

## 思科电子邮件安全设备



如今，每天往来的企业电子邮件超过一千亿封。随着电子邮件的使用量不断增加，安全问题变得愈发重要。各种瞬息万变的动态威胁都在伺机侵入您的组织。思科® 电子邮件安全解决方案可为您提供高度可用的电子邮件保护，免除您的后顾之忧。

### 功能和优点

无论是物理环境、虚拟环境、云，还是混合环境，我们公认业界一流的电子邮件安全解决方案都能为其提供以下优势：

- **快速、全面的保护：**反应时间通常比竞争产品早数小时或数日
- **最庞大的威胁情报网络之一：**以思科 Talos 广泛的综合安全分析作为基础
- **出站邮件保护：**通过设备内置防数据丢失 (DLP) 和电子邮件加密功能，以及与 RSA 企业 DLP 解决方案的可选集成提供出站邮件保护
- **较低的总拥有成本：**通过较小的占用空间、轻松的实施方式和自动化管理功能，实现长期成本节省

### 产品概述

如今，电子邮件安全形势十分复杂，各种入站威胁和出站风险比比皆是，垃圾邮件和恶意软件便是其中一种形式。集多种功能于一身的思科电子邮件安全设备不仅部署简单快速，而且具有维护需求少、延迟时间短、运营成本低的优势。这些设备采用“一次性设置”技术，当自动策略设置生效后，您的员工即可抽身去做其他事情。这些设备随后会自动推动思科[基于云的威胁情报解决方案](#)的安全更新。思科电子邮件安全设备每 3 到 5 分钟会刷新一次威胁情报数据，从而确保先于其他供应商数小时或数日对各种最新的威胁做出响应。这些设备不仅具有灵活的部署选项，而且可以与您的现有基础设施轻松集成，因此能够出色地满足您的业务需求。

### 虚拟设备

思科电子邮件安全虚拟设备可显著降低电子邮件安全解决方案的部署成本，特别是在高度分布的网络环境中，其优势更加显著。利用虚拟设备，您的网络经理可以根据需要随时随地使用您的现有网络基础设施创建实例。作为物理设备的软件版本，虚拟设备运行在 VMware ESXi 虚拟机监控程序和思科统一计算系统™（思科 UCS®）服务器之上。购买任何一款思科电子邮件安全软件捆绑包后，您便会获得虚拟设备的无限许可证。

