress and rejects requests until the application can serve new ones. Suspicious host IPs are blacklisted.

Physical Security

Domotz is hosted on Amazon Web Services (AWS).

AWS and Domotz implement what is defined as a *Shared Security Responsibility Model*.

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

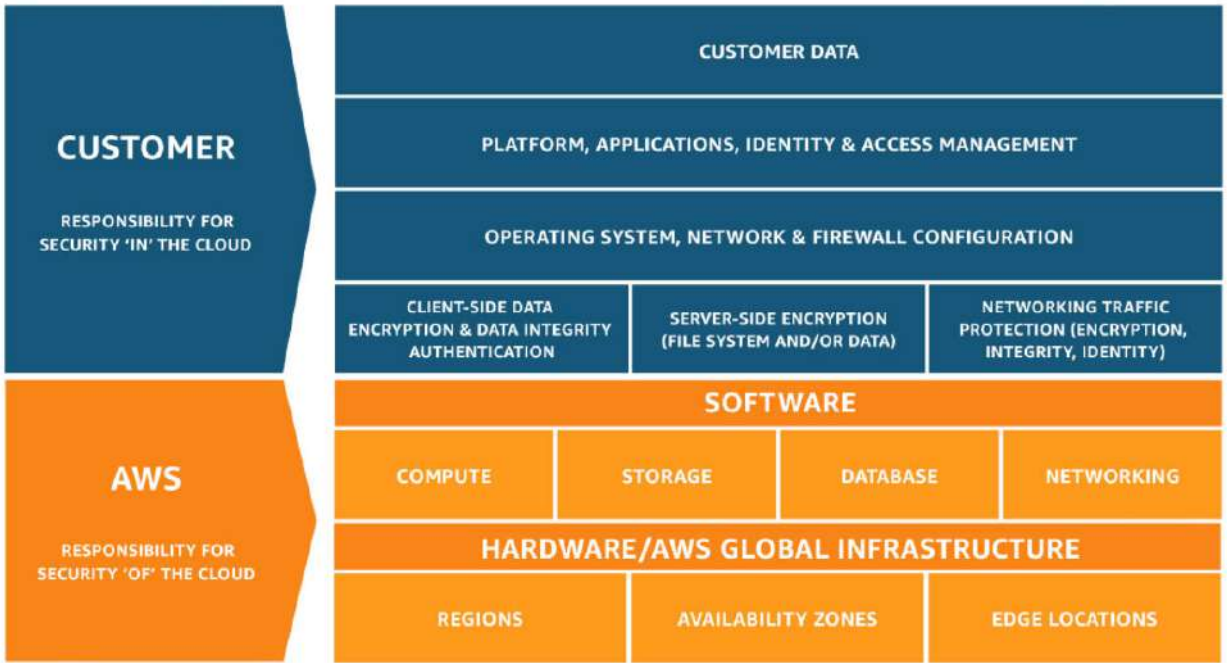


Figure 2 AWS Shared Security Model

AWS data center physical security begins at the Physical Perimeter Layer. This Layer includes several 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/controls/

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
- Certification

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://linfordco.com/blog/user-control-considerations-cuec-soc-report/

Security Policies, Procedures, 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:

- Information Security
- IT Acceptable Use
- Access Onboarding and Termination
- Remote Access
- Data Protection
- Encryption
- Disposal of Information Technology
- Risk Assessment
- System Change
- Security Incident Response
- Disaster Recovery
- Password
- Training
- Vendor Management
- Employee Hiring
- Social Engineering Defense Policy
- Business Continuity
- Data Classification

All our employees are accurately selected and follow periodic training and assessment on Data Privacy and Security awareness. Several phishing simulations are regularly conducted to ensure that all employees stay alert and aware of how to recognize and report social engineering attack attempts. Our Engineering teams follow special training programs for security best practices and security coding.

Identity Access and 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 Domotz uses and imposed at every level of the Domotz organization.
- **Single Sign On (SSO)** is enforced on several 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. Access rights are monitored and periodically reviewed.

