白皮书
物联网

开发物联网解决方案

英特尔® 产品、解决方案和服务正助力打造安全、无缝的物联网（IoT）解决方案。

简介

世界正在经历一场剧烈的变革，孤立的系统将迅速转变为互联网连接的“事物”，它们无处不在，所产生的数据能够通过分析而提取出有价值的信息。这便是我们通常所说的物联网（IoT），这种新事物将丰富我们的日常生活，提高企业生产效率，改善政府办公效率等等。

英特尔正与多家解决方案提供商共同合作，面向广泛组织和企业开发 IoT 解决方案，包括工业、零售业、汽车行业、能源和医疗保健行业等。这些解决方案能够针对在设备和云之间移动的数据（始终安全、可管理并易于使用），运行分析软件和实施服务，从而产生有价值的信息。

推动业务变革

无论是用户可穿戴设备，是交通工具，还是工厂控制器，人们都希望能够快速、无缝地连接至互联网。本文解释了英特尔® 产品和技术可如何通过为开发端到端 IoT 解决方案的庞大生态系统提供基本构建模块而帮助这一切成为现实。

实现 “从事物到云” 创新的构建模块

IoT 的愿景是通过支持全球数十亿系统在云端共享和分析数据，创造各种形式的机遇，从而帮助变革商业、人类生活乃至整个世界。借助这些功能，IoT 解决方案能够帮助我们改善医疗成果，加速创造更优质的产品，增加购物的趣味和乐趣，或者优化能源生产和消耗等不一而足。展望未来，几乎每个设备都需要内置安全、互联的智能。同样，支持性网络和云基础设施必须得到强化，以更好地保护数据、管理设备和执行数据分析。

目录

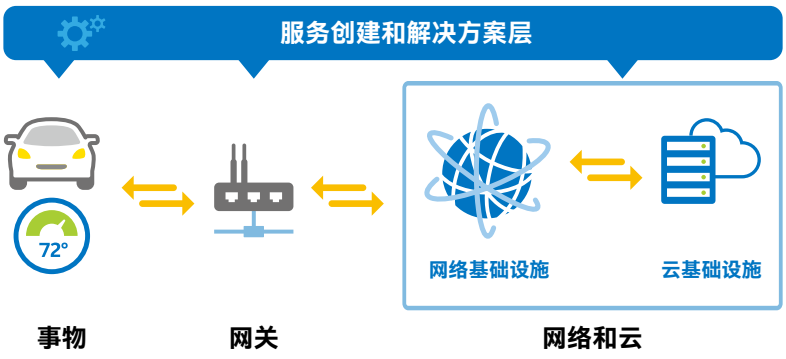

图 1. IoT 解决方案整合了多个系统

IoT 架构可简化为四类互联系统：事物、网关、网络和云、服务创建和解决方案层（如图 1 所示）。凭借在所有这些领域的丰富专业知识，英特尔就如何确保在这些系统之间可靠和安全地双向通信有着自己的独特见解。

事物

如今在商业和工业环境中、在人们家中以及移动用户的手中，存在着数以亿计的事物。汽车、设备传感器、可穿戴设备和移动手机早已通过宽带无线网络直接连接并访问互联网。IoT 解决方案要求事物要么具备智能特性以在本地过滤和管理数据，要么能够连接到可提供这种功能的网关。

示例：

- **移动设备：** 智能手机、平板电脑、GPS 系统、可穿戴设备
- **家居：** 安全警报、能耗监控器、照明开关、恒温器
- **工业：** 智能建筑、工厂自动化、电网、车队

网关

实现 IoT 完整愿景的一个主要障碍就在于大约 85%[1] 的现有事物无法连接至互联网且无法与云端共享数据。要解决该问题，移动、家居和工业网关需要在传统事物和云之间发挥中介作用，提供所需的连接性、安全性和可管理性。

网络和云

网络基础设施： 互联网是一个全球性互联 IP 网络系统，能够将计算机系统连接在一起。该网络基础设施由路由器、聚合器、网关、中继器和能够控制数据流动的其他设备组成，同时能够连接至服务提供商运营的电信和电缆网络（如 3G、4G/LTE）。

数据中心/云基础设施： 数据中心和云基础设施包含联网的大型虚拟化服务器和存储池。要支持 IoT，该基础设施需要运行应用来分析设备和传感器数据，以生成可用于服务和决策的有用信息。

服务创建和解决方案层

能否加速上市并实现 IoT 的全部价值取决于对整个系统的协调，以及对来自传统系统和现有业务资产的数据进行分析。为了帮助提供该功能，英特尔携手应用编程接口（API）管理软件领域业内公认的领导者，包括：

- **Mashery*：** API 管理的先驱，具有庞大的 API 开发人员群体和市场
- **Aepona*：** 领先的 API 和货币化解决方案提供商（面向服务提供商）

IoT 价值链

如前面章节所述，IoT 涉及的系统非常广泛，因此所需的 IoT 生态系统也应该能够提供多种多样的功能，如图 2 价值链所示。圆圈内包含相对标准的部件，第一个内圆是*组件*，如处理器、模块、操作系统和安全软件等。原始设计制造商（ODM）使用这些组件构建了*主板*，并最终由原始设备制造商（OEM）构建为*设备*。

