WHITE PAPER

Fire Safety Cloud Apps:

Cybersecurity meets Secured Cloud Connectivity

siemens.com/firesafety

SIEMENS

Executive Overview

Timing is everything when it comes to fire safety because people, assets and business continuity are at stake. Keeping fire protection systems up and running is a 24/7 undertaking that involves two important goals today. The first is to make the communication between fire protection systems and the interfaces that collect data quicker, more reliable and smart. The second is to give service providers and their customers a solution that helps fix issues as quickly and seamlessly as possible. Both goals can be accomplished more easily and cost-effectively with remote access and maintenance.

As defined in this paper, cybersecurity is:

"The protection of life and company assets from harm caused by digital attacks against the availability, confidentiality, integrity, authenticity and reliability of information in cyberspace. Cyberspace is the complex system of interaction between people, software and services that is facilitated by using technical means to connect them to the Intranet and Internet."

However, a minority of buildings today have the cloud connectivity needed to make remote access possible. This despite inroads that digitalization and the Internet of Things (IoT) have made in the fire industry in recent years, unlocking new value like real-time operations, optimization and prescriptive analytics. Then comes COVID-19, which might have an unexpected acceleration of remote access use to manage fire safety and other building technologies. Perhaps the pandemic's requirement for everyone to keep their distance will speed the acceptance of remote monitoring, maintenance and control of fire safety systems.

Even with the pandemic, though, the question of cybersecurity comes into play immediately. Is cloud connectivity secured, is the first question asked by many professional services companies, who provide fire safety system monitoring and maintenance for customers of all types and sizes in a broad spectrum of industries. The question is echoed by many of their customers as well. The answer is a resounding yes – if cloud connectivity follows strict cybersecurity methods. This paper explores the impact of cybersecurity on remote monitoring, maintenance and control of fire safety systems. Cloud connectivity with security in mind stands to make a dramatic difference in how optimal uptime is maintained for these crucial systems.

Introduction

We live and work in an exciting era. It’s one defined by Industry 4.0 – the digitalization of business. Digitalization provides numerous advantages, including greater convenience and increased efficiency. It also presents security challenges. Cyber attacks are a constant and increasing threat due to the across-the-board connectivity that makes digitalization possible. In today’s connected world, the likelihood of a cyber attack is high.

How do you confidently face and mitigate cyber threats? You take a holistic approach to security measures across all aspects of your organization.

At Siemens Smart Infrastructure, we believe security begins during product development. We’ve adopted a “think security” philosophy in the development of our fire detection products, solutions and services. This paper provides insight into how Siemens approaches cybersecurity requirements during the product development and lifecycle management processes.

Before discussing cybersecurity, let’s define it. For this document, we define cybersecurity as the protection of life and company assets from harm caused by digital attacks against the availability, confidentiality, integrity, authenticity and reliability of information in cyberspace. Cyberspace is the complex system of interaction between people, software and services that is facilitated by using technical means to connect them to the Intranet and Internet.

Let’s also define what it means to take a holistic approach to security. Leading companies and institutions take into account four key factors that impact security strength – people, communication, processes and technology. In general:

- People need a broad and lasting awareness of the importance of security, both physical security and cybersecurity
- Communication helps establish a culture of security when it’s clear and concise
- Processes that are actively applied are as important as technology in protecting organizations from cyber threats
- Technology needs to be tested, vetted and matched with other suitable building blocks in order to make an organization's asset more secure

The spectrum of security challenges is broad. While physical threats are more obvious and change less often, cyber challenges can be more nefarious due to an ever-changing threat landscape. When it comes to aligning security with business needs and the inevitable move toward convenience, we put a focus on cybersecurity from the outset.

Capturing the remote connectivity market

The market for remote connectivity for fire safety systems is vast, since the majority of buildings are not connected to the cloud. Additionally, most sites do not have an on-premise danger management station. This means that service providers and customers can't obtain an overview of happenings at their sites without running to a fire alarm control panel. Fire safety solution and service providers are left asking themselves:

> "Being smart about cloud platforms and services can make the difference between gaining a competitive edge and falling behind rivals."

- How do I gain a quick overview of my customers' fire protection systems?
- How can I reduce high traveling costs and increase customer service quality?
- How can I provide periodic maintenance more efficiently and deliver evidence of executed tests to customers?

Our Cloud Apps from Siemens solve these problems by connecting fire safety solutions to the cloud, which helps digitalize the fire industry and create remote-accessibility. They use a gateway to connect each site to the cloud so that panel events can be sent to the cloud. Service providers and customers are then able to directly monitor and operate the fire control panels without having to stand in front of them.