利用虚拟设备，您可以通过简化的容量规划功能即时对不断增加的流量做出响应。您不必购买和运输设备，也无需增加数据中心的复杂性或另外雇用员工，即可为新商机提供支持。

## 主要功能

适用于物理环境、虚拟环境、云和混合环境的思科电子邮件安全解决方案可以为您的任务关键型电子邮件系统保驾护航。表 1 概括列出思科电子邮件安全解决方案的主要功能。

表 1. 主要功能

容量	说明
<a href="#">全球威胁情报</a>	<p>受全球最大的威胁检测网络之一支持，可提供快速、全面的电子邮件保护。思科电子邮件安全设备将广泛的可视性与强大的处理能力集于一身，具体包括：</p> <ul style="list-style-type: none"> <li>• 每天 100 太字节 (TB) 的安全情报</li> <li>• 160 万个已部署的安全设备（包括防火墙、思科入侵防御系统 [IPS] 传感器，以及网络和电子邮件设备）</li> <li>• 1.5 亿个终端</li> <li>• 每天 130 亿个网络请求</li> <li>• <a href="#">全球 35% 的企业邮件流量</a></li> </ul> <p>通过思科 Talos，您可以全天 24 小时查看全球流量活动。思科 Talos 能够分析异常、发现新的威胁并监控流量趋势。思科 Talos 还持续生成规则，通过这些规则将更新反馈给安全设备，以阻止零小时攻击。这些更新每 3 到 5 分钟刷新一次，从而确保提供业界领先的威胁防御。</p>
<a href="#">垃圾邮件拦截</a>	<p>垃圾邮件是一个复杂的问题，需要一个全面的解决方案。思科使之变得轻松简单。为了阻止垃圾邮件进入收件箱，思科提供一个多层防御系统，该系统将基于发件人信誉的外过滤层与对邮件执行深入分析的内置过滤层相结合。借助信誉过滤，超过 80% 的垃圾邮件在还未到达您的网络之前就能被拦截。最新的增强功能包括情景分析、强化自动化和自动分类，可很好地防御雪鞋垃圾邮件攻击。</p> <p>在短时间内收到大量电子邮件的客户可以根据发件人或主题应用过滤器，从而拦截或隔离相关邮件。</p>
<a href="#">灰色邮件检测和安全取消订阅</a>	<p>所谓灰色邮件，通常包括市场营销邮件、社交网站邮件和群发邮件。灰色邮件检测可以对进入组织网络的灰色邮件进行精确分类和监控。管理员可以在此基础上，对各类灰色邮件执行适当的操作。灰色邮件往往会带有取消订阅链接，供最终用户用来向发件人表明他们不想再接收此类邮件。由于伪装取消订阅机制是十分常见的网络钓鱼手法，所以用户应谨慎点击此类取消订阅链接。</p> <p>安全取消订阅解决方案具有以下优势：</p> <ul style="list-style-type: none"> <li>• 防御伪装成取消订阅链接的恶意威胁</li> <li>• 为管理所有订阅提供统一界面</li> <li>• 邮件管理员和最终用户可以更好地了解此类邮件</li> </ul>
<a href="#">高级恶意软件防护</a>	<p>思科电子邮件安全设备目前包含思科高级恶意软件防护 (AMP) 功能。此外，这些设备还具有文件信誉评分和拦截、静态和动态文件分析（沙盒）以及文件追溯功能。文件追溯功能可持续对文件执行威胁分析，即使文件已经通过电子邮件网关也是如此。借助这些功能，用户可以拦截更多攻击、跟踪可疑文件、缩小爆发范围，并快速进行补救。高级恶意软件防护功能可作为附加许可功能，供所有购买电子邮件安全设备的客户使用。思科 <a href="#">AMP Threat Grid</a> 通过内部部署设备提供恶意软件保护，非常适合那些因为合规性或政策上的限制，而无法将恶意软件样本上传到云的组织。</p>
<a href="#">病毒爆发过滤器</a>	<p>病毒爆发过滤器旨在防御各种新型威胁和混合攻击。病毒爆发过滤器可以发布由六种参数（包括文件类型、文件名称、文件大小和邮件中的 URL 等）以任意组合构成的规则。当思科 Talos 对病毒爆发事件掌握更多信息后，病毒爆发过滤器会相应地修改规则，并酌情释放隔离区中的邮件。病毒爆发过滤器还能重写可疑邮件中的 URL 链接。点击新 URL 后，系统会通过 <a href="#">思科网络安全</a> 代理对收件人进行重新定向。然后，系统会主动扫描目标网站的内容，如果该网站包含恶意软件，病毒爆发过滤器会显示拦截窗口。</p>
<a href="#">Web 互动跟踪</a>	<p>Web 互动跟踪是一个完全集成的解决方案，IT 管理员可以使用此功能来跟踪那些点击已被 ESA 重写的 URL 的最终用户。此功能会提供包含以下内容的报告：</p> <ul style="list-style-type: none"> <li>• 点击恶意 URL 次数排名靠前的用户</li> <li>• 最终用户点击数排名靠前的恶意 URL</li> <li>• 日期/时间；重写原因；对 URL 采取的操作</li> </ul> <p>管理员还可以反向跟踪所有包含特定 URL 的邮件。</p>
<a href="#">出站邮件控制</a>	<p>思科电子邮件安全设备可以通过 DLP、电子邮件加密，以及与 RSA Enterprise Manager 的可选集成，对出站邮件进行控制。此类控制有助于确保您的最重要邮件既符合行业标准，也能在传输过程中受到保护。此外，出站反垃圾邮件和防病毒扫描以及出站速率限制也可用于防止您的公司因被盗的计算机或帐户而被列入电子邮件黑名单。新功能：除传输层安全 (TLS) 协议外，思科电子邮件安全设备现在还支持安全/多用途互联网邮件扩展 (S/MIME) 加密和签名。</p>
<a href="#">卓越的性能</a>	<p>思科电子邮件安全设备可以快速拦截各种新型入站电子邮件病毒。域投递队列可防止因电子邮件无法投递而导致关键的投递内容备份到其他域中。这些设备可以实现超过 99.9% 的垃圾邮件捕获率，以及不足百万分之一的误报率，领先于整个行业。</p>
<a href="#">DLP</a>	<p>您可以使用一个或多个预定义的策略（可供选择的策略超过 100 个）来防止机密数据从网络中泄露。如果您愿意的话，也可以使用这些预定义的部分策略来创建您自己的自定义策略。内置的 RSA 电子邮件 DLP 引擎可使用预调整的数据结构以及您自己的可选数据点（如字词、短语、字典和正则表达式），来快速创建误报率接近于零的准确策略。由于 DLP 引擎会按严重性对违规行为进行评分，因此，您可以根据自己的需求来应用不同级别的补救措施。</p>

