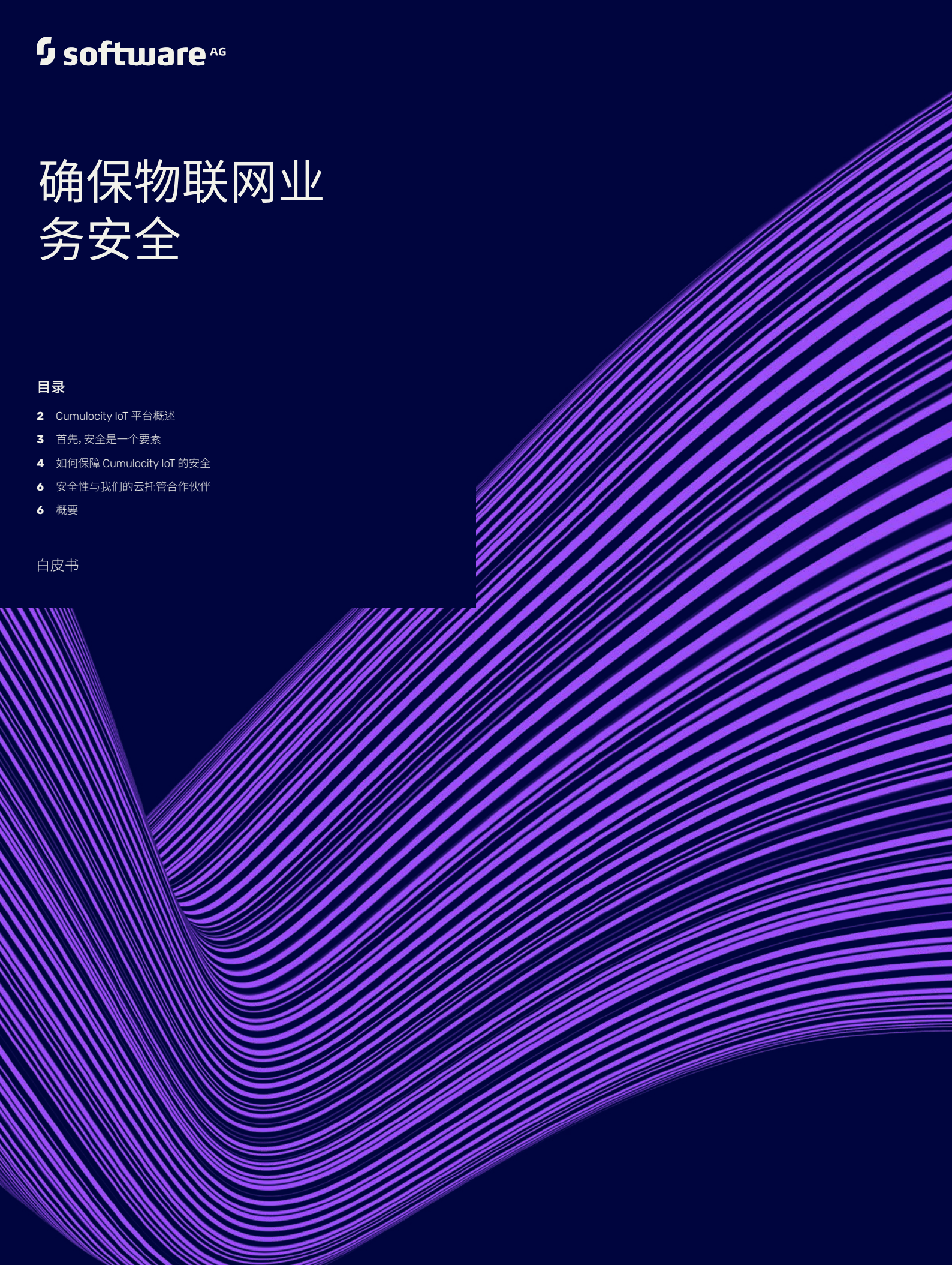
确保物联网业务安全

目录

白皮书



物联网安全解决方案是在当今互联世界开展业务的绝对必要条件。如果没有安全保障，您的企业很容易受到黑客攻击和数据安全漏洞的袭击。隐私信息可能被公开和利用，威胁到公司、客户和业务伙伴的利益和声誉。通过物联网安全解决方案，您可以阻止黑客及其恶劣行为，从而将风险降至最低，并确保业务连续性。

