SAGE® 安全性

您的数据资料是您所拥有的最有价值的资产之一，而我们的首要目标之一是使用一些最先进的安全系统来对其进行保护。

Armstrong®提供的SAGE®安全性

安全的托管环境

合作伙伴

为了提供高级别的基础设施安全性，Armstrong® 选用Amazon Web Services (AWS) 来托管SAGE®。AWS具有最高级别的云安全性，有关AWS安全性的更多信息，请参见：https://aws.amazon.com/security/

AWS遵守众多全球合规性计划，有关 AWS 合规性计划的更多信息，请参见：

https://aws.amazon.com/compliance/programs/

除了AWS，Armstrong® 还与Pivotal Web Services (PWS)和MongoDB Atlas合作。这些提供商在AWS的基础上构建服务，有关这些提供商的更多安全性信息，请参见：

https://run.pivotal.io/policies/gdpr-and-data-security-faqs/
https://www.mongodb.com/cloud/trust

物理安全性

物理和环境安全性由AWS 数据中心实体建筑提供。AWS 物理和环境安全性的详细信息，请参见：
https://aws.amazon.com/compliance/data-center/controls/
https://aws.amazon.com/compliance/data-center/infrastructure-layer/

虚拟化安全性

SAGE® 托管遵循虚拟化安全性方面的行业最佳实践。虚拟化解决方案的固有特性是能够随时迁移实时环境中的服务器和数据存储。系统无需脱机，也能够向服务器分配额外的资源。虚拟机监视器在虚拟机之间和数据存储之间提供逻辑保护分段。为Armstrong® 配备了使用安全专用VLAN的专用网络。此外，虚拟防火墙还可以保护和限制网络之间的数据传输。多个防火墙和网关可监控和保护贯穿云基础架构的流量。

操作系统和应用程序修补

PWS定期自动处理应用服务器的系统升级。了解更多信息，请参见：
https://community.pivotal.io/s/article/PWS-Upgrade-Frequency

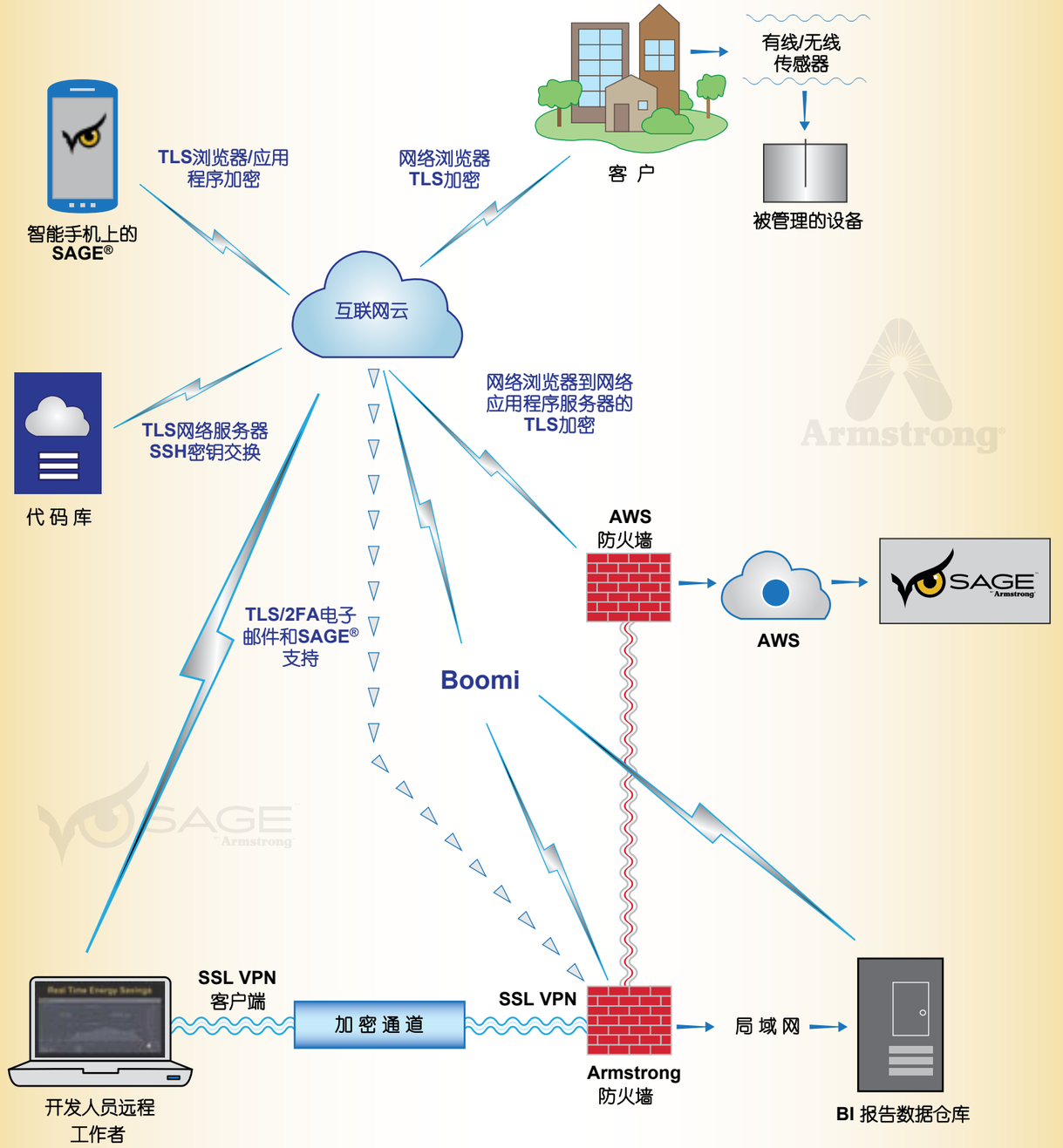
MongoDB Atlas 会定期自动更新操作系统软件和数据库软件的维护版本。如果 数据库软件的主要/次要版本可用时，则Armstrong®会得到通知。在测试环境中应用和观测更新。一旦功能性和安全性得到验证，更新就会应用到生产环境中。