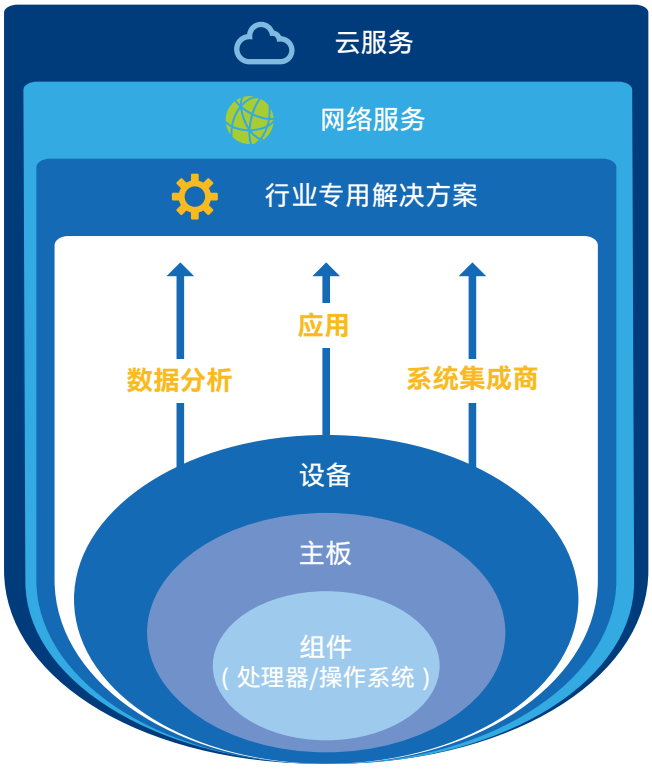

图 2. 物联网价值链包含多种解决方案提供商

然后*系统集成商*会整合*应用和数据分析软件*和其他专业要素，从而将这些通用产品转变成行业专用解决方案。与移动宽带一样，*网络服务*提供了设备与*云服务*之间的连接性，并利用分析和应用软件将原始数据转变成有用信息。

英特尔的系列产品和技术能够为 ODM、OEM、系统集成商、应用开发商以及网络和云服务提供商提供端到端 IoT 解决方案所需的基本功能。具体请见以下四个章节。

请点击此处探索 IoT 价值链每个层级上的英特尔生态系统。

面向事物的英特尔构建模块

本章节详细介绍了英特尔解决方案，内容涵盖处理器、芯片组、操作系统、安全解决方案和网络连接。

处理器和芯片组

端到端策略需要提高事物的智能和安全水平，以在本地可靠地过滤和管理数据。客户对分析、加密和新应用的需求增加了对高级别能源优化型性能的需求。

英特尔提供了四种基于后向兼容架构的英特尔® 处理器系列，全部具有可扩展的性能（图 3）— 从节能的英特尔® Quark™ SoC X1000 到高性能的英特尔® 至强® 处理器 — 可供设计事物的工程师选择。借助一套适合各种处理器的通用代码，英特尔计算平台能够为您提供各种价位和性能的解决方案。

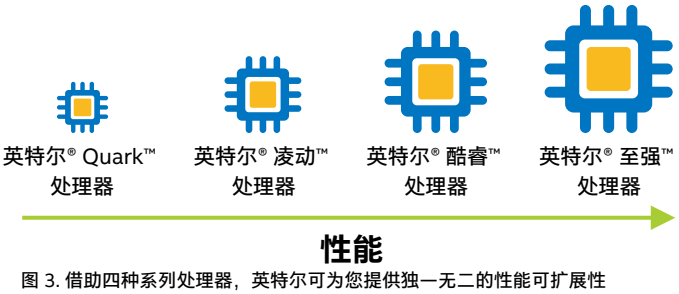

图 3. 借助四种系列处理器，英特尔可为您提供独一无二的性能可扩展性

- 英特尔 Quark SoC X1000 是低能耗的片上系统（SOC）系列，适用于能耗和规模要求优于高性能的环境。其 32 位、单核、英特尔® 架构兼容的 CPU 运行速度可高达 400 MHz。
- 英特尔® 凌动™ 处理器 E3800 产品系列能够在小外形设备中提供能源消耗低、散热效率高的应用性能。该系列处理器具有增强型媒体和图形性能、错误校正码、工业温度范围、内置安全特性和集成式图像信号处理功能。

- 英特尔® 酷睿™ 处理器产品系列可提供出色的计算、图形和媒体性能，以及更高的安全性和 I/O 灵活性。第 4 代英特尔酷睿处理器（U 处理器系列）专门针对小外形应用而设计，采用多芯片封装（MCP），将一个低能耗 CPU 和平台控制器集线器（PCH）集成到了一个通用封装基板上，如图 4 所示。

图 4. 第 4 代小外形英特尔® 酷睿™ 处理器将 CPU 和芯片组集成至一个封装内

- 英特尔至强处理器专门针对需要最高可用性能的计算密集型应用而设计，将多核性能和出色的计算密度结合在一起，提供了基于硬件的可管理性、安全性、虚拟化和能源管理。

操作系统

英特尔处理器可以运行 Linux* 、Microsoft* 和 Google* 的多种操作系统，以及 Wind River* 的以下系统：

- *Wind River VxWorks** 是全球领先的商用实时操作系统（RTOS），已为各种外形和尺寸的嵌入式系统提供服务逾 30 年之久。
- *Wind River Linux* 是领先的商用嵌入式 Linux 平台，率先将开源优势无风险地普及至所有行业的公司。
- *Wind River for Android** 提供了一系列可帮助面向运行 Android 操作系统的设备快速开发高质量平台和应用的软件和测试产品。