To combat the wide array of security threats that are introduced by this technological transformation, Siemens has developed a layered defense approach that detects, responds and remedies multiple levels of threat. This includes continuous product development and an ongoing process for identifying and mitigating the challenges that come with exposing building and fire data from the local network to the cloud.

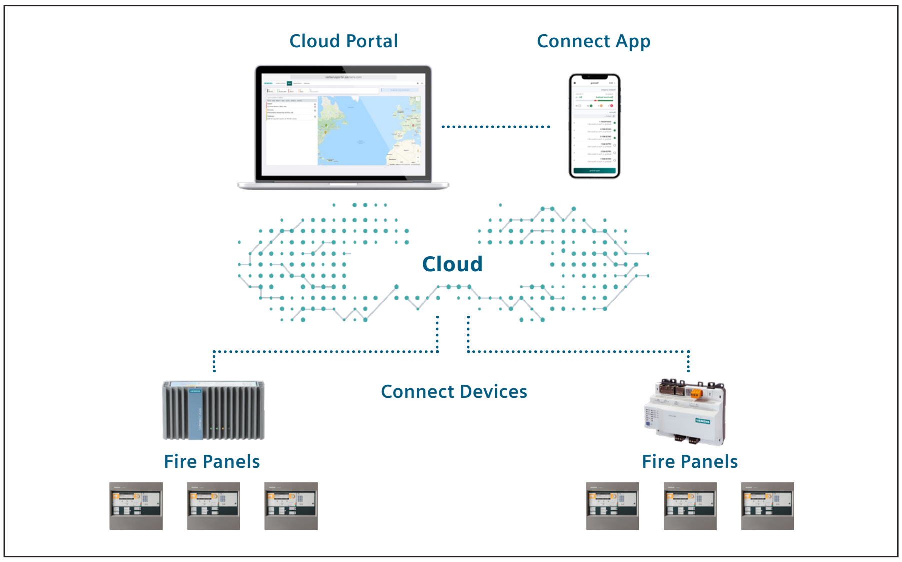


Figure 1 – Cloud Apps Portfolio

"Being smart about the use of cloud platforms and services can make the difference between gaining a competitive edge and falling behind rivals," according to McKinsey and Company's Andrea Del Miglio, Partner, and Will Forrest, Senior Partner.[1]

Siemens Cloud Apps portfolio

To help service providers and their customers get the most from cloud platforms and services, Siemens developed the fire safety Cloud Apps portfolio that includes a web-based Portal and Connect App (iOS and Android). They are part of Siemens' holistic approach to fire protection in which every element of fire protection matters – from detection and evacuation to extinguishing, danger management and cloud services.

The Portal makes services more efficient for both service providers and customers.

Cloud Apps

Portal

The Portal website delivers an overview of all connected sites as well as easy access to them. It also eliminates unnecessary service visits and prepares service engineers for those that still need to take place.

The Portal makes services more efficient for both service providers and customers by providing secured 24/7 connectivity, multi-site dashboards, real-time monitoring and simple operation. The 24/7 connectivity allows access to customer sites from anywhere and at any time.[2] So, there's no need to be on site unless local regulations require it; permitted users just open their browsers, go to the Portal website and login to find everything they need.

[1] Del Miglio, Andrea and Will Forrest, "Creating value with the cloud," Digital McKinsey Insights, December 2018, p. 3.

[2] Depending on local and technical restrictions. Please check with your local Siemens account.

The built-in, multi-site dashboard shows a simple overview of connected sites in real time, in one place and at a glance. Color indications on the status bar show which sites are running smoothly and which may be having problems. By monitoring everything in real time, service providers will often know issues before their customers do. They can learn more about a specific site by just clicking on it to see a detailed overview. Service engineers can also check each site to discover any issues before starting their maintenance routes. That way they'll arrive on site with the right information, equipment and tools, saving time and travel expenses.

The Portal includes a remote access functionality which helps avoid unprepared or unneeded service visits. Through a virtual PMI version of the panel, service engineers can remotely view what is happening on site, while the Engineering Tool enables remote commissioning and configuration changes. The service engineer can thus remotely advise the customer and offer additional services and support without having to be on site.

The Portal can be used to streamline maintenance activities. It automatically stores the configured devices and tracks testing and maintenance activities for connected sites. This information can be used to create and assign test plans, store test results and export to code compliant test reports.