远程连接

Armstrong®开发人员不会直接访问应用程序和数据库服务器。使用PWS 或 MongoDB Atlas提供的工具进行更新和配置更改。这些工具仅供必要人员使用，并由强密码和 2FA 保护。所有通讯都是加密的。

数据库访问受强密码和加密保护。

使用 SAGE®，即可安全存储您的数据和所有数据事务。



使用 SAGE®，即可安全存储您的数据和所有数据事务。

安全的托管环境

最佳编码实践

SAGE®是一款世界顶级公用系统管理软件，采用应用程序开发安全性的最佳实践开发而成。该应用程序使用简单高效的代码开发，降低了出错的可能性。它能对来自可信数据源的数据执行输入验证，其他输入则被删除。利用深度防御原理开发的SAGE®软件具有固有的整体安全性。

SAGE® SDLC

作为软件开发生命周期的一部分，Armstrong® 应用程序开发团队通过综合使用 Waterfall 和 Agile 编程实践来创建软件解决方案。在设计、编码和测试阶段定期召开开发人员会议，确保在团队的努力下发现并减少安全性问题。对安全代码和报告的错误进行迭代审查，可确保及时解决应用程序漏洞。

编码框架

采用经过行业测试的通用编码框架和库来增强应用程序的可靠性和完整性。该框架提供了一个全面的编程和配置模型。SAGE®的开发使用安全性框架来集成身份验证和授权。

访问控制

Armstrong®应用程序的访问控制涉及使用最小权限来限制访问，只有已识别的监控和管理用户才有访问权限。每个用户都有登录SAGE®应用程序的唯一凭据。使用授权模块中配置的访问列表强制执行安全应用程序问。

代码库

必须保护自定义应用程序的源代码不被篡改。获得专利的SAGE®监控系统将客户端，服务器和移动应用程序的源代码保存在安全的源代码库中。云格式允许利用SSH访问和公共密钥非对称加密技术进行安全的开发协作和代码存储。

检测

该安全框架可以抵御常见的网络应用程序攻击，例如CSRF攻击、XSS攻击和注入攻击。开发人员知道采用安全编码实践可以有效防止后门漏洞和程序特征更改。

移动应用程序开发

移动应用程序采用与网络应用程序相同的身份验证、授权和加密机制。iCloud钥匙串用于存储SAGE®用户的登录凭据。

使用 SAGE®，即可安全存储您的数据和所有数据事务。

安全的运行环境

身份验证

集中式目录身份验证用于访问SAGE®环境。身份验证是环境安全不可或缺的一部分。密码作为目录中的静态数据进行加密。

传输安全（网络）

SAGE® 应用程序的前端网络访问依赖于SSL/TLS 提供的安全性。公钥加密（PKI）算法提供128位（或更高）的加密保护 。身份验证服务器流量使用受 TLS 保护的事务进行加密。

