Building X
Cybersecurity

SIEMENS

BUILDING X CYBERSECURITY

Executive Summary

Building X is a versatile digital building platform that offers scalable solutions for digitizing, managing, and optimizing building operations and supports your journey towards smart buildings with a best-in-class user experience. Building X provides superior connectivity and breaks the data silos. Making data accessible to all stakeholders involved under one user interface, comprising all domains and aspects of building operations and management, and replacing numerous island solutions in an easy and productive way, is bringing you closer to your business goals.

The fact that Building X combines the physical and digital worlds in a single source of truth makes solid cybersecurity an essential element for trustworthiness of our solution. "Attacks always get better; they never get worse". At Siemens we believe it is important to look at cybersecurity holistically and proactively throughout the whole lifecycle of our products, solutions and services, to stay ahead of cyber attacks.

This paper explores Siemens' commitment to comprehensive cybersecurity. It explains how Building X achieves security by design and default, and how it is securely deployed and operated complying with the cybersecurity standards and best practices for cloud service providers and industrial automation and control systems.

Introduction

We live and work in an exciting era. It is one defined by the digitalisation of business and a transition to a sustainable, human-centric and resilient industry that contributes to society. Digitalisation 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 digitalisation 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 organisation.

At Siemens Smart Infrastructure, we believe security begins during product development.

We have adopted a 'think security' philosophy in the development of our Building X family of 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 on 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 consider four key factors that impact security strength – people, processes, technology and communication. In general:

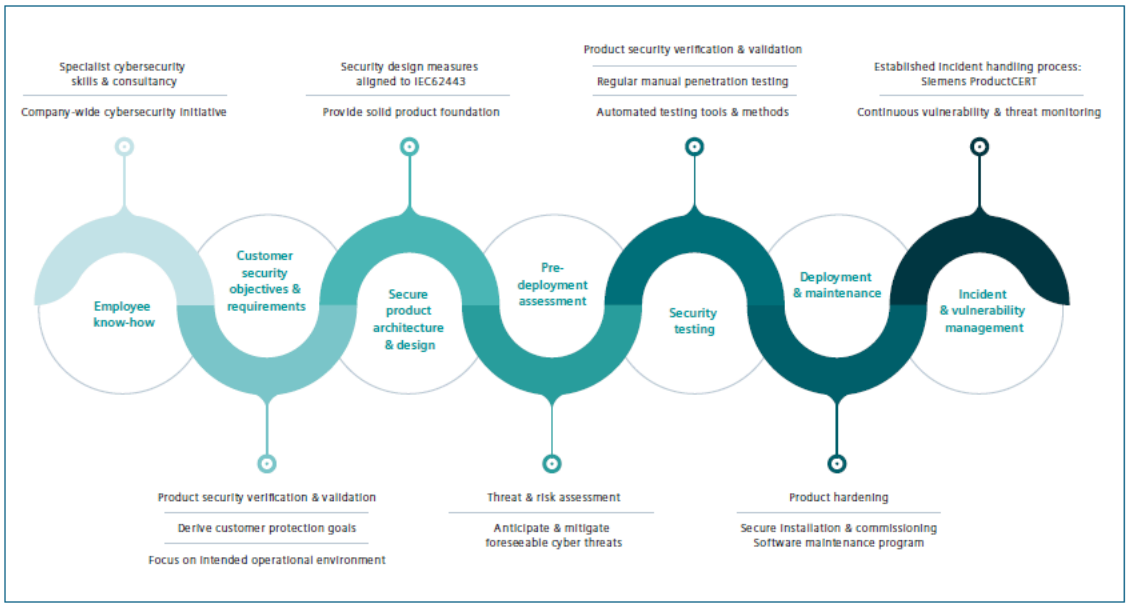
• **People** need a broad and lasting awareness of the importance of security, both physical security and cybersecurity.

•**Processes** that are actively applied are as important as technology in protecting organisations from cyber threats.

• **Technology** needs to be tested, vetted and matched with other suitable building blocks in order to secure an organisation's assets.