It was designed to be easy to use on any smart mobile device. The user interface is simple so that service providers and customers can focus on what is important. The application is continuously improved and updated automatically.

The user interface is simple so that users can focus on what is important.

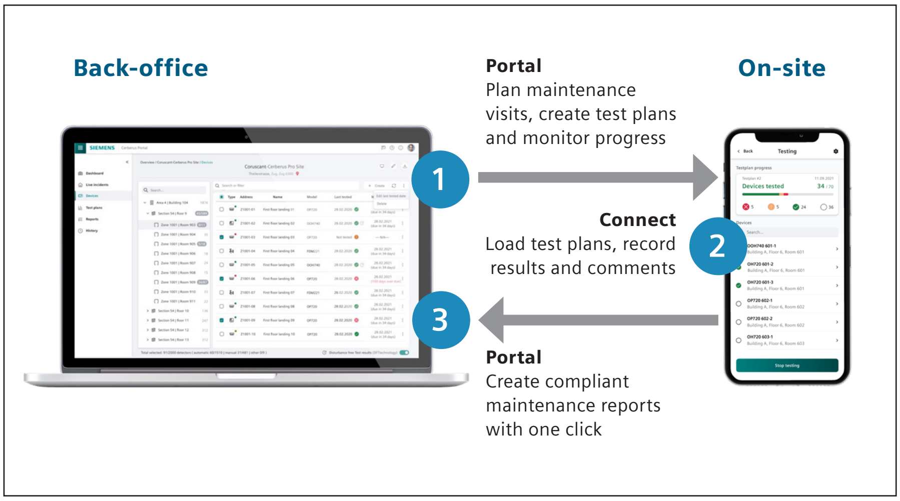

Back-office
On-site
Portal
Plan maintenance visits, create test plans and monitor progress
1
Connect
Load test plans, record results and comments
2
3
Portal
Create compliant maintenance reports with one click

Figure 2 – Test and Inspect Management

Connect app

The Connect app is a smartphone application that enables service providers to use only one person to deliver efficient testing during periodic maintenance. The application then provides reports of those tests to the customer. It reduces the service engineer's manual work and proves that the fire safety system is running as expected according to the service level agreement.

Additionally, the Connect app allows end customers (e.g., building owners and technical facility managers) and service engineers to get full transparency of their fire site. They can view current and past events of their site, as well as set up push notifications directly on the app to always know what is happening.

Connect application is faster and more efficient than regular detector testing since only one person is needed.

Additional benefits of the Cloud Apps

The Cloud Apps introduce a number of additional benefits for three important groups: system integrators or service companies, owners or investors, and consultants, planners or designers.

Systems integrators or service companies are looking for new opportunities to increase their competitiveness. For example, remote configuration and commissioning of the systems will reduce travel costs and improve utilization of fire safety engineers, who are becoming an increasingly rare commodity.[3]

By using Cloud Apps to digitalize the service business, system integrators and service companies can take the next step in further improving their resource utilization. They can monitor, operate[4] and service connected sites from remote locations with minimum hardware costs and without investing in additional in-house server capacity. These companies can also discover new digital business opportunities that extend their offerings and develop new business models. In addition, they can increase satisfaction for customers and employees alike by offering real-time monitoring, proactive services, notifications and remote operational support.

[3] Remote control requires local jurisdiction approval if not permitted under current codes of practice.

[4] Depending on local and technical restrictions. Please check with your local Siemens account.

Owners and investors find that Cloud Apps put peace of mind at their fingertips.

Owners and investors find that Cloud Apps put peace of mind at their fingertips. For example, live overviews let them know what is happening with their fire protection systems at anytime and anywhere.[5] The system is set up to initiate quick responses to fire events. The owners and investors can determine the category of events that trigger notifications and who will receive them. The detailed information about the event makes troubleshooting more time efficient. This means that the Cloud Apps help maintain business continuity by increasing the uptime of the fire protection systems.

The consultants, planners and designers are looking for innovative solutions with future-ready fire protection systems that ensure adherence to standards and regulations.

"Without security, the truly transformative benefits of connectivity and automation are at risk. Embracing cybersecurity means protecting your customers and your bottom line," according to Sedar Labarre, Vice President, Booz Allen Hamilton.[6]

"Security by Design:" Siemens Commitment to Comprehensive Security

Cyber attacks are among the fastest growing criminal activities in the world today. They range from insider threats, ransomware attacks, opportunist threats and hacktivism all the way up to business espionage, terrorism and state-sponsored cyber terrorism. In order to be prepared to respond to a fast, complex and constantly changing threat landscape, it's essential that organizations like yours take a holistic approach to security.

