WHITE PAPER

Securing your business on the Internet of Things

Table of contents

An IoT security solution is an absolute essential to doing business in today's connected world. Without security, your business is vulnerable to hacks and data security breaches. Private information can become public and exploited, threatening the well-being and reputation of your company, your customers and business partners. With an IoT security solution, you can block hackers and their abhorrent practices to minimize risks and assure business continuity.

This paper introduces you to how Software AG robustly secures the Cumulocity IoT platform so it's a safe place for your IoT solutions. As an executive helping to select an IoT platform, you'll learn how:

- The platform was built from the start with security in mind—it's "carrier grade"
- Your data is safe in the cloud, on-premises and in edge solutions on our platform
- We work continuously, vigorously, to enhance platform security in a changing world

See how we keep IoT security simple for you while earning the highest grade from respected security firm SSL Labs.

Recap of Cumulocity IoT platform

Software AG's Cumulocity IoT platform is designed to give you complete business visibility and control of all the remote assets in your organization. These assets could be machines, individual sensors and valves in a production facility, environmental controls, robots or whole production lines.

Essentially if it can be measured or controlled electronically, then Cumulocity IoT can collate the data from it. You can connect and manage tens of thousands of devices to bring new insights into your operations, automate processes and improve efficiency. Cumulocity IoT enables you to rapidly build an IoT solution your company needs, not the one we think you need, with access to more than 100 device types, 300+ protocols, and a host of solution accelerators out of the box.

Cumulocity IoT is delivered as a cloud service, at the edge or on-premises (or any combination of these three) with device connectivity, management, data visualization and remote-control functions. You'll have access to a range of secure certified Application Programming Interfaces (APIs) and software libraries for extending functionality or interfacing Cumulocity IoT with your other IT assets, such as ERP or CRM systems.

Unlike other solutions that require a lot of painful development time and financial investment, our design philosophy keeps IoT simple for you. In fact, you can get value from the IoT immediately without having to worry about other aspects of your IT infrastructure, including hosting, networking, security, storage and backup. You can start using Cumulocity IoT for free, and experience for yourself how easy it is to start a new IoT journey using a wide range of customizable functionality out of the box.

First and foremost, security is a mindset

Every IoT platform vendor will tell you they take security seriously. However, few—if any—will be able to demonstrate it in the way we can at Software AG. Our global deployments in mission-critical systems across a wide range of vertical markets are testament to the trust that is placed in Cumulocity IoT. Bosch, Siemens, Dürr and Gardner Denver are among the companies that rely on our IoT platform.

Security has been at the heart of the Cumulocity IoT architecture development since 2010, when it was designed to meet carrier-grade requirements based on Nokia's security hardening guidelines. Our commitment to security is validated and independently audited by external security experts. Cumulocity IoT has passed security tests defined by the world's biggest carriers, including Deutsche Telekom, KPN and Telstra.

All data is transported using TLS 1.2, and the platform is graded A+, the highest possible, by respected security firm SSL Labs.

There is no single security component within Cumulocity IoT. Every component is developed from the ground up to meet the same stringent requirements. Security is an intrinsic part of the software development process, woven into every line of code. Whether you choose individual components of our platform to integrate with an existing implementation or the whole platform, you can rest assured Cumulocity IoT will not be a weak point.

There is no direct access to the internal code and functions of Cumulocity IoT. All interactions take place through a set of secure public-facing APIs, which expose every function of the platform in a way that can be used with your own applications or devices.

The Cloud Information Security Management System at Software AG has attained ISO 27001, ISO 27017 and ISO 27018 Information Security Management standards. This certifies our software development processes and management controls are sound and support the development of secure products. Software AG continuously invests in achieving new standards relevant to our sector.

Of course, security is not just about the code. It is also about attitude to risk. You have to respect that threats and bad actors exist; the enemy is always evolving and looking for new ways to cause disruption and harm. Vendors and enterprises alike fundamentally have to accept that an attack could happen.

Software AG's security philosophy means we never consider the job finished. Our IoT platform is enhanced continuously. Here are three ways we ensure every stage of the software development lifecycle meets the highest security standards:

- Everything we do related to security is driven by a security program based on the OpenSAMM (Open Software Assurance Maturity Model) framework. This model allows us to define and measure all security-related activities for the development, verification and deployment stages of Cumulocity IoT, ensuring good governance and continuous improvement.
- We have strongly defined security policies and standards for our product security compliance that are not just technical but aligned with both regulatory and individual industry needs.
- We work closely with security researchers and third-party vendors to understand emerging threats in market and supplement this with employee training to ensure these threats can be mitigated. The same parties also independently test Cumulocity IoT.

Our approach means Cumulocity IoT supports security standards and protocols that ensure communication with its APIs are secure and data cannot be compromised while stored or in transit between the cloud, devices and your local network. Our platform also integrates seamlessly with a range of security frameworks, which means it can conform to the standards, roles and access privileges already defined in your organization.

How Cumulocity IoT is secured

Security is woven into every component of Cumulocity IoT, so there is no module dedicated to security. This means all platform components are developed to the same standard with no dependency on other software for security. Cumulocity IoT is designed for highly secure IoT solutions without compromising performance in live production environments, where operations such as device management, storage and data ingestion could be impacted by a poor security implementation.