本文向您介绍 Software AG 如何确保 Cumulocity IoT 平台的安全性，使其成为物联网解决方案的安全场所。作为一名物联网平台选型的高管，您将了解到：

- 这个平台从一开始就考虑到安全，安全性达到“运营商级别”的
- 您的数据在云中、本地和边缘等解决方案中都是很安全
- 我们不断地努力工作，在持续变化的世界中加强平台安全

了解我们如何为您提供简易的物联网安全性，同时赢得备受认可的安全公司 SSL 实验室的最高评级。

Cumulocity IoT 平台概述

Software AG 的 Cumulocity IoT 平台旨在为您提供完整的业务可视性，并帮助您掌控组织中所有远程资产。这些资产包括机器、生产设施中的单个传感器和阀门、环境控制器、机器人或整个生产线。

从本质上说，如果某个事物可以通过电子方式测量或控制，那么 Cumulocity IoT 就可以从中采集数据。您可以连接和管理数以万计的设备，为您的操作带来新的见解，自动化流程并提高效率。Cumulocity IoT 使您能够快速构建公司所需的物联网解决方案，而不是我们认为您需要的解决方案，可以访问 100 多种设备类型、300 多种协议和大量现成的解决方案加速器。

Cumulocity IoT 可提供云服务、在边缘或本地（或这三者的任意组合）等部署方式，具有设备连接、管理、数据可视化和远程控制功能。您可以通过访问一系列经安全认证的应用程序编程接口 (API) 和软件库，以扩展功能或将 Cumulocity IoT 与其他 IT 资产（如 ERP 或 CRM 系统）连接起来。

与其他需要大量时间痛苦开发和经济投入的解决方案不同，我们的设计理念使物联网对您来说非常简单。事实上，您可以立即从物联网中获得价值，而不必担心 IT 基础设施的方方面面，包括托管、网络、安全、存储和备份。您可以开始免费试用 Cumulocity IoT，体验如何利用开箱即用的丰富的定制功能，轻松地开始新的物联网旅程。

2

首先，安全是一个要素

每个物联网平台供应商都会告诉您，他们非常重视安全问题。然而，很少有人能像我们 Software AG 那样印证自己的能力。我们全球，各个垂直市场的关键任务系统的成功案例，证明了客户对 Cumulocity IoT 的信任。博世、西门子、Dürr 和 Gardner Denver 都依赖于我们的物联网平台。

自 2010 年以来，安全性一直是 Cumulocity IoT 基础架构开发的核心，当时它的设计是为了满足运营商级别的要求（基于诺基亚的安全强化准则）。我们对安全的承诺得到了外部安全专家验证和独立审查。Cumulocity IoT 已经通过了包括德国电信、KPN 和澳大利亚电信在内的世界最大运营商的安全测试。

所有数据都采用 TLS 1.2 进行传输，该平台被权威的安全公司 SSL 实验室评为 A+ 最高级别。

Cumulocity IoT 中没有单一的安全组件。每个组件都是从头开始开发的，以满足同样严格的要求。安全性是软件开发过程中固有部分，融入到每一行代码中。无论您是选择将我们平台的单个组件与现有实施项目进行集成，还是与整个平台集成，您都可以放心 Cumulocity IoT 不会是脆弱环节。