While the responsibility to secure your environment lies with your organization, Siemens is committed to developing products that enable you to take a holistic approach to security. This is true for our broad portfolio of building technology products, solutions and services.

[5] Depending on local and technical restrictions. Please check with your local Siemens account.

[6] Labarre, Sedar, "Cybersmart Buildings: Securing Your Investments in Connectivity and Automation," February 2017, Booz Allen Hamilton, p. 3.

Our commitment is multifaceted. First and foremost is “Security by Design,” our end-to-end approach to product development that builds in security from the beginning. It includes an ongoing cycle of testing, enhancements and evolution to keep our products and solutions at the forefront. In addition, we are a founding member of the global Charter of Trust,[7] which calls for binding rules and standards to build trust in cybersecurity and further advance digitalization.

Our end-to-end "Security by Design" approach to product development builds in security from the beginning.

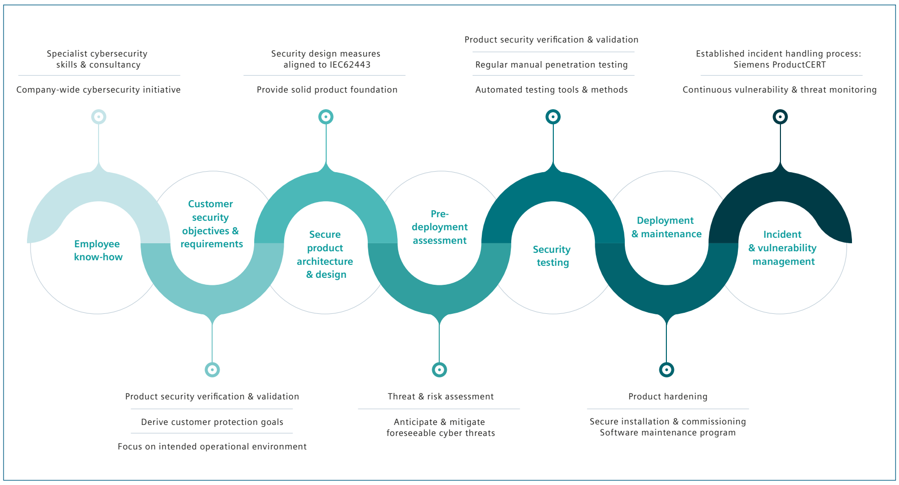

Specialist cybersecurity skills & consultancy
Company-wide cybersecurity initiative
Security design measures aligned to IEC62443
Provide solid product foundation
Product security verification & validation
Regular manual penetration testing
Automated testing tools & methods
Established incident handling process: Siemens ProductCERT
Continuous vulnerability & threat monitoring
Employee know-how
Customer security objectives & requirements
Secure product architecture & design
Pre-deployment assessment
Security testing
Deployment & maintenance
Incident & vulnerability management
Product security verification & validation
Derive customer protection goals
Focus on intended operational environment
Threat & risk assessment
Anticipate & mitigate foreseeable cyber threats
Product hardening
Secure installation & commissioning
Software maintenance program

Figure 3 – Siemens Cybersecurity Initiative Highlights

Simply put, we design with security in mind. Our company-wide initiative provides a risk management program that actively drives comprehensive security methodology for all Siemens products, solutions and services. It identifies best practices and sets technical standards, processes and policies that must be met. We also contribute to international standards and strive to deliver products that meet security standards such as ISA/IEC 62443, UL2900, ISO/IEC 27001 and OWASP.

Security by Design expertise

The effectiveness of a product’s cybersecurity design is attributed to the expertise of the development team. As part of our Security by Design methodology, we invest not only in technology developments for digital protection and product security, but also in the training required to maintain high levels of employee cybersecurity expertise.

Throughout the lifecycle of the product, our experts perform security threat and risk assessments in order to address expected risk in the intended application of use. This assessment starts early on in the process and is repeated as required to identify and mitigate risks appropriately.

[7] For more information, go to www.charteroftrust.com

Throughout the lifecycle of the product, solution or service, our experts perform security threat and risk assessments.

In addition, regular product security testing is conducted by external experts who use manual penetration tests, alone or in combination with automated machine security testing. The idea is to break the system in order to make it more secure. This testing ensures that the selected product, solution or service meets our security requirements. The test results are recorded and used to identify any necessary corrective actions.