更多了解 Wind River 操作系统。

数据和事物安全性

在保护敏感数据、防止设备失窃和恶意软件攻击方面，企业所面临的压力日趋加大。保护个人可识别信息（PII）的全球性法规正变得日益严苛，而不合规的企业为此付出的代价也将更加惨重。此外，如果相关数据记录失窃或遭到未授权个人的访问，能创造竞争优势的宝贵知识产权（IP）也将岌岌可危。

网络犯罪社区从没有像现在这么猖獗。从图 5 可知，McAfee* Labs 采集到的威胁样本从 2014 年第 3 季度到第 4 季度增长了 15%，并且互不相同的恶意软件样本已超过 1.96 亿例。

端到端 IoT 解决方案潜在的广泛部署可能会增加企业面临安全漏洞的风险。为了帮助规避风险，英特尔及其子公司 McAfee 提供了一系列广泛的安全保护产品，可部署于设备、网关、网络和云基础设施等多个地方。例如：

- *McAfee 嵌入式控制*仅支持运行授权代码和做出授权变更，因此可有效保持设备、网关和服务器的完整性。它可以在系统上自动创建 “授权代码” 的动态白名单。白名单一旦创建和启用，系统就会锁定在已知活动范围内。授权集之外的任何程序或代码都无法运行。白名单可帮助防止病毒、间谍程序、蠕虫（如 Stuxnet 蠕虫）以及其他恶意软件在 IoT 系统上执行非法操作。

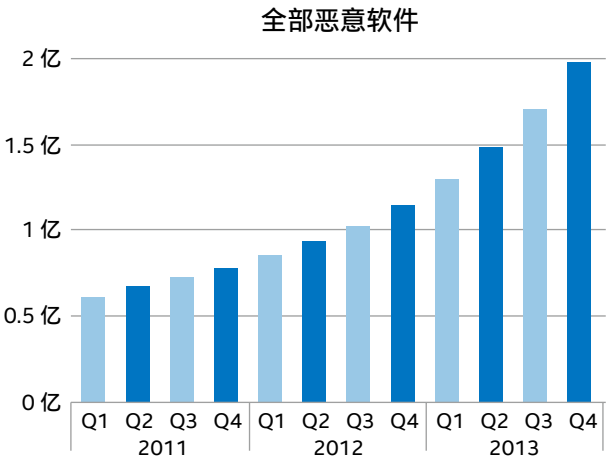

图 5. 恶意软件数量在 3 年内增长至超过 3 倍
资料来源：McAfee* Labs 威胁报告，2013 年第 4 季度

- *McAfee ePolicy Orchestrator* (McAfee ePO*)* 是行业内最先进、最具可扩展性的集中式安全管理软件。这款开放性平台支持统一的安全管理，有助于大幅降低安全和合规性管理的成本与复杂性。

- *McAfee 完整性控制*将 McAfee 嵌入式控制和 McAfee ePolicy Orchestrator (McAfee ePO) 控制台结合至一起，支持产品提供集成式审计和合规性报告，以帮助满足多种法律法规的要求。

- *McAfee* 终端加密*是数据保护的基石，因为它可在整个 IoT 环境中加密数据，包括设备、网关、网络文件和文件夹、可移动介质和 USB 便携式存储设备等。该软件采用在英特尔酷睿处理器上实施的英特尔® 高级加密标准新指令 (Intel® AES-NI) [2]，能够将数据加密速度提高多至 10 倍 (并行模式) [3,4]，同时不影响系统速度 (图 6)。

了解更多内容：McAfee 安全产品和解决方案。

- 英特尔® 身份保护技术 (英特尔® IPT) [5] 可通过利用强大的基于硬件的身份验证功能，有效防止未授权访问存储在云端的数据。该防篡改解决方案独立于操作系统运行。它还为网站和企业提供了一种简单方式以验证用户是否使用可信任设备登录。

网络连接

IoT 背后的基本概念便是将全球绝大多数的系统连接至一个公共网络和接触设施。英特尔计算平台和网卡可支持广泛的网络接口和协议，以提供所需的连接性：

- 英特尔® 以太网控制器 I210 是一个具备集成式 MAC 和 PHY 的低能耗、小尺寸、单端口千兆位板载局域网 (LOM) 网络控制器，是小型设备的理想之选。

- 英特尔® XMM™ 平台是一款支持 2G/3G/ LTE 的超薄调制调解器，支持高速数据和语音传输。它们结合了成本优化的 IC、参考设计和特性丰富的软件堆栈，并有着跨整个价值链的专业客户支持。其较小的体积基于一种灵活的模块化概念，仅凭一种设计便可满足不同应用领域的需求，如移动手机、移动计算或远程通信等。

  举例来说，英特尔® XMM™ 7160 蜂窝平台便可同时用作 LTE 智能手机、平板电脑以及机器对机器 (M2M) 应用的超薄调制调解器。它是一款面向全球市场的极为紧凑的 LTE/DC-HSPA 连接设备解决方案，可支持高速纯数据解决方案和具有语音功能的 4G 移动电话。