• **Communication** helps establish a culture of security.

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.



Siemens Cybersecurity Initiative Highlights

Security by design: Siemens' commitment to comprehensive cybersecurity

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 is essential that organisations like yours develop a fully comprehensive defense.

While the responsibility to secure your environment lies with your organisation, 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.

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, which calls for binding rules and standards to build trust in cybersecurity and further advance digitalisation.

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 in the process and is repeated as required to identify and mitigate risks appropriately.

In addition, regular product security testing is conducted by independent 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, most 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 is 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. During our development, 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 a high level of security when 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. 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, there should be a strict recommendation in place to demand the 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 is now a mandatory requirement.

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. It is 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 authorised users of a system to have the minimum necessary access – or privilege – 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 are less likely to occur. When properly applied, the principle of 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 has been compromised.

*J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," in Proceedings of the IEEE, vol. 63, no. 9, pp. 1278-1308, 1975

The Principle of Least Privilege 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 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 does not need administrative access should work with fewer privileges and limited scope whenever appropriate. It is also important that technical users have only the minimum privileges needed to access the resources they are working on and no 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.

The separation of duties principle

Another IT security concept that is closely related to the principle of least privilege is the separation of duties principle. This divides critical functions among different authorised users to minimise the risk of fraud and other abuses by employees or other authorised eople. It states that no user should be given enough privileges to misuse the system on their own. This separation of

duties can be enforced either by defining roles that cannot 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 authorised user, while the second person must be a different authorized user

As part of our holistic approach to cybersecurity, we use the Principle of Least Privilege 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.

Cybersecurity compliance

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 holistic approach that is driven by international compliance standards.

The ISO/IEC 27001:2022 certification provides our foundation by operating an Information Security Management System (ISMS) that enables us to apply a risk-based approach to manage, monitor, and improve cybersecurity within our organization among our product portfolio. Furthermore, as a cloud service provider for software-as-a-service offerings, the organization complies to the code of practice for information security controls relevant to cloud services as defined in ISO/IEC 27017:2015.

Another important standard 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 is aimed at plant operators, integrators and component manufacturers, and covers the urgent security-relevant aspects of industrial security.

Siemens Smart Infrastructure Buildings is certified according to IEC 62443-4-1 with maturity level 3. This certification is prerequisite to certifying separate products, i.e., achieving IEC 62443-4-2 product certification for Connect gateways.

Achieving security by design and default in Building X

Building X is designed and developed with security-by-design and security-by-default principles in mind.

Building X security by design: Adhering to Siemens' company-wide cybersecurity initiative, our experts ensure that Building X achieves security by design by infusing each phase of the system development lifecycle with security principles and best practices in alignment with applicable cybersecurity standards.

Building X security by default: We adopt and incorporate the highest appropriate level of security and data protection into the design of the product, functionalities, processes and operations and ensure that appropriate level of security is preconfigured and activated immediately once the system is put into use.