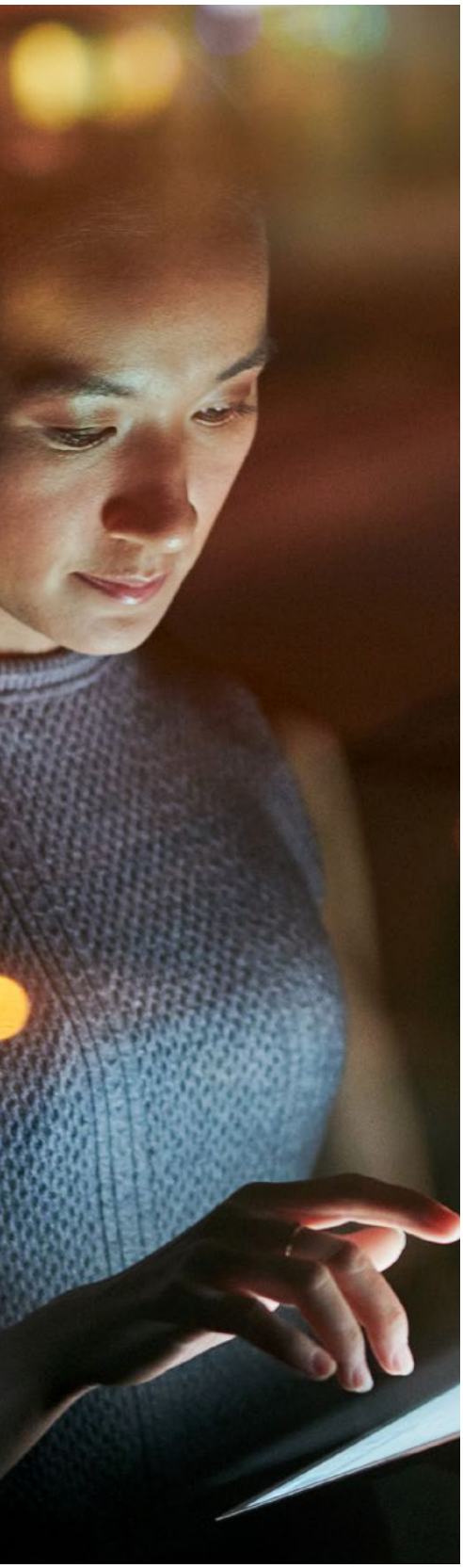
Cumulocity IoT 的内部代码和功能无法直接访问。所有交互都通过一组安全的、面向公众的 API 进行，这些 API 可以与您自己的应用程序或设备一起使用，以此展现平台的每项功能。

Software AG 的云信息安全管理系统已达到 ISO 27001、ISO 27017 和 ISO 27018 信息安全管理标准。这证明我们的软件开发流程和管理控制是健全的，并支持安全的产品开发。Software AG 不断进行相关投入，以满足与我们行业相关的新标准。

当然，安全不仅仅涉及代码。这也关乎对风险的态度。您必须尊重这一事实：威胁和不良行为者总是存在；敌人一直在进化，寻找新的方法来破坏和入侵您的系统。供应商和企业都必须从根本上接受这样一个事实：攻击可能随时发生。

Software AG 的安全理念意味着我们从来不对安全问题掉以轻心。我们的物联网平台一直在不断完善中。以下是确保软件开发生命周期的每个阶段都符合最高安全标准的三种方法：

- 我们所做的一切与安全相关的工作均由基于 OpenSAMM (Open Software Assurance Maturity Model) 框架的安全程序驱动。该模型使我们能够定义和衡量 Cumulocity IoT 开发、验证和部署阶段的所有安全相关活动，确保良好管理和持续改进。
- 我们为产品安全合规性制定了严格的安全政策和标准，这些政策和标准不仅关乎技术，而且符合监管并满足特殊行业的需求。
- 我们与安全研究人员和第三方供应商密切合作，了解市场中出现的威胁，并通过对员工进行培训以确保这些威胁能够得到有效的防治。相同机构还对 Cumulocity IoT 进行了单独测试。



我们的方法意味着 Cumulocity IoT 支持安全标准和协议，可确保与 API 的通信安全，并且数据在云、设备和本地网络之间存储或传输时不会受到损害。我们的平台还与一系列安全框架无缝集成，这意味着它可以符合组织中已定义的标准、角色和访问权限。

如何保障 Cumulocity IoT 的安全

Cumulocity IoT 的每个组成部分都融入了安全，因此没有专门用于安全的模块。这意味着所有平台组件都按照相同的标准开发，不依赖其他软件来确保安全性。Cumulocity IoT 是为高度安全的物联网解决方案而设计的，不会影响现场生产环境中的性能，在现场生产环境中，设备管理、存储和数据提取等操作可能会受到较差的安全实施不佳的影响。

Cumulocity IoT 的安全框架有助于公司满足其市场的安全、治理和监管要求（例如 HIPAA、PCI-DSS 或 NERC-CIP 和 NIST 等安全关键标准）。Cumulocity IoT 安全的灵活性使得实施严格的控制措施变得简单直接，我们以最佳方式运用广泛的最佳实践指导，以实现这一点。

原生支持多租户模式

Cumulocity IoT 具有多租户模式，这意味着 Cumulocity IoT 的单个实例可以安全地服务于多个企业客户，而不会将任何数据置于泄露风险之中。我们通过在至少两个层次上分离数据来实现这一点。数据可以在不同租户之间实现物理隔离，以确保安全性，并在租户内部使用基于角色的访问控制。例如，工业机器制造商将其数据与其竞争对手完全隔离，并在使用其机器的客户（工厂）之间实现 100% 的隔离。Cumulocity IoT 上的所有数据都被隔离和保护，确保所有租户及其客户的隐私。