- 英特尔® 芯片组可支持多种 I/O 接口，包括以太网、USB、RS-232、RS-485、CAN、线路输出、PCI Express* 和 SPI。这些接口还可以连接支持蜂窝技术、蓝牙*、ZigBee*、WiFi 以及其他无线技术的模块。

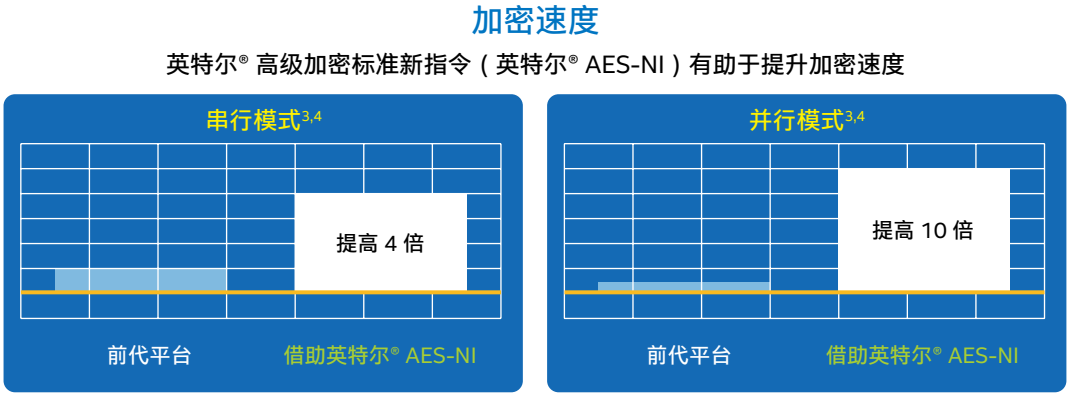

图 6. 英特尔新指令大幅加快加密速度

英特尔网关解决方案

面向物联网的英特尔® 网关解决方案（面向 IoT 的英特尔® 网关解决方案）能够加速上市时间，帮助设备制造商更快地开发、设计和部署应用服务，从而让企业专注于创造新的增值服务。这些解决方案能够为设备制造商提供多种平台，以开发可安全聚合、共享和过滤数据并进行分析的网关。

面向 IoT 的英特尔网关解决方案构建于开放的基础设施之上，可确保系统间的互操作性，支持广泛的应用开发并简化服务部署。经过验证的集成式组件（图 7）可提供最大限度的灵活性，支持快速应用开发和现场部署。该解决方案提供了完整的经过验证的平台，后者由软硬件构建模块组成，包括：

- 多种英特尔处理器选择：英特尔 Quark SoC X1000、英特尔® Quark™ SoC X1020 和英特尔® 凌动™ 处理器 E3826
- Wind River* 智能设备平台开发环境
- McAfee 嵌入式控制安全技术
- Wind River 智能设备平台是一款可扩展、可持续的安全开发平台，能够简化 IoT 网关的开发、集成和部署。如下页图 8 所示，它提供了支持大多数 IoT 系统所用协议的网络堆栈，并且支持设备提供商构建高性能、高价值的产品，以加速、分析和保护网络流量和应用。该平台基于 Wind River 业内领先的操作系统（符合标准且已经过全面测试）之上，还包括 Wind River 开发工具。该平台提供了设备安全、智能连接和设备管理功能以及丰富的网络选项。智能设备平台包括专门针对开发机器对机器（M2M）应用而构建的即用组件。

图 7. 网关软件堆栈

图 8. Wind River* 智能设备平台组件

关键特性:

网关安全: 提供内置安全特性，可有效保护通信信道、数据和终端设备。

应用支持: 提供 Lua、Java 和 OSGi 应用环境，支持在资源受限型设备和全功能设备上进行可移植、可扩展和可重复使用的应用开发。

设备连接: 支持 IoT 数据传输协议 MQTT，并对 WiFi、蓝牙*、ZigBee 和广泛应用于 IoT 设备中的短程无线协议提供本地支持。

远程设备管理: 支持 TR-069 和 OMA DM 等成熟的管理协议。

面向网络和云的英特尔解决方案

随着电信行业向全 IP 网络的过渡，设备制造商开始融合通信与计算技术两方面的优势。软件定义网络（SDN）和网络功能虚拟化加速了这一趋势的发展，帮助更加轻松地将网络、云和数据中心功能整合到标准的高容量服务器、交换机和存储设备上。

英特尔服务器技术被广泛用于网络和云基础架构，支持在虚拟服务器上运行范围广泛的应用和分析工作负载。在有线和无线网络领域，利用基于英特尔技术的服务器、存储和网卡的连接正在变得越来越经济，越来越普遍。随着电信行业加入企业和云行业一同部署全 IP 网络，英特尔解决方案被用于控制和数据平面，以支持软件定义的基础架构所需的本地化、安全性、API 和各种协议。

英特尔处于开发、保护和管理网络与云基础架构的前沿，提供了处理器、操作系统、开发平台、安全性解决方案、数据中心管理工具和高吞吐量网络连接。

计算平台和操作系统

网络和云中的计算平台需要能够交付最高级别的性能和可用性，英特尔提供了以下技术和产品，使得这一切成为可能:

- 面向通信基础架构的英特尔® 平台旨在同时运行不同的工作负载（如数据包处理、控制平面和应用软件），以提供优异的工作负载整合。这一专注于软件的平台具有内置安全性、压缩引擎和更快的数据包处理速度。
- 面向 Wind River Linux 的 Carrier Grade Profile 是首个满足 Linux 基金会 Carrier Grade Linux 5.0 规范的注册要求的产品，专门为 Yocto Project* 兼容产品而构建。这一交钥匙解决方案为所有行业提供了基本的功能，可满足下一代嵌入式 Linux 设计对基于标准的安全可靠解决方案的需求。

开发平台

以下开发平台可帮助开发人员轻松使用推荐的开源和英特尔®组件，协助他们制作各种设计的原型、开展性能评估、迁移应用软件，从而最终交付生产就绪型解决方案。

- 英特尔® 开放式网络平台（英特尔® ONP）得到了服务器和交换机参考设计的支持，能够支持设备制造商在虚拟化或基于硬件的网络设备中快速实现高性能、低延迟交换。这些 SDN 合规设计灵活且强大，并且支持对当今的网络环境和数据中心交换环境至关重要的增强特性。

  英特尔® 开放式网络平台服务器参考设计（Intel® ONP 服务器参考设计）如图 9 所示，可以在几乎任何基于英特尔至强和英特尔酷睿处理器的硬件平台上运行。KVM 虚拟机管理程序[6] 和英特尔® 虚拟化技术（英特尔® VT）[7] 提供了高性能且可靠的虚拟化环境。

  通过英特尔® 数据平面开发套件（英特尔® DPDK）加速的一个 Open vSwitch 版本可以在一个或多个虚拟机上运行。另外，未来还将有进一步优化，以支持远程管理和向协调基础架构的集成。对于某些工作负载，PCI-SIG 单根 I/O 虚拟化（SR-IOV）可用于供给虚拟设备。

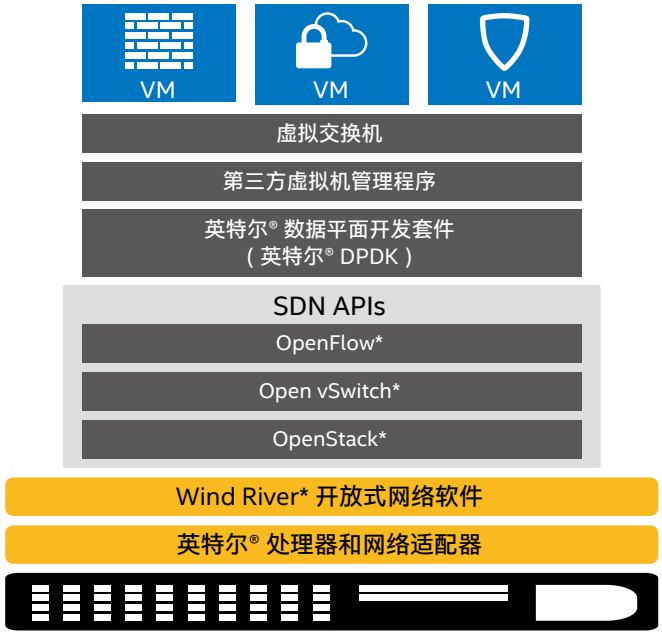

图 9. 参考设计

- Wind River 智能网络平台是一套优化的集成式软件系统，由构建高性能的下一代智能网络元件所需的关键运行时组件和生命周期开发工具组成。图 10 展示了两种基本的深层数据包检测技术的预集成：用以提供应用和内容感知的 IP 流分析技术以及用以检测恶意软件的正则表达式模式匹配技术。

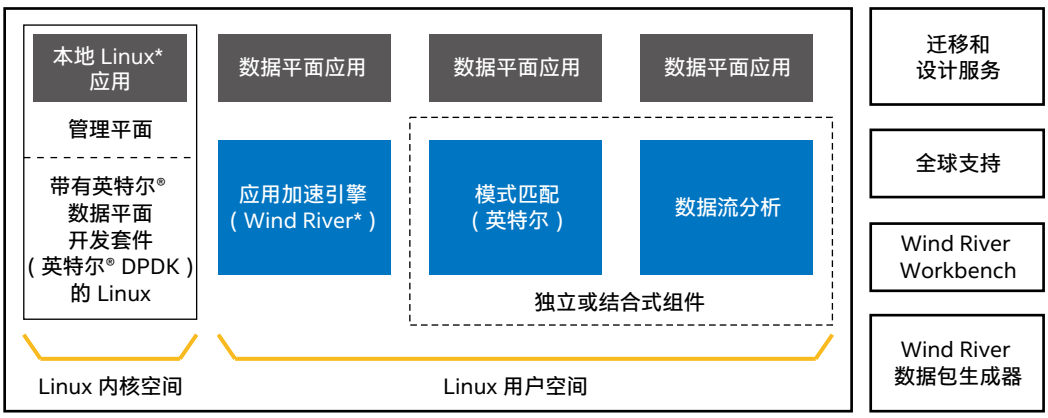

图 10. Wind River* 智能网络平台的关键组件

- *Qosmos* ixEngine*：这套软件库和工具执行 IP 流分类，可支持对第 4–7 层流量的深层可视性，从而与其他网络应用一起促进实时数据包分类、流量分类和通信协议识别。这类信息（精细应用和数据可视性的产物）大幅增强了网络运营商的环境感知能力，让他们能够更好地执行安全规则和管理流量。该解决方案使用应用/协议签名数据库对流量进行模式匹配、数据流关联和行为分析，该数据库包含数以千计的动态协议，这些协议会定期根据实时网络分析进行更新。