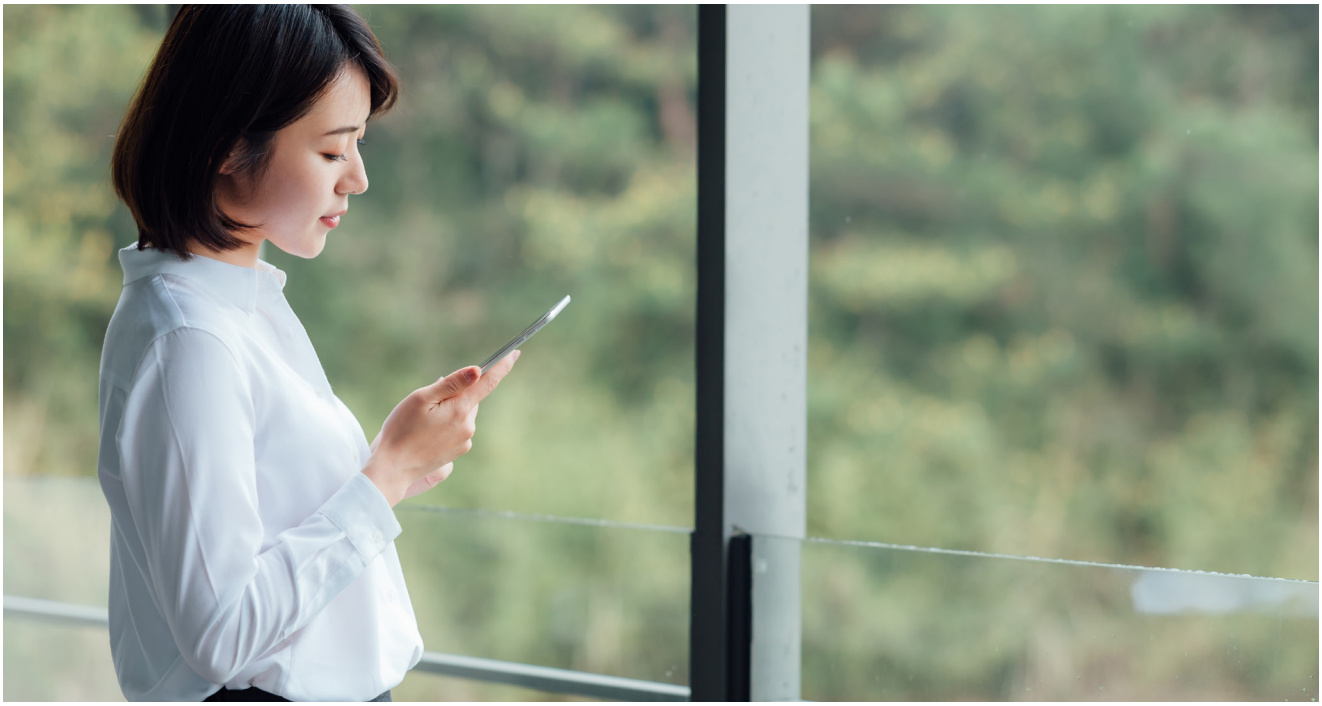
Achieving a desirable product and solution security level requires not only product-specific technical security capabilities but also suitable information security maturity at the organisation level as well as in the product development processes. In developing Building X, we follow our internal security policies, processes and procedures that are established by our company-wide information security management system in alignment with applicable international and national standards, such as ISO 27001, NIST CSF and BSI IT-Grundschutz. These established and implemented best practices help us continuously maintain and improve our general organisational security posture.

Furthermore, in alignment with the industrial cybersecurity standards IEC 62443, ISO/IEC 27017, and the charter of trust principles, we have incorporated holistic security thinking into our Building X development lifecycle. By applying the security controls, we embed cybersecurity measures into our products and solutions to reduce the risk of security problems. We are continuously looking for security improvements to further enhance Building X resilience against emerging cyber threats and attacks.

Building X cloud security

Cloud security is a shared responsibility between the cloud service providers and customers. Our Building X suite of cloud-based applications, offered as Software-as-a-Service (SaaS), reduces the security responsibility burden on our customers, so that they simply configure the provided security features by following clear instructions provided in the Building X cybersecurity guidelines.

Building X uses AWS (Amazon Web Services) to host its platform and application services. This provides, together with Siemens connect gateways, Siemens IoT devices and on-premises software products, an end-to-end solution to unlock new customer value. AWS provides a cloud infrastructure with hardware, software, or networking able to meet the requirements of the most security-sensitive organizations. Likewise, AWS is responsible for protecting the global infrastructure that runs all their services offered to customers. Building X uses the AWS security services including, but not limited to, AWS Key Management Service, AWS Secrets Manager, AWS Security Hub and AWS Config.



Access to resources is restricted by authentication followed by authorisation, an additional step to further protect important resources once users have provided authentic identification.

Building X implements the security principles of least privilege and separation of duties with role-based access control (RBAC), limiting a user's access to resources, applications and features.

Cryptography employed for securing data

Building X relies on advanced cryptographic technologies provided by AWS and Siemens to protect security and privacy of user and application data at rest and in transit.