物理安全

在物联网解决方案中，物理安全包括对物联网设备的未经授权访问，例如，重定向或操作来自设备的数据，读取来自设备的身份凭证或更改设备的配置。

我们与客户合作，提供保护设备的最佳实践和指导。Cumulocity IoT 基础架构还可以监测和报告安全事件，例如防篡改设备激活状态，这可能表示有人试图控制设备。

我们的云托管合作伙伴还能确保服务器、存储器和网络设备的物理安全。请参见第 6 页了解详细信息。

网络安全

所有数据保密，不可篡改。Cumulocity IoT 包括从设备到应用程序的端到端 HTTPS 实现，并使用 SSL 实验室独立评定为 A+ 的 TLS 1.2 加密技术进行传输。Cumulocity IoT 的设计不要求您的基础设施的特定端口或服务暴露于公共互联网，这是可能会被黑客利用的严重安全风险。此外，所有与 Cumulocity IoT 的通信都需要单独的身份验证和授权，无论是设备、应用程序还是用户。

应用程序安全

Cumulocity IoT 遵循应用程序级强化的标准实践，例如确保仅使用正确升级的操作系统和 Web 服务器。其他的最佳实践通过设计让 Cumulocity IoT 变得更安全。

所有 Cumulocity IoT 功能都使用同一套公开的、无状态的 REST API 实现的。这意味着，流行的“会话窃取”技术对 Cumulocity IoT 均行不通。

Cumulocity IoT 不使用 SQL 数据库存储物联网数据，也不基于脚本语言。这意味着所谓的“注入式攻击”对 Cumulocity IoT 无效。

设备是通过 TLS 保护的 HTTP 或 MQTT协议连接到平台的；这让流行的设备攻击失效。设备通过 Cumulocity IoT 的设备注册功能单独连接。如果设备被盗或被篡改，则可以单独断开与 Cumulocity IoT 的连接。

访问控制

Cumulocity IoT 使用基于区域、用户、用户组和权限的标准身份验证和授权流程，为每个租户创建一个新的区域来存储该租户的用户。该区域与其他租户完全隔离，并指定管理员，他们通过自己的管理应用程序分配权限。还可以在非常精细的级别创建设备和设备组的权限和角色，并设定自定义配置，以满足组织的需求。

在发生安全事件时，无论是在应用程序级别还是在网络上，Cumulocity IoT 都允许应用程序和代理写入审计日志，这些日志被永久存储，并且在写入后不能在外部修改。Cumulocity IoT 还编写平台与登录和设备控制操作相关的审查记录。在发生安全事件时，管理员也会收到提醒，以便采取补救措施。

此外，Cumulocity IoT 中的安全模型可由第三方扩展，如 Software AG 物联网生态系统中的合作伙伴，提供额外的功能，如完整的公钥基础设施、入侵检测和预防性解决方案。

安全性与我们的云托管合作伙伴

确保 Cumulocity IoT 的安全性不仅仅停留在软件设计和开发上。我们的云托管合作伙伴也发挥着关键作用。它们有助于确保 Cumulocity IoT 的弹性和性能能够满足任何关键任务系统的期望，并确保服务器、存储器和网络设备的物理安全。我们有一系列战略托管合作伙伴选项。所有 Cumulocity IoT 标准租户都托管在亚马逊网络服务上。亚马逊网络服务已根据 ISO 27001 和 PCI DSS 以及其他安全标准进行认证，具有广泛的物理安全措施，并经过独立审查。

选择我们的托管合作伙伴以确保客户在任何地点实施 Cumulocity IoT 时都能获得最佳性能。数据中心不仅有强大充足的运算和存储能力，可以轻松管理成千上万的设备，而且其位置经过精心选择，以确保最佳带宽和低延迟连接。

总结

我们的目标是为您提供市场上最安全、最灵活、功能最丰富的物联网平台。从制造业到电信业，龙头企业都在 Cumulocity IoT 上进行创新。他们正在快速构建和扩展解决方案，将他们的设备连接起来，以实现自动化操作，获得实时的洞察力，从容推出新的商业模式，同时，Software AG 正在确保 Cumulocity IoT 达到最高标准。

进入下一步

让我们将物联网变成您成长和创新的平台。要了解更多信息，请联系您当地的 Software AG 客服并访问网站 www.softwareag.com/iot

wp-cumulocity-iot-security-zh

software AG