“Security by Default”

The concept of Security by Default is closely related to Security by Design. It calls for all protective measures to be automatically activated and in force by default at the time of product delivery, installation or initial commissioning. Security by Default is applied more frequently today to counteract the fact that many developers used to ship software with wide-open settings because they assumed users would configure the security at setup. Unfortunately, the majority of users never even consider security once the software is running. For security to work effectively, it must be built in and active from day one. Furthermore, security that’s added later is difficult to patch or retrofit when new methods of attack are identified.

While Security by Default is gaining ground, there are no uniform regulations currently governing this approach. As a result, appropriate security settings are often not defined in advance, resulting in the need for users to adjust them after the product is installed. Siemens, on the other hand, designs and preconfigures its systems to use the most secure settings at installation by default and as a standard. We adopt the highest appropriate level of security and data protection and incorporate it into the design of the product, functionalities, processes and operations. Finally, we make sure that the embedded security is activated immediately once the system is put into use.

Making Security by Default successful involves examining the issue of how products can provide optimum security once they leave the factory. Well-known examples of vulnerabilities in real-life settings show how many businesses were easy targets for malicious actors. In one of the most unusual incidents, cybercriminals hacked a casino through an Internet-connected thermometer in an aquarium in its lobby.[8] This foothold gave the hackers access to the casino's network and then its database of high-roller gamblers, which they uploaded to the cloud. Some solutions are easier than others. To maintain a reasonable level of security on site, it makes sense to demand creation of a new password when the user initially logs in. But what further security measures need to be considered and what trade-offs may arise in the interest of user-friendliness? There have been no simple, universal answers to date, let alone specific recommendations for action. Instead, the actions are developed by the responsible product team. The signal is clear, however: cybersecurity is no longer optional. It's now a mandatory requirement.

Careful delegation of access rights according to job duties can limit damage from both system users and potential hackers.

"Principle of Least Privilege"

The Principle of Least Privilege has been a staple of information security since it was introduced by Jerome Saltzer and Michael Schroeder in 1975.[9] It's based on the concept that careful delegation of access rights according to job duties can limit damage from both system users and potential hackers. It calls for authorized users of a system to have the minimum necessary access – or privilege – and for the shortest duration needed to get their work done. It can also be used to limit the number of interactions possible so that unintentional, unwanted or improper use of privileges is less likely to occur. When properly applied, least privilege helps prevent the damage that can result from a user's accident or error and helps limit what a hacker can do based on the user account that's been compromised.

The least privilege principle is helpful at every level of a system and for any user, database and process. We apply it to our systems based on a user's "need to know," limiting data and application access to the minimum needed for a specific task. This is crucial in the event of a successful cyber-attack because the hacker

[8] For more information, see https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/.

[9] Smith, Richard E. "A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles," IEEE Security & Privacy, Volume 10, Issue 6, Nov.-Dec. 2012.

gains the privileges of the user account accessed. If an attack is through the account of an employee with administrative privileges, an infection can spread system-wide. Therefore, a user who doesn't need administrative access should work with fewer privileges and limited scope whenever appropriate. It's also important that technical users have only the minimum privileges needed to access the resources they are working on and not more. Otherwise, if a technical user's account is compromised, a hacker can misuse the designated privileges to perform unwanted activities such as dropping an entire database or installing malware.

Divide critical functions among different authorized users to prevent fraud and other abuses.

"Separation of Duties Principle"

Another IT security concept that's closely related to the Principle of Least Privilege is the Separation of Duties Principle. It divides critical functions among different authorized users to prevent fraud and other abuses by employees or other authorized people. It states that no user should be given enough privileges to misuse the system on his or her own. Separation of duties can be enforced either by defining roles that can't be executed by the same user or by enforcing the four-eyes principle at access time. In the latter, the first person to execute a two-person operation can be any authorized user, while the second person must be a different authorized user.

As part of our holistic approach to cybersecurity for our offerings, we use the least privilege principle to address the complete lifecycle of a system, from design, to commissioning and operation, to migration and decommissioning. Direct benefits of applying the principle are better security and minimized attack surface. Beyond this, there may be additional benefits in stability, traceability and other resource-dependent services.

Siemens' comprehensive approach to our portfolio's cybersecurity is driven by international standards.

ISA/IEC 62443

Digitalization and cybersecurity are two closely interrelated topics that are of great strategic importance for organizations around the world. When it comes to the cybersecurity of our portfolio, Siemens takes a comprehensive approach that is driven by international standards.