- *来自英特尔的 HyperScan*：该引擎执行精细的表达式模式匹配，高速扫描大量数据以搜索恶意软件。该引擎会访问具有成千上万个静态签名（用以检测文件内病毒）的数据库，是需要入侵防护（IPS）、防病毒和统一威胁管理（UTM）的系统的理想选择。虽然 Hyperscan 是一个面向 ixEngine 和 INP 的插件，但它同时也是一款独立的高性能匹配引擎，能够支持大部分行业模式数据库。

主要特性：

整合的管理与数据平面： 可以通过集成两种通常需要独立计算系统的工作负载来降低 BOM 成本和能量消耗。

数据包加速和吞吐量： 在 IP 转发和 UDP 与 TCP 终止方面实现了显著性能提升。[8]

应用加速引擎： 提供了全面的优化型网络堆栈，旨在加速第 3 层和第 4 层网路协议。

深层数据包检查： 识别流量、通信协议和应用。

网络元素安全性

- McAfee 网络安全平台使用高级威胁检测方法来发现和拦截网络中的复杂威胁，是理想的下一代入侵防护产品，其主要特性如图 11 所示。这一具有独特智能的安全解决方案已不再局限于单纯的模式匹配，能够以极高的准确性抵御隐形攻击，同时它的下一代硬件平台的速度已扩展至超过 80 Gbps[9]，能够满足要求苛刻的网络的需求。

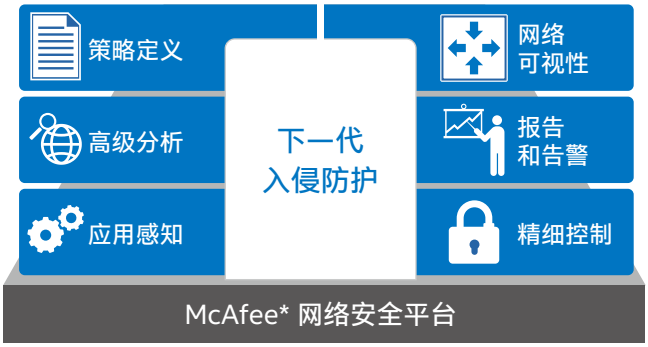

图 11. McAfee* 网络安全平台

数据中心管理

- 英特尔® 数据中心管理器（英特尔® DCM）产品组合为当今的数据中心提供了关键的管理功能。借助英特尔 DCM 产品组合，IT 和设施管理人员可以获得相应的工具以针对关键参数（如能源使用、监控、安全性、自动化和云）改进可管理性、提高可用性以及降低成本。这一多功能解决方案提供了关键的数据中心功能，包括：
- 能源管理工具
- 虚拟的键盘-显示器-鼠标（KVM）
- 设备管理 API
- 服务级别协议执行
- OpenStack* 插件

网络连接

- 英特尔® 82599 10 Gb 以太网控制器产品系列是英特尔的第三代 10 GbE 控制器，延续了其前代产品的创新趋势。英特尔 82599 10 Gb 以太网控制器是一个单芯片、双端口 10 GbE 实施。它能够通过集成串行 10 GbE PHY 来降低物料清单（BOM）成本和设计复杂性，同时还能提供简单固件接口（SFI）和 KR 接口。该设备旨在实现高性能和低内存延迟。

服务创建和解决方案层

为了实现物联网的价值，我们需要将通过设备和网关收集的数据发送至现有的后端系统，与其他来源的数据融合，然后将其提供给合作伙伴、客户和员工。这一点可以通过应用编程接口（API）管理来实现。

公开并管理数据以支持新服务

端到端的物联网解决方案需要一个控制层，不仅收集来自各种仪器的数据，同时还协调关键的物联网流程和核心的软件模块。该服务“平台”层是面向垂直行业的增值物联网服务创建的基础，或者独特的物联网业务模式的基础。该平台必须具有针对整个物联网部署的所有其他层的可视性和互操作性（跨硬件、网关、网络、分析和安全性），以便控制所有资源。

管理和控制必须具有很强的适应性，能够转译来自传统事物的信息并插入增值生态系统组件，以从物联网中获利并跟踪新发现的业务价值。物联网要求具有灵活性，不能基于一套单一的标准或全部通过单一厂商的软件堆栈实施。

API 管理是物联网的关键[10]

目前，很大一部分物联网互操作性、扩展和控制都可以通过 API 管理实现。基于标准的 Web API 设计模式、API 管理和 RESTful 架构在简化处理海量数据的异构系统之间的互操作性任务方面提供了巨大的价值。由于 API 的应用已经非常普遍，因此覆盖广泛细分市场的物联网部署能够受益于该成熟架构。