Security Governance, Risk Management, and Compliance

The Domotz Management System is adopted to comply with the Domotz Code of Conduct. The Domotz Management System is designed to ensure the following:

- compliance with applicable laws, regulations, and customer requirements;
- conformance with the Domotz Code of Conduct;
- mitigation of risks;
- a process to track, measure and drive improvements in the management system.

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

NIS-2 Compliance

What is NIS-2

The NIS-2 is a European Union directive aimed at improving cybersecurity across EU member states by ensuring a high common level of cybersecurity for critical sectors.
General requirements include:

- Implementing robust cybersecurity measures
- Conducting comprehensive risk analysis
- Establishing incident handling procedures
- Ensuring business continuity plans
- Securing the supply chain
- Protecting network and information systems

Domotz NIS-2 Compliance

Domotz's information security framework ensures compliance with the NIS-2 directive and current applicable laws that incorporate its requirements through
procedures:

- Risk Assessment: we conduct regular risk assessments, to identify potential threats and implement mitigation strategies.
- Security Incident Response: we have established a detailed security incident response plan that outlines specific responsibilities for responding to security incidents. This plan ensures prompt and effective action to mitigate the impact of incidents, preserve evidence, and restore normal operations.

• Business Continuity and Disaster Recovery: business continuity and disaster recovery plans are designed to maintain operational continuity and quickly recover from any disruptions. These plans include backup procedures to ensure data integrity and availability, with regular testing to maintain their effectiveness.

• Vendor Management: we conduct security assessments of our vendors before their onboarding and on regular basis, to ensure our supply chain security.

• Vulnerability Management: monitoring processes are in place to ensure the continuous detection, assessment, and remediation of vulnerabilities.

• Processes Monitoring: we perform regular audits of our processes to ensure compliance with security policies

• IT Acceptable Use: we have a clear IT acceptable use policy that outlines the appropriate use of our IT resources. This policy is designed to prevent misuse and ensure that all users understand their responsibilities.

• Training: all employees receive regular security training to enhance their awareness and understanding of cybersecurity threats.

• Encryption: we enforce stringent encryption requirements for data at rest and in transit. This ensures that information is protected from unauthorized access and breaches.

• Password: we adopt password requirements based on international standards and industry best practices, including complexity requirements and mandatory multi-factor authentication (MFA).

• Access Onboarding and Termination: onboarding and termination policies are in place to ensure that access is granted appropriately and promptly removed when no longer needed for employees and contractors. We conduct regular reviews of access permissions to ensure they remain appropriate for each role.

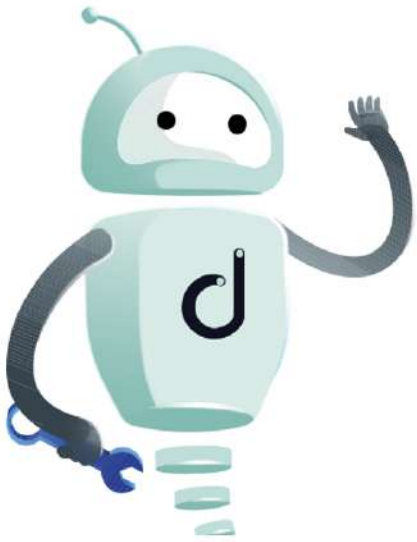
• Remote Access: we have established requirements for secure remote access to our systems. These requirements include the use of VPN and MFA to ensure the security of remote connections.

Security Monitoring and Management

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 nearly real-time to the personnel in charge of the specific controls so that we can guarantee a prompt response to security threats to the relevant team in charge.

The Incident Response Team is responsible for implementing the plan by executing an Incident Response Procedure, which is established to provide a quick, effective, and orderly response to security incidents.



