增强的防火墙集成

自动保护所有网络连接设备的安全

在超连接的企业中，从简单的*IoT*设备到复杂的数百万美元的系统都已连接到网络。庞大的网络连接设备影响并增强了我们每天与之互动的一切。

但是，创新的扩散正在如此大规模地发生，以至于传统的*IT*和安全实践根本无法跟上。每个连接的设备都代表着企业网络中潜在的漏洞点，而要降低风险，则需要闭环安全系统，该系统允许通过已就位的防火墙系统自动生成并实施策略。

已经拥有的防火墙的闭环安全性

在Ordr，我们消除了识别、分类、调节和保护数量庞大且不断增长的网络连接设备的复杂性和不确定性。我们提供了一个无代理平台，该平台专门用于调节并保护整个企业中的连接设备；该平台提供即时、细粒度的设备可见性，并使组织能够通过优雅、简单、直观的界面，快速、自动地识别、分类、调节并保护所有与网络连接的设备。而且该界面与现有的同类最佳防火墙解决方案无缝集成，只需单击几下即可降低风险。

我们知道，随着设备的添加，移动和更改会定期发生，而强大的安全策略并不是“一劳永逸”的，并且漏洞攻击的威胁会定期且持续地发生。 Ordr系统控制引擎（SCE）连续不断地监视整个网络的活动，立即识别和分类任何新设备或设备行为，评估风险级别并实时更新可视仪表板。如您所见， Ordr从不休眠。

以四种方式通过最佳防火墙平台实施增强的安全管理

区域分割

自动独立设备组用以调节网络区域之间的通信流。

(防止工业自动化设备访问internet。)

端口分段

利用系统的大量设备智能来管理和限制设备的特定端口使用授权。

(即，仅允许IP安全摄像机向上访问内部监控系统。)

设备标签分段

创建设备白名单以授权特定设备类型之间的流，并创建设备黑名单以阻止设备之间的所有不应有流。

(即，仅允许图像服务器访问装有Windows XP的X光机，而不允许受感染的笔记本电脑传播恶意软件。)

协议分段

对所有网络流量进行深入的数据包检查，可以授权专有设备协议，同时阻止可能损坏的通信协议。

(即，任何设备都无法“登录”到任何其他设备或“ftp”来传输大量数据。)

使您的整个基础架构更安全、更高效、更贴合利益

识别和分类连接到网络的所有设备

即插即用的配置和直观的界面意味着Ordr SCE会在安装后的几分钟内立即自动开始查找，识别和分类所有设备。该平台可发现详细的设备信息，包括制造商、型号、序列号、操作系统、软件版本以及许多其他数据点。该界面以图形方式显示此全面清单，从而使监视和控制一目了然。重要的是，该平台可自动并立即识别每个设备的漏洞和威胁，并提供可操作的风险评分，以便IT部门可以快速找到，确定优先级并纠正所有有风险设备的安全缺陷。

大数据分析可实现令人难以置信的精细化设备智能

Ordr SCE监视每个设备会话流，并为每个设备创建行为基线，并利用复杂的AI自动将异常行为标记为该设备类型。另外，此流映射使管理员可以快速轻松地识别可能存在问题或可能代表恶意通信意图的设备间关系及其对话映射。通过详细处理大量数据，机构可以显着提高单个设备的利用率，从而对计划、预算、购买和放置产生积极影响。