容量	说明
<b>较低的成本</b>	思科电子邮件安全解决方案占用空间小、易于安装，而且能够自动管理更新，可在整个生命周期中为您节省成本。思科解决方案的总拥有成本 (TCO) 低于绝大多数竞争对手。
<b>灵活部署</b>	<p>所有思科电子邮件安全解决方案都支持简单实施。系统设置向导可以应对非常复杂的环境，只需短短几分钟即可帮您完成设置并获得保护，从而提高您的安全性和速度。由于许可是基于用户，而不是基于设备，因此，您可以按用户（而不是按设备）应用许可，以便提供入站和出站电子邮件网关保护，而不会额外增加成本。这样一来，您可以通过反垃圾邮件和防病毒引擎扫描出站邮件，从而完全满足您的业务需求。</p> <p>虚拟设备的功能与物理设备几乎完全相同，不同之处仅在于前者采用虚拟部署模式，不仅更方便您使用，而且还可以节省更多成本。虚拟设备还提供即时自助调配功能。获得思科电子邮件安全虚拟设备许可证后，您无需使用互联网连接，即可在您的网络中部署电子邮件安全网关。此许可证中会内嵌各种已购买的软件许可。您可以随时将这些许可证应用于本地存储的新虚拟映像文件。如果需要，您可以复制原始的虚拟映像文件，以便能够立即部署多个电子邮件安全网关。</p> <p>您可以在同一部署中运行电子邮件安全解决方案的硬件版本和虚拟版本。这样，您的小型分支机构或远程地点无需在其所在位置安装硬件并提供相关支持，即可获得与总部相同的保护。您可以使用<a href="#">思科内容安全管理设备或思科内容安全管理虚拟设备</a>来轻松管理自定义部署。</p>
<b>满足您业务需求的解决方案</b>	<p><a href="#">思科云电子邮件安全解决方案</a>是一项高度可靠的全方位服务，它将软件、计算功能和支持集于一身。它采用与思科电子邮件安全解决方案的硬件版本和虚拟版本完全相同的共同管理用户界面。因此，您只需极少的管理开销，而且不必部署需要监控和管理的现场硬件，即可获得优质保护。</p> <p>混合解决方案可方便您现场对敏感邮件进行高级出站控制，同时还能让您充分享受具成本效益的云所带来的便捷性。</p> <p>混合解决方案同时提供内部部署硬件和虚拟设备。您可以选择最适合您环境的模式，在您的网关保护入站和出站邮件。</p>

## 产品规格

表 2 和表 3 分别列出思科电子邮件安全设备的性能规格和硬件规格。表 4 为虚拟设备的规格。表 5 为思科安全管理设备的规格。

表 2. 思科电子邮件安全设备的性能规格

部署	型号	磁盘空间	RAID 镜像	内存	CPU
大型企业	ESA C690	2.4 TB (600 x 4)	有 (RAID 10)	32 GB DDR4 内存	2 个 2.4 GHz CPU (八核)
大型企业	ESA C690X	4.8 TB (600 x 8)	有 (RAID 10)	32 GB DDR4 内存	2 个 2.4 GHz CPU (八核)
大型企业	ESA C680	1.8 TB (300 x 6)	有 (RAID 10)	32 GB DDR3 内存	2 个 2.0 GHz CPU (六核)
中型企业	ESA C390	1.2 TB (600 x 2)	有 (RAID 1)	16 GB DDR4 内存	1 个 2.4 GHz CPU (八核)
中型企业	ESA C380	1.2 TB (600 x 2)	有 (RAID 1)	16 GB DDR3 内存	1 个 2.0 GHz CPU (六核)
中小型企业或分公司	ESA C190	1.2 TB (600 x 2)	有 (RAID 1)	8 GB DDR4 内存	1 个 1.9GHz CPU (六核)
中小型企业或分公司	ESA C170	500 GB (250 x 2)	有 (RAID 1)	4 GB DDR3 内存	1 个 2.8 GHz CPU (双核)