API 降低了实现互联的门槛并支持从各种事物到处于任何位置的应用（在任何云或数据中心内，或可通过支持 API 的设备访问）的安全通信。

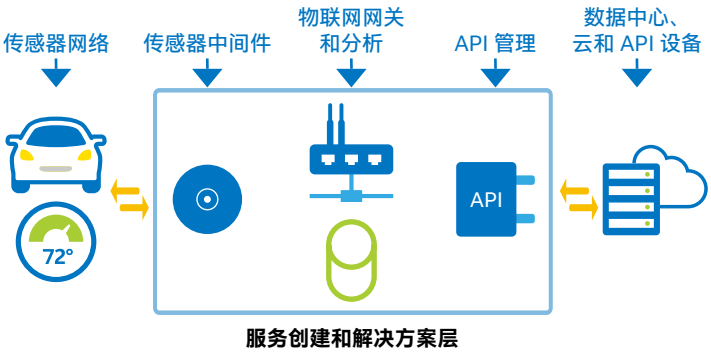

图 12. 面向 API 管理和物联网的概念性架构

图 12 展示了面向物联网网关解决方案的传感器中间件和 API 管理的价值所在：它们提供数据融合、环境信息、数据通信、协调和同步、数据和协议互操作性、隐私和安全性，以及容错能力。

实现物联网管理和控制的平台方法

英特尔基于 API 管理将可互操作的核心软件和服务能力聚集在一起作为物联网的基础，可以帮助企业、集成商和更大的物联网生态系统快速启动他们的物联网部署。该基础通过实施服务创建和垂直解决方案层来提供物联网管理和控制，如图 13 所示。

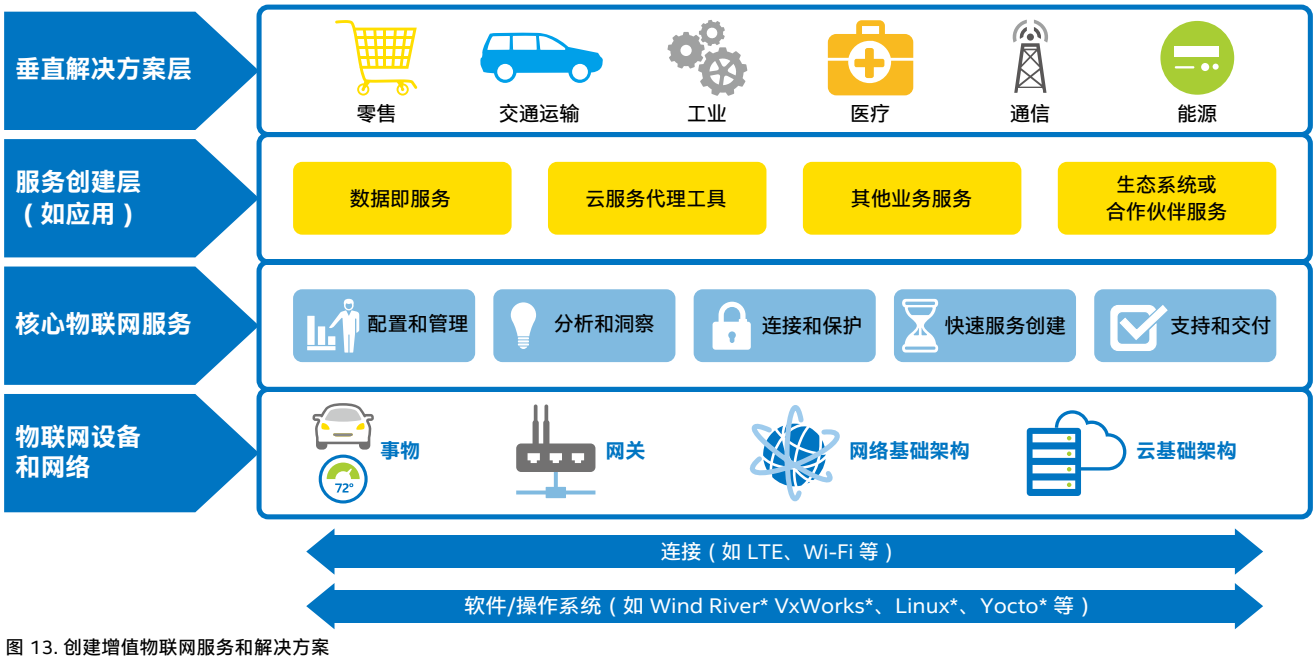

图 13. 创建增值物联网服务和解决方案

图 14. 互联物联网的基础

为了实现物联网的真正价值，企业应专注于他们可以通过来源于物联网的数据而实现的增值服务，以及如何将这些数据与他们的传统系统和企业资产结合起来。这种数据混搭存在于多个垂直行业，并且正是物联网的真正创新所在。再多的独特物联网业务战略和上市业务模式都能得到支持，不管它们是专注于内部、外部、移动，还是渠道合作伙伴。

英特尔将提供核心的物联网软件层来帮助协调垂直解决方案的装配。该层可通过以下特性来支持采用英特尔产品和技术的物联网服务和解决方案：

- 从各种事物到云的安全的端到端通信
- 互联且具有全球可扩展性的端到端解决方案
- 远程可管理性
- 平台间的互操作性
- 英特尔® 架构处理器优化的性能
- 智能数据分析