Data-at-rest encryption: All data stored in the cloud is secured using AWS cryptographic services and tools, supporting among others, the state-of-the-art standard authenticated-encryption algorithms (e.g. AES_256_GCM). AWS cryptographic modules conform with the Federal Information Processing Standard (FIPS) 140-2.

Data-in-transit encryption: All data in transit (for example, communications to and from Building X cloud applications) is secured using Transport Layer Security (TLS) protocol (TLS 1.3 or TLS 1.2 configured with secure profiles for its cipher suite).

The underlying Public Key Infrastructure (PKI) includes the following Certification Authorities (CAs) for issuing digital certificates: Siemens CA (issued by QuoVadis), AWS CA, Comodo CA and Digicert CA. The state-of-the-art standard digital signature algorithms supported (e.g. RSA_2048/4096_SHA256).

PKI involves the management of digital certificates during their lifetime (issuance, distribution, storage and revocation). End point certificates are stored on AWS and managed by Siemens. For renewals, AWS notifies Siemens prior to certificate expiration.

Post-quantum cryptography: Siemens' researchers and experts in cryptography have been actively participating in the ongoing international research and standardisation projects in the area of post-quantum cryptography (PQC); in particular, the National Institute of Standards and Technology (NIST) standardisation of new quantum-secure algorithms for public-key encryption, key-establishment and digital signature.

While a cryptographically relevant quantum computer capable of breaking RSA (with a large module e.g. 2048 bits) does not yet exist, toward a longer-term security we are investigating these PQC algorithms including the AWS hybrid post-quantum TLS for their potential performance and compatibility impacts.

Building X cybersecurity deployment

We publish the Building X cybersecurity guide / application guide to support secure deployment of our Building X offerings. These guidelines describe how our systems, products and solutions need to be configured for secured operation in the intended environment. For example, configuration options include which settings to activate or deactivate, firewall configurations and the setting of access rights. The cybersecurity guidelines are maintained throughout the product's lifecycle.

As part of our Maintenance Program, we periodically release software updates that remove new known vulnerabilities and increase our Building X level of protection against emerging threats and attacks. Our documentation and customer service center holds all the latest information regarding our Building X offerings' cybersecurity.

In keeping with cybersecurity expectations, each cybersecurity-relevant feature undergoes threat and risk analysis, and Building X is submitted to regular penetration tests. We are able to refine our Building X protections as new security threats appear because we continuously enhance and evolve our products, solutions and services.

Security emergency management

For our offerings, we have incident and vulnerability handling processes in place in case that a security issue or vulnerability is detected.

Incident and vulnerability handling process: Our support mechanism for customer-reported security issues follows a four-step process that includes reporting, analysis, handling and disclosure. Vulnerabilities and/or incidents are submitted to our technical support team, which is supported by the global Siemens ProductCERT team that operates on a 24/7 basis. The necessary steps are taken to handle the situation and the incidents and remedies are disclosed.

Vulnerability management: This is our internal detection process for fine-tuning the security level of our products and solutions. Continuous threat monitoring enables us to detect and mitigate potential vulnerabilities in our products and solutions. Software components in our Building X systems are registered so that if any security vulnerabilities are found, the necessary remedies can be implemented and disclosed. Identified vulnerabilities are announced by the ProductCERT team via security advisories. You can subscribe to the ProductCERT security advisories at:

https://new.siemens.com/global/en/products/services/cert.html

Summary

As a market leader in building technologies, Siemens understands the challenges you face in meeting your cybersecurity needs in today's world. Our comprehensive security approach to the product lifecycle means our Building X suite of products is developed with your security in mind. We can refine our Building X protections as new security threats appear, because we continuously enhance and evolve our products, solutions and services.

Siemens has over 30 years of experience in the field of cybersecurity and have deliberately helped shape security in the industrial cyberspace. Ultimately, smart organisations make security one of the cornerstones of their businesses today.

You can rely on our experience and ingenuity to provide a solution that helps you protect what matters to you, something Siemens has been doing since 1851.

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 unauthorised 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 you 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