客户数据

能源管理系统创建的客户数据不被视为敏感数据。实时数据由任意数据组成，例如管线压力、温度和声学数据等。存储的数据由聚合的设备信息组成。该解决方案的优势来自对数据进行的计算，以及通过分析和趋势预测实现的成本节约。

网络和应用程序安全性

代理软件和SAGE®之间的实时事务使用SSL 加密协议进行加密。向SAGE® 发送实时读数需要用户名、密码和唯一令牌。此外，收到读数后会进行验证，如果验证失败，则读数会被删除。

在客户浏览器和SAGE® 网络服务器之间提供网络应用程序安全性。开发人员管理SAGE®服务器的事务时同样使用网络浏览器安全性进行身份验证、授权和加密。有关更多信息，请参见图 1。

恶意软件

所有SAGE®服务器都运行Linux 。软件仅从受信任和经过验证的存储库中安装，并通过安全补丁随时更新。

安全性审核

关于任何系统访问和资产修改的日志条目都会受到维护。审查对技术基础设施的威胁警报。安全性分析涵盖所有逻辑技术层，包括物理安全性、应用程序、操作系统、网络传输、数据存储和访问控制，以确保深度防御。内部审核通过外部第三方审核和渗透测试进行验证，符合行业标准安全法规（PCI和HIPAA）的要求。

使用 SAGE®，即可安全存储您的数据和所有数据事务。

业务连续性和灾难恢复

数据备份

SAGE®数据库持续备份。快照每六小时拍摄一次，并保留两天。每日快照保留七天。每周快照保留四周。每月快照保留 13个月。

二级数据中心

尽管SAGE®的主要数据中心位于美国东部（弗吉尼亚州），但服务器和数据可能会根据具体情况位于其他位置。出于冗余、可用性或性能原因考虑，可能会复制数据。自然灾害或长期环境故障可能会迫使数据复制到二级数据中心站点。复制过程通过连接这些位置的专用网络进行加密。有关AWS区域和可用性区域的信息，请访问：
https://aws.amazon.com/about-aws/global-infrastructure/

连接性

水、电、电信和互联网连接均设计有冗余，因此我们可以在紧急情况下维持连续运行。电力系统被设计成完全冗余，因此在发生电力中断的情况下，可以启用不间断电源装置来执行某些功能，同时发电机可以为整个设施提供备用电力。人员和系统监测和控制温度和湿度以防止过热，进一步减少可能的服务中断。

SAGE®支持

安装

授权代表负责安装用于监控蒸汽和热水组件的SAGE®解决方案。Armstrong®或我们的客户均可能需要代理安装，这将具体取决于商定的部署拓扑。客户必须在其防火墙和安全设备上配置适当的连接（NAT 和访问列表）。托管SAGE®基础设施是Armstrong®的特权和责任。

应用支持

对 SAGE® 应用方面的支持由 Armstrong® 的开发人员和工程师提供。首先应联系SAGE® 支持部门，我们可以通过电子邮件和语音服务为您提供帮助。联系信息，请参见：
https://www.armstronginternational.com/products-systems/sage%E2%84%A2-armstrong.

应急响应

服务器和应用程序的可用性受到全天候监控。我们已经设置了应用程序可用性警报，以便在操作系统或应用程序出现故障时联系Armstrong®的工作人员。CPU、内存、网络和磁盘利用率等资源会被记录下来并绘制成图表，以便进行分析和故障排除。预计的增长将通过服务器的资源升级来实现。

如果发生安全事故或数据泄露，Armstrong®将立即通知客户。将定期提供及时更新，直到达成解决方案。任何计划停机时间都将根据提交给Armstrong®的组织联系人名单传达给客户。

使用 SAGE®，即可安全存储您的数据和所有数据事务。

Armstrong International
蒸汽、空气和热水智能解决方案
北美•拉丁美洲•印度•欧洲/中东/非洲•中国•环太平洋地区

armstronginternational.com