注：为准确确定所需设备规格，请与思科内容安全专家一起评估峰值邮件流速率和平均邮件大小，以确认您的选择是否适当。

表 3. 思科电子邮件安全设备的硬件规格

型号	ESA C690	ESA C690X	ESA C680	ESA C390	ESA C380	ESA C190	ESA C170
机架单元 (RU)	2RU	2RU	2RU	1RU	2RU	1RU	1RU
尺寸 (高 x 宽 x 深)	3.4 x 19 x 29 英寸 (8.6 x 48.3 x 73.7 厘米)	3.4 x 19 x 29 英寸 (8.6 x 48.3 x 73.7 厘米)	3.5 x 19 x 29 英寸 (8.9 x 48.3 x 73.7 厘米)	1.7 x 19 x 31 英寸 (4.3 x 48.3 x 78.7 厘米)	3.5 x 19 x 29 英寸 (8.9 x 48.3 x 73.7 厘米)	1.7 x 19 x 31 英寸 (4.3 x 48.3 x 78.7 厘米)	1.67 x 16.9 x 15.5 英寸 (4.24 x 42.9 x 39.4 厘米)
直流电源选项	是	是	是	否	是	否	否
远程重新通电	是	是	是	是	是	否	否
冗余电源	是	是	是	是	是	是 (配件选项)	否

热插拔硬盘	是	是	是	是	是	是	是
以太网接口	6 端口千兆 Base-T 铜缆网络接口 (NIC), RJ-45 连接器	6 端口千兆 Base-T 铜缆网络接口 (NIC), RJ-45 连接器	6 端口千兆 Base-T 铜缆网络接口 (NIC), RJ-45 连接器	6 端口千兆 Base-T 铜缆网络接口 (NIC), RJ-45 连接器	6 端口千兆 Base-T 铜缆网络接口 (NIC), RJ-45 连接器	2 端口千兆 Base-T 铜缆网络接口 (NIC), RJ-45 连接器	2 端口千兆 Base-T 铜缆网络接口 (NIC), RJ-45 连接器
速度 (兆位/秒)	10/100/1000, 自动协商	10/100/1000, 自动协商	10/100/1000, 自动协商	10/100/1000, 自动协商	10/100/1000, 自动协商	10/100/1000, 自动协商	10/100/1000, 自动协商
光纤选项	是, 独立 SKU 6 端口千兆 1G Base-SX 光纤: ESA - C690-1G 6 端口万兆 Base-SR 光纤: ESA - C690-10G	是, 独立 SKU 6 端口千兆 1G Base-SX 光纤: ESA - C690-1G 6 端口万兆 Base-SR 光纤: ESA - C690-10G	是, 独立 SKU 6 端口千兆 1G Base-SX 光纤: ESA - C690-1G 6 端口万兆 Base-SR 光纤: ESA - C690-10G	否	否	否	否

表 4. 思科电子邮件安全虚拟设备规格

邮件用户				
邮件用户	型号	磁盘	内存	核心
仅限评估	ESAV C000v	200 GB (10K RPM SAS)	4 GB	1 (2.7Ghz)
小型企业 (最多 1000)	ESAV C100v	200 GB (10K RPM SAS)	6 GB	2 (2.7Ghz)
中型企业 (最多 5000)	ESAV C300v	500 GB (10K RPM SAS)	8 GB	4 (2.7Ghz)
大型企业或运营商	ESAV C600v	500 GB (10K RPM SAS)	8 GB	8 (2.7Ghz)
服务器				
Cisco UCS	VMware ESXi 5.0、5.1 和 5.5 虚拟机监控程序			