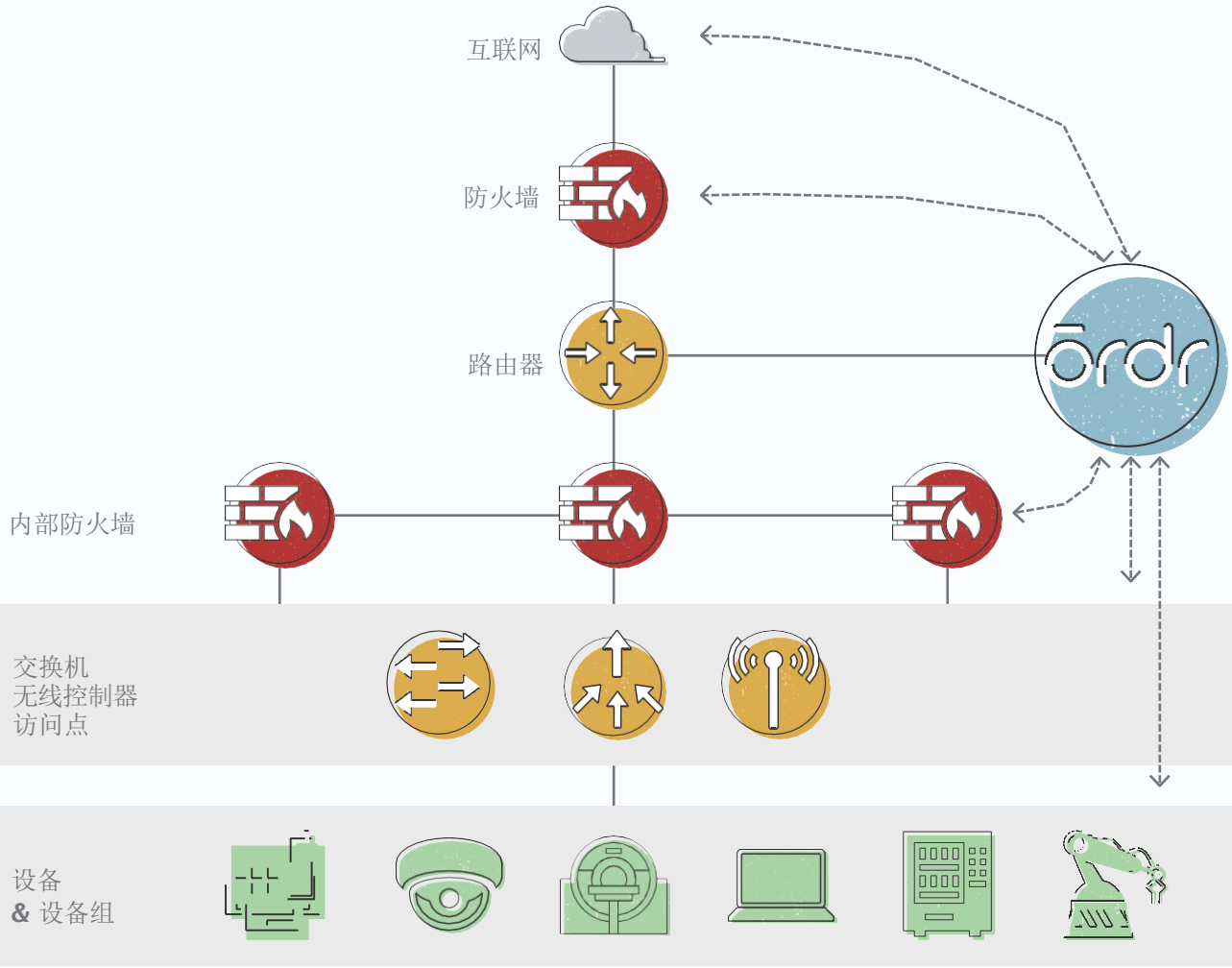
大量智能功能，只需单击几下鼠标，即可实现前所未有的设备级安全性

凭借Ordr SCE提供的超人可视性和知识，实现巨大的风险和漏洞缓解非常简单。立即识别并隔离受到安全事件危害的所有设备，并从单个窗格中快速修复威胁。实施微细分策略，以使用独特的保护策略准确隔离每个设备或设备组，以提供一种快速、简单而有效的方法来保护所有有风险的设备并防止未经授权的设备流关系。

利用您现有的网络基础设施来实现设备的安全性

Ordr SCE将无数的设备和应用程序智能与庞大且不断增长的网络基础架构设备专业知识库相结合，可自动实施这些精确控制，以缓解所有安全漏洞，甚至包括横向的内部攻击。该系统提供详细的CLI命令，以通过现有的网络交换机、无线控制器、访问点和防火墙来制定新的、更复杂的安全策略管理域。

防火墙架构



达到可见性、情报能力和安全性的新水平

Ordr是第一家也是唯一一家简单的并可以自动识别、分类、监管和保护所有规模企业中的网络连接设备的平台。借助Ordr SCE的强大功能，我们可以减少这种日益增长的智能设备所代表的复杂性和忧虑，并且该平台与现有的同类最佳防火墙解决方案无缝集成，从而只需单击几下即可缓解潜在的风险。减少复杂性和焦虑感是我们所有人都可以体会的。

但是，不要仅听我们的一面之词。让Ordr向您展示，今天它如何在您的环境中工作，明天您如何更轻松。

ōrdr

take control.

info@ordr.net
www.ordr.net

2445 Augustine Drive Suite 601
Santa Clara, CA 95054