One of the most important standards is ISA/IEC 62443, developed by the International Society of Automation (ISA) and adopted by the International Electrotechnical Commission (IEC). ISA/IEC 62443 has proven its worth in the industrial automation environment. It's aimed at plant operators, integrators and component manufacturers, and covers the urgent security-relevant aspects of industrial security.

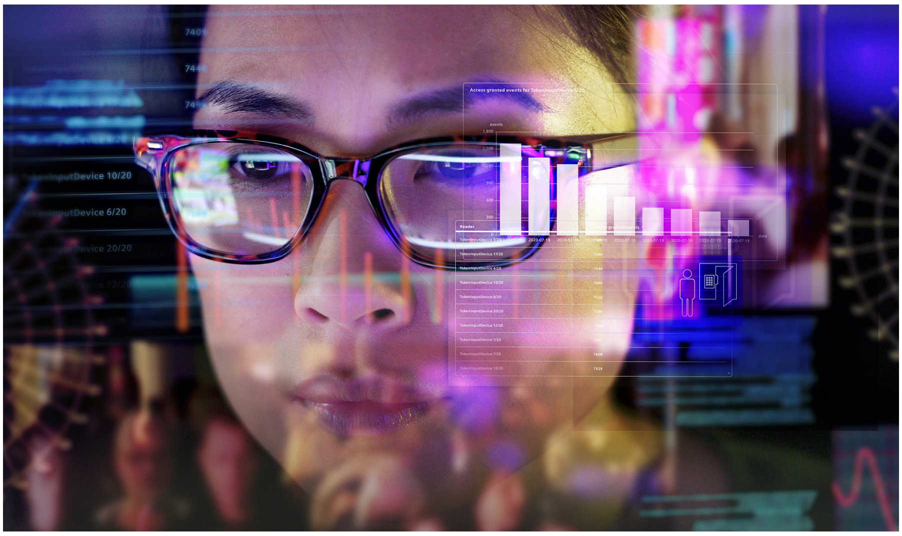
Siemens Smart Infrastructure Building Products are certified according to IEC 62443-4-1 with maturity level 3. This certification is prerequisite to certifying separate products, i.e., achieving IEC62443-4-2 product certification, and establishing secured fire systems.

Applying Security by Design to Cloud Apps

Siemens has taken the Security by Design approach to all aspects of the Cloud Apps portfolio. The following is a close look at the key features of our cybersecurity program for these cloud-based applications, beginning with the secured gateway that is certified according to IEC62443-4-2.

Gateway applications are developed according to the latest standards and security design measures are aligned to ISA/IEC62443. These applications feature end-to-end encryption between devices and access points to cloud services. The apps have certificate-based communication security in place, including easy integration of certificates within the customer's IT infrastructure. Access to the system is based on appropriate user roles and their designated tasks and responsibilities.

The Cloud Apps support antivirus and malware protection software on customer devices.



The Cloud Apps support antivirus and malware protection software on the customer devices. Since the gateway is a closed box, customers and service engineers can trigger updates of gateway firmware via the cloud but they cannot install their own software on the gateway. The apps support hardware and software firewalls. Off-premise, the Cloud Apps use Amazon Web Services (AWS) to host infrastructure and platform services and to perform access control functions.

The services, along with Siemens Connect Devices, enable an end-to-end solution that unlocks new value for customers. AWS provides the cloud infrastructure hardware, software and networking needed to meet the requirements of security-sensitive organizations. AWS is also responsible for protecting the global infrastructure that runs all the Cloud Apps services offered through the cloud.

Access control to the Cloud Apps is a two-step process for both service providers and customers. It begins with user authentication and identification conducted by Siemens ID, which is based on an Identity as a Service (IDaaS) platform. The main benefit of Siemens ID is that it provides a single sign-on to the Siemens applications. It includes ID administration and security token services.

The next step in access control is authorization, a security mechanism used to determine user privileges to devices, services, data and application features. It defines the specific part of the infrastructure resource that can be accessed and the set of actions the identified user can perform. The Cloud Apps implement role-based access control (RBAC), which limits a user to authorized applications and features. Access to sites and devices is limited by organizations and scopes.