Availability
Uptime and Service Availability

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

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

The status of the Domotz services can be monitored by the users anytime at this URL: https://status.domotz.com/

In Q2 2024, Domotz had an uptime of 99.967%, including 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

To prevent disruption to services, faults in 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 methodology, a high level of automated testing, and wide adoption of real-time system monitoring, together with post-implementation review, retrospective analysis, and customer feedback, are the main frameworks adopted to reduce the possibility that unwanted changes and faults are introduced into the Domotz solution and to improve the availability of our 24/7 service continuously.

Capacity Planning

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

Backup, Recovery, Disaster Recovery

Domotz has implemented procedures to recover its cloud infrastructure and services within set deadlines in the case of a disaster or other disruptive incident. This plan aims 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.

Persistent Data Backup

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

Dynamic Data Backup

Dynamic data are strictly related to Domotz users.

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.

All Data (relational and non-relational/historical) are backed up continuously 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 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 manual administrative intervention. In case of an infrastructure failure, the expected RPO is less than 30 min.

In addition to the real-time backup on standby instances, Domotz performs periodical backups exported outside the data center over a secure channel to a different data center. All the transfer of backups is ensured on a secure and encrypted channel. A write-once read-many policy is applied and protects backups against unauthorized changes and ransomware attacks.

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 primary node failure, backup instances are provisioned with the latest snapshot of dynamic data and started. In this case, the expected RTO is less than 30 min.

Disaster Recovery

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

In case of a catastrophic disaster hitting an AWS data center, Domotz can rebuild the entire infrastructure in a different data center (AWS region) and provision the nodes requiring Dynamic data. In this case, the expected RTO is less than 1 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 GDPR Affects

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

Implications of GDPR

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 continually demonstrate the security of the data they are processing and their compliance with GDPR by implementing and regularly reviewing robust technical and organizational measures and compliance policies.

Domotz GDPR compliance

Domotz is fully compliant with the GDPR regulation.
Domotz's information security framework includes policies dedicated to GDPR regulation. The procedures to comply with the rights of our customers are periodically reviewed and tested.

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 affected data subjects, where feasible, within 72 hours of becoming aware of it.

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

Domotz GDPR Compliance Support

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 by ensuring that we have in place robust processes and security standards and that 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).

Documentation as a Data Processor

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

Information that Domotz Collects

Domotz only collects minimal data that are strictly necessary to provide its services, such as its users' Name, Address, telephone, and email contact. 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. They're decrypted and made available to the system only as needed for delivering product features.

Geo-location of the networks: Domotz may collect approximate locations where our products and services are installed to provide our services and assist you in 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 the real-time operating status of your network and its connected devices (i.e., 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 to send alerts when something happens. Since network related personal information is encrypted (location and public IP address), no one entering the Domotz database can relate this technical information to the network location.

Remote connections audit: One of the features of Domotz is to provide you, or people enabled by you, to connect to your networks via secure sessions remotely. For example, you (or others you allow) could be accessing a PC remotely via our Remote Desktop feature, or you could log in remotely to 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**.

Data Storage Locations

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.

Data Sharing Circumstances

Domotz does not use any external contractors to develop or manage 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 pass them some information. In such cases, third parties will only receive information on a strictly need-to-know basis and only perform 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 perform functions on our behalf. Examples include fulfilling orders, delivering packages, sending postal mail and e-mail, providing marketing assistance, and 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.

Domotz Information Security

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, includi encryption, firewalls, and SSL (Secure Sockets Layer). The first part of this document explains t Security measures we have in place. We remind our customers that no one can be 100% secure, so we cannot guarantee the absolute security of your information.

Your Data, Retention and Deletion

Network Data

Domotz stores data related to the networks you monitor on Domotz's cloud servers for as long as the Domotz Collector is configured in the system. You can view and edit all network collectors as lon as the collector is in the system and you pay for it. You can delete an collector 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 to provide them with Domotz Services and products for legal compliance. Customers can view and edit their information on the Domotz web or mobile applications. Customers can delete their personal data anytime by terminating their account, writing us at privacy@domotz.com. Accounts and all their data will be removed within 1 working day. We may retain some de-identified data in the system.