The security framework in Cumulocity IoT allows companies to meet the security, governance and regulatory requirements of their market (for example, HIPAA, PCI-DSS or safety critical standards such as NERCCIP and NIST). The flexibility of the security in Cumulocity IoT makes implementing the stringent controls straightforward, and we use extensive best practice guidance on the best way to achieve this.

Native multi-tenancy

Cumulocity IoT has native multi-tenancy, which means a single instance of Cumulocity IoT can securely serve multiple enterprise customers, without placing any data at risk of compromise. We achieve this by segregating data on at least two levels. Data can be physically segregated across different tenants for security and within a tenant using the role-based access controls. As an example, an industrial machine manufacturer would have its data fully isolated from its competitors and offer 100% segregation between the customers (factories) that use its machines. All data on Cumulocity IoT is isolated and protected, ensuring the privacy of all tenants and their customers.

Physical security

In IoT solutions, physical security includes unauthorized access to IoT devices, for example, to redirect or manipulate data from devices, read credentials from devices or change a device’s configuration.

We work with customers to provide best practice and guidance on protecting devices. The Cumulocity IoT architecture can also monitor for and report secure incidents, such as activation of tamper devices, which may indicate an attempt subjugate a device.

Our cloud hosting partners also assure servers, storage and network devices are physically secure. See page 6 for more details.

Network security

All data stays confidential and cannot be tampered with. Cumulocity IoT includes an end-to-end implementation of HTTPS from devices to applications and is transmitted using TLS 1.2 encryption technology that has been independently rated A+ by SSL Labs. Cumulocity IoT has been designed not to require specific ports or services from your infrastructure to be exposed to the public Internet, which can be a severe security risk, exploited by hackers. Additionally, all communication with Cumulocity IoT requires individual authentication and authorization, whether a device, application or user.

Application security

Cumulocity IoT follows standard practices for application-level hardening, such as making sure only properly upgraded operating systems and web servers are in use. Additional best practices make Cumulocity IoT secure by design.

All Cumulocity IoT functionality is coherently implemented with the same set of publicly documented, stateless REST APIs. This means that none of the popular “session stealing” techniques will work with Cumulocity IoT.

Cumulocity IoT does not use a SQL database for IoT data storage and is not based on a scripting language. This means that socalled “injection attacks” will not work with Cumulocity IoT.

Devices are treated like any client application connecting to the platform via HTTP or MQTT secured by TLS; this negates popular device attacks. Devices are individually connected with Cumulocity IoT's device registration feature. If a device is stolen or tampered with, it can be individually disconnected from Cumulocity IoT.

Access control

Cumulocity IoT uses a standard authentication and authorization process based on realms, users, user groups and authorities with a new realm created for each tenant to store the users of that tenant. This realm is fully isolated from other tenants, and administrators are appointed that assign permissions through their own administration application.

Permissions and roles for devices and groups of devices can also be created at very granular levels and custom configurations defined to meet the needs of your organization.

When a security event occurs, whether at an application level or on the network, Cumulocity IoT enables applications and agents to write audit logs, which are persistently stored and cannot be externally modified after being written.

Cumulocity IoT also writes its own audit records related to login and device control operations. Administrators are also alerted to security events as they occur so remedial action can be taken.

In addition, the security model in Cumulocity IoT can be extended by third parties, such as those partners in the Software AG IoT ecosystem, offering additional capabilities, such as full public key infrastructure, intrusion detection and prevention solutions.

Security and our cloud hosting partners

Making sure Cumulocity IoT is secure doesn't stop at software design and development. Our cloud hosting partners play a critical role. They help ensure the resilience and performance of Cumulocity IoT meets the expectations of any missioncritical system and that the servers, storage and network devices are physically secure.

We have a range of strategic hosting partner options. All Cumulocity IoT Standard Tenant accounts are hosted on Amazon Web Services. AWS has been certified according to ISO 27001 and PCI DSS as well as other security standards, features extensive physical security measures and is independently audited.

Our hosting partners are chosen to ensure customers receive the best possible performance from their implementation of Cumulocity IoT in any location. Not only do the data centers have the capacity and redundancy to easily cope with managing tens of thousands of devices, their locations are carefully selected to ensure the best bandwidth and low-latency connections.

Summary

Our goal is to offer you the most secure, flexible and feature-rich IoT platform on the market. From manufacturing to telecommunications, leading enterprises are innovating on Cumulocity IoT. They're quickly building and scaling solutions that connect their devices to automate operations, get time-critical insights and launch new business models with the peace of mind that Software AG is securing Cumulocity IoT to the highest standards.

Take the next step

Let's turn the IoT into your platform for growth and innovation. To learn more, contact your local Software AG representative and visit **www.softwareag.com/iot**

ABOUT SOFTWARE AG

Software AG simplifies the connected world. Founded in 1969, it helps deliver the experiences that employees, partners and customers now expect. Its technology creates the digital backbone that integrates applications, devices, data and clouds; empowers streamlined processes; and connects "things" like sensors, devices and machines. It helps 10,000+ organizations to become a truly connected enterprise and make smarter decisions, faster. The company has more than 5,000 employees across more than 70 countries and annual revenue of over €830 million.

Learn more at **www.SoftwareAG.com**. Follow us on **LinkedIn** and **Twitter**.

software AG