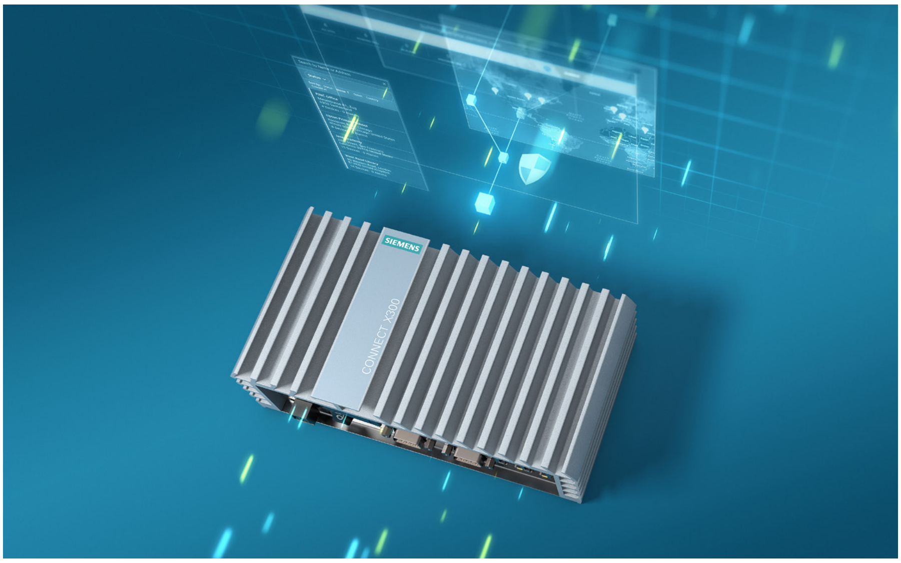
Data privacy is another important feature of the Cloud Apps.

All personal data processed in context with the Cloud Apps complies with European Union General Data Protection Regulation (EU GDPR), which gives individuals control over their personal data.

All data is secured by encryption both at rest and in transit. Data encryption-at-rest uses standard AWS encryption that conforms to the Federal Information Processing Standard (FIPS) 140-2 standards. All data in transit, such as in communication to and from the Cloud Apps, is encrypted using HTTPS/TLS1.2.

The remote access to the fire networks enables commissioning engineers to remotely service and access fire networks without requiring inbound connectivity.[11]

The Connect Devices are designed with a number of security hardening principles that limit unauthorized access and reduce security risks.



Connect Device

On-premise activities

The Connect Device is the edge connectivity device used to gather building data on premise and then provision it to the Cloud Apps or other Siemens digital services.

The Connect Devices are designed with a number of security hardening principles that limit unauthorized access and reduce security risks. It employs access control through authentication and authorization. All Connect Devices feature port restrictions to increase the security of the device from tampering.

The Connect Device operating system is protected by encryption keys with SSH connections disabled. To onboard the Connect Device to the Cloud Apps, a factory imprinted certificate or unique activation key is required.

To further increase the security of the system and to decrease the installation time, the Connect X200 can be mounted inside the fire panel.

Only people with the right to view the data have regular access to it.

Other considerations to mitigate cyber threats

Communication between the Connect Device and the Cloud Apps is via the Internet. The connection is always outbound traffic that is initiated by the Connect Device on premise utilizing HTTPS. All data communication via the Internet is encrypted.

Cloud Apps cybersecurity deployment

The Cloud Apps have cybersecurity policies that preserve three things about data: confidentiality, integrity and availability. Only people with the right to view the data have regular access to it. Those who access the data may rely on its accuracy. And the apps make it easy to access the data when and where needed.

However, it must be recognized that security is a shared responsibility. Security is not solely under the purview of the cloud infrastructure and cloud application providers. Neither is it solely under the purview of on-premise IT/OT network managers and users.

The cybersecurity hardening guidelines for the Cloud Apps are published and maintained throughout their product lifecycles. These guidelines describe how the system needs to be configured, commissioned and operated in order to ensure reliable operation of these services. They consist of, for example, which settings to activate or deactivate, firewall configurations, and the setting of user and system accounts and access rights.

As part of Siemens constant development process for the Cloud Apps, we periodically release patches, updates and upgrades that remove new known vulnerabilities and increase the level of protection against threats. Patches and updates for the cloud-based applications are made available directly with deployment. Firmware updates for the connected devices are also made available and can be pushed to the devices remotely. This practice ensures that the firmware is up-to-date and secured, both on and off site.