该核心物联网软件层通过提供以下功能为互联的物联网（图 14）建立了基础：

连接和保护 — 使用安全的 API，借助实时网关控制安全地连接和远程管理事物以提高互操作性。

配置和管理 — 远程管理从边缘到数据中心的全套解决方案，具有一致的用户体验。

数据服务和分析 — 使用世界级的数据中心技术安全传输、存储和分析大数据，同时在边缘利用智能算法来优化性能。

通过开发人员参与来提供服务支持 — 通过开发人员宣传和 API 门户积极吸引开发人员，以发挥社区创新威力。

快速服务创建 — 通过 API 创建和管理来快速轻松地支持流程集成，物联网 API 数据与现有系统融合，以及通过 API 集成合作伙伴产品。

面向物联网的 API 管理解决方案

英特尔的解决方案和服务可以进行混合和匹配，以适应特定的物联网部署和使用模式。

API 管理 — 通过软件即服务（SaaS）内部门户来管理和封装 API，以及管控来自各种事物的流量和分析 API 指标。该解决方案可支持开发人员发现、交互和测试 API，从而加速物联网应用的创建。

API 安全性和中介 — 通过移动友好型 OAuth、API 秘钥管理、开发人员参与和经过 PCI 认证的 SaaS 环境简化合作伙伴计划和开放 API 计划。根据需要，可应用企业级安全机制，如 API、安全防护、身份系统集成和跨安全域代理。

令牌化中介 — 利用一个中介来确保物联网数据负载（如个人身份信息（PII））的隐私性和安全性，该中介用作各种事物与处理物联网数据流的后端数据中心应用之间的代理。

API 创建和货币化 — 创建并向深度集成传感器数据、业务流程、网络和传统系统的合作伙伴和最终用户公布 API。关于付款和结算方面，工具 API 可支持各种计费、业务和支付网络模式。

API 上市服务 — 在开发业务案例、合作伙伴战略和上市计划时，可获得物联网和 API 专家的帮助。向最大的市场发布 API，该市场具有 24.5 万活跃开发人员和 86,000 款活跃应用。

智能物联，从芯开始

新兴的端到端的物联网解决方案将支持个人、企业和政府收集和分析各种数据并挖掘其中的含义，以支持改善人们的生活和提高企业的盈利。英特尔广泛的开放式和可扩展解决方案组合使得连接、保护和管理设备变得更加简单，从而帮助让这一切成为现实。凭借涵盖整个物联网架构（事物、网关、网络和云以及服务创建和解决方案层）的系统专业知识，英特尔正加速业务改造。

如欲了解有关英特尔物联网解决方案的更多信息，请访问：
www.intel.com/iot

[1] 资料来源：IMS 调研。

[2] 英特尔® AES-NI 要求电脑系统配备支持 AES-NI 的处理器并且要求非英特尔软件能够按正确序列执行指令。指定英特尔® 酷睿™ 处理器提供英特尔 AES-NI。详请请咨询您的系统制造商。如欲了解更多信息，请访问：**http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni**

[3] 在性能检测过程中涉及的软件及其性能只有在英特尔微处理器的架构下才能得到优化。诸如 SYSmark 和 MobileMark 等测试均系基于特定计算机系统、硬件、软件、操作系统及功能，上述任何要素的变动都有可能导致测试结果的变化。请参考其它信息及性能测试（包括结合其它产品使用时的运行性能）以对目标产品进行全面评估。

注意：以下声明应被包含在所有一般声明当中，但应单独标注：配置：[描述配置 + 测试中用到的部分 + 测试人]。如欲了解更多信息，请访问：**http://www.intel.com/performance**

[4] 如欲了解基准测试和配置信息，请访问以下网址查看白皮书：**http://software.intel.com/sites/default/files/m/d/4/1/d/8/10TB24_Breakthrough_AES_Performance_with_Intel_AES_New_Instructions.final.secure.pdf**

[5] 没有任何系统能够在所有情况下均能提供绝对的安全性。此项技术需要一个支持英特尔® 身份保护技术的系统，包括采用第二代或更高版本英特尔® 酷睿™ 处理器、支持英特尔技术的芯片组、固件和软件及相关网站。详情请咨询您的系统制造商。英特尔对数据和/或系统丢失或被盗责任以及任何其它损失不承担任何责任。如欲了解更多信息，请访问：**http://ipt.intel.com**

[6] 如欲了解更多信息，请访问：**www.linux-kvm.org**

[7] 英特尔® 虚拟化技术（英特尔® VT）要求计算机系统具备：支持英特尔® 虚拟化技术的英特尔® 处理器、基本输入输出系统（BIOS）、虚拟机管理程序（VMM）以及用于某些应用的特定平台软件。功能、性能或其它优势会根据软硬件配置的不同而有所差异，可能需要对 BIOS 进行更新。相关应用软件可能无法与所有的操作系统兼容。请咨询您的应用厂商以了解具体信息。

[8] 如欲了解性能和测试信息，请访问以下网址查看白皮书：**http://www.intel.com/content/www/us/en/communications/communications-packet-processing-brief.html**

[9] 如欲了解更多性能信息，请访问以下网址查看产品简介：**http://www.mcafee.com/us/resources/data-sheets/ds-network-security-platform-m-series.pdf**

[10] 资料来源：**https://blogs.intel.com/application-security/2013/10/08/api-management-for-the-internet-of-things-iot/**

0514/VF/TM/PDF ♻ 请注意环保 330562-001CN