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.

Appendix

How Domotz can improve the security of your networks

Alerting on unexpected devices

One of the easiest ways to protect your network is to 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 to ensure a functioning network and business. When unnecessary devices are placed onto a network, vulnerabilities can be exposed. A Domotz collector continuously scans the network, looking for device changes, and can alert you when new devices appear on the network. You must 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 and in your control.

Hardware asset inventory

When Domotz scans your network, it returns a list of devices. Information such as MAC Address, IP Address, manufacturer, make, model, and type are born about those devices. The MAC address is a unique number associated with each network device. This MAC address can be associated with 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. Keeping control and an understanding of where your assets are is an essential part of security in a system.

Monitoring Open Ports

The Domotz service can be configured to monitor ports opening on your network's WAN side. 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 uses the default, or commonly used credentials, then this network is completely exposed. Domotz continuously checks for opened ports and alerts you to this potential vulnerability. It is up to you to take action by accessing the router/firewall and closing the port or accepting the port as a known vulnerability. If you reject the exposure 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 forwarding

In addition to looking for open WAN-side ports, the Domotz service also looks 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 should be more secure. While Domotz recommends that UPnP Management should be disabled on your network, some cases may require it. Domotz looks at which devices are receiving open ports from the UPnP server and alerts you to these devices and their open ports. You can be alerted to this information and 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 configuring a network, system integrators often 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 a sign of a potential spoofed MAC address. Leveraging this Domotz monitoring feature helps ensure your network schema is solid and resilient.

Monitoring of Physical Security Devices

Part of maintaining any company's Security Standards is ensuring a physical security system is in place. While all businesses will have locks on the doors, most companies will not have access-controlled doors, locks and gates, security cameras, and video recorders. Today's systems are network owned and operated. While these systems are often on a separate VLAN, they should still be monitored for online/offline status. These security systems are critical to the operation of any business and, therefore, should be treated as critically essential networks. Domotz tells you immediately when one of these systems goes offline, allowing you to take action quickly on these critical systems. Furthermore, Domotz will enable 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.

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 entry point 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 and what device was remotely accessed. As a service provider to your clients, this feature provides a historical record of what you and your employees have accessed within your client's network. The date and time stamping allows you to associate events within the network with your team's accessibility of that network. In addition, access can be easily controlled through your Domotz portal if team members leave your company or role changes.

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

Monitor the DHCP request rate.

Domotz monitors the number of DHCP requests traveling on the network. Changes in the rate of DHCP requests can be identified and reported. This feature helps respond promptly to configuration issues or malfunctioning devices and discover potential network attacks like DHCP flooding.

Configuration Monitoring of Network Infrastructure Devices.

The configuration associated with network devices, such as managed switches, wireless access points, routers, and firewalls, is critical to network security. 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. Still, once a configuration is locked down and ready, Domotz can alert you when the device configuration file has been updated or modified. This feature lets you stay on top of these critical components, see what has been changed, and revert to known configuration files as appropriate. Moreover Domotz allows to backup the configuration both automatically and manually, providing easy restoration and quick recovery from issues.

Firmware Upgrades and Patch Management.

Management of network devices means ensuring proper configuration of the systems and devices themselves and ensuring 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 the devices and systems you install up-to-date. When a manufacturer makes a system update available, Domotz makes it easy for you to remotely and securely connect to that system and issue the update. Leveraging features like VPN on Demand makes it easy to connect to multiple devices simultaneously and issue updates, whether through direct connectivity to one or more devices or by using a 3rd-Party tool associated with that manufacturer and instrument(s).

Detection of IP conflicts

Domotz can identify any duplication of IP address in your network. You will receive an email when such event occurs, reporting which devices are involved. This feature allows to discover misconfigurations and security issues, such as the presence of unauthorized DHCP servers, potential Man-in-the-Middle (MitM) attacks, and rogue devices.

domotz