Emergency Management

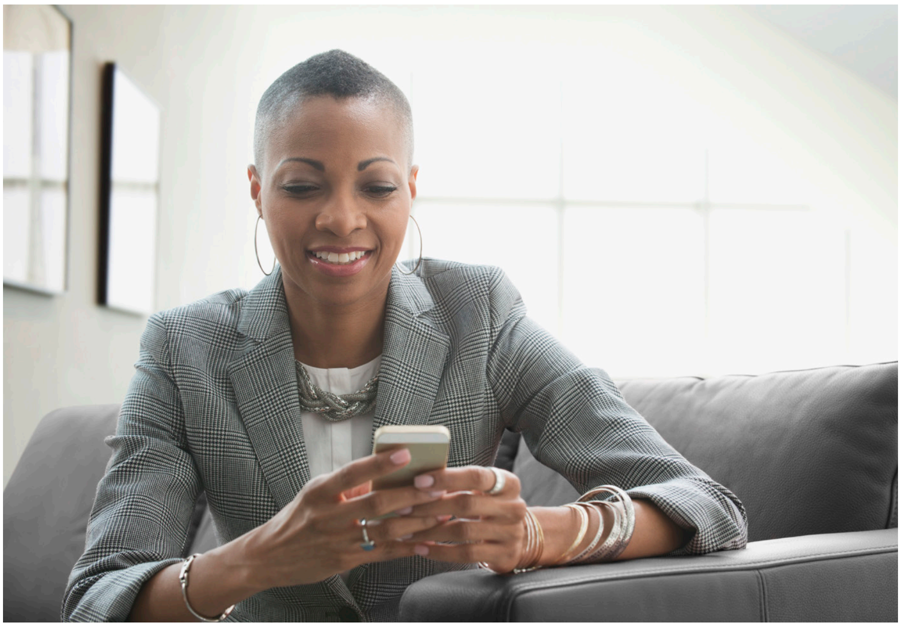
Siemens has processes in place for handling security incidents. In an event where a cybersecurity threat is suspected or found, immediately contact Siemens Computer Emergency Response Team for products (Product CERT) or your local Siemens customer service.

Siemens ProductCERT is a dedicated team of seasoned security experts that manages the receipt, investigation, internal coordination and public reporting of security issues related to Siemens products, solutions or services. ProductCERT cultivates strong and credible relationships with partners and security researchers around the globe to advance Siemens product security, to enable and support development of industry best practices, and, most importantly, to help Siemens customers manage security risks.

The team acts as the central contact point for security researchers, industry groups, government organizations and vendors to report potential Siemens product security vulnerabilities. This team will coordinate and maintain communication with the involved parties, internal and external, in order to appropriately respond to identified security issues. Security Advisories are released in order to inform customers about necessary steps to securely operate Siemens products and solutions.

Siemens CERT is a dedicated team of Security Engineers with the mission to secure the Siemens infrastructure. CERT monitors the current cyber threat landscape for Siemens and assesses its potential impact on the enterprise. Based on that know-how and the latest technological trends, CERT consults with the Information Technology department at Siemens to improve the enterprise IT Security. The team is responsible for coordinating the response to cybersecurity incidents within Siemens. To achieve its mission, CERT leverages the relationships with various internal and external stakeholders worldwide, such as CSIRT networks, technical communities and the security researcher communities. CERT is also recognized as a trusted research partner by academia and industry, with numerous projects and publications in its expert area.

Summary



As a market leader in building technologies and fire safety systems, Siemens understands the difficulties in meeting today’s cybersecurity challenges. In fact, we design our products with security in mind from day one. Our Cloud Apps are a case in point: their built-in cybersecurity measures will give you and your customers the peace of mind to use the apps to connect fire protection systems to the cloud. The Cloud Apps increase safety and business continuity by enabling issues with fire protection systems to be fixed as quickly and seamlessly as possible via the cloud. These apps are part of our holistic approach to helping digitalize the fire industry. Make the Cloud Apps a cornerstone of your ongoing digitalization efforts for you and your customers.

Cybersecurity Disclaimer

Siemens provides a portfolio of products, solutions, systems, and services that includes security functions that support the secure operation of plants, systems, machines, and networks. In the field of building technologies, this includes building automation and control, fire safety, and security management as well as physical security systems.

In order to protect plants, systems, machines, and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines, and networks, which should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g., firewalls and/or network segmentation) are in place. Additionally, Siemens guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit
https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security.html.

Siemens portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under
https://new.siemens.com/global/en/products/services/cert.html.

Published by
Siemens Switzerland Ltd.

Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
6300 Zug
Switzerland
Tel +41 58 724 24 24

For the U.S. published by
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

Article no. SI_0198_EN (status 2/2022)

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.