表 5. 安全管理设备 M 系列平台规格

型号	SMA M690/690X/680	SMA M390/380	SMA M190/M170
用户数量	10000 或更多	最多 10000	最多 1000

## 部署位置

思科电子邮件安全解决方案支持以下部署方式：

- **现场部署：**思科电子邮件安全设备作为网关，通常部署在防火墙隔离区内部。根据您的邮件交换记录所设置的规范，传入的简单邮件传输协议 (SMTP) 流量会定向到设备的数据接口。设备会对这些流量进行过滤，然后将过滤后的邮件重新传递到您的网络邮件服务器。此外，您的邮件服务器也会将外发邮件定向到设备的数据接口，设备会根据外发策略过滤邮件，然后将邮件传递到外部目标位置。
- **虚拟部署：**您可以利用在您的小型分支机构运行的思科 UCS，来托管虚拟设备和其他思科产品（如思科网络安全虚拟设备）。这些产品可共同提供与其对应硬件同等级别的保护，同时还能节省空间和电力资源的成本投入。您可以通过安全管理设备或虚拟设备集中管理这类自定义部署。

## 云安全选项

[思科云电子邮件安全解决方案](#)为您提供灵活的电子邮件安全部署模式。此解决方案可通过共同管理帮助您降低成本，而且您无需部署任何现场电子邮件安全基础设施。

[思科混合电子邮件安全解决方案](#)不仅具备思科云电子邮件安全解决方案的优势，而且支持加密邮件高级出站控制和现场 DLP 功能。通过此混合解决方案，您可以随心所欲地过渡到云解决方案。



## 思科电子邮件安全解决方案：物理和虚拟设备许可证

以下所有思科电子邮件安全软件捆绑包都包含虚拟设备许可证：思科电子邮件安全入站捆绑包、思科电子邮件安全出站捆绑包，以及思科电子邮件安全高级版捆绑包。此许可证的期限与捆绑包中的其他软件服务一样，并可视需要用于多个虚拟实例（只要不超过所购买的用户数量）。所有思科电子邮件安全软件捆绑包中均包含思科电子邮件安全设备许可证。只需先按所需提供支持的邮箱数量购买适量的许可证，然后购买相应的内部部署设备即可。对于虚拟设备，只需订购软件许可证即可获得授权。

### 基于期限的订用许可证

此类许可证按 1 年、3 年和 5 年订用期限进行购买。

### 基于数量的订用许可证

思科电子邮件安全产品组合使用基于邮箱数量的分级定价。销售代表和合作伙伴代表会帮助确定正确的客户部署。

### 电子邮件安全软件许可证

我们提供三种电子邮件安全软件许可证捆绑包以及一种定制产品，分别为：思科电子邮件安全入站捆绑包、思科电子邮件安全出站捆绑包、思科电子邮件安全高级版捆绑包，以及高级恶意软件防护。表 6 列出每种软件产品的主要组件。

表 6. 软件组件

捆绑包	说明
思科电子邮件安全入站基本版	思科电子邮件安全入站基本版捆绑包提供多种电子邮件威胁防御方法，包括：基于灰色邮件检测的反垃圾邮件功能、Sophos 防病毒解决方案、病毒爆发过滤器和群集技术。
思科电子邮件安全出站基本版	思科电子邮件安全出站基本版捆绑包可借助 DLP 合规性、邮件加密和群集技术来防止数据丢失。
思科电子邮件安全高级版	思科电子邮件安全高级版捆绑包将上述两种思科电子邮件安全基本版许可证中包含的入站和出站保护功能结合在一起，在防范电子邮件威胁的同时，提供必要的防数据丢失能力。
定制产品	说明
思科高级恶意软件防护	思科高级恶意软件防护 (AMP) 是一款可与任意思科电子邮件安全软件捆绑包一起购买的定制产品。AMP 是将恶意软件检测与拦截、持续分析和追溯性警报集于一身的综合恶意软件防护解决方案。 AMP 具有文件信誉评分与拦截、静态和动态文件分析（沙盒），以及文件追溯功能，可以持续分析各种威胁，即使这些威胁已通过电子邮件网关也是如此。因此，它可以使思科电子邮件安全设备中固有的防恶意软件检测和拦截功能得到进一步增强。购买任何必要的硬件后，您便会获得 <a href="#">AMP Threat Grid</a> 的无限许可证。
灰色邮件安全取消订阅	此功能可使用真正安全的“取消订阅”选项来标记灰色邮件。借助此标记，您可以替最终用户安全地管理“取消订阅”操作。此功能还会监视不同的灰色邮件取消订阅请求。您可以在 LDAP 组级别（策略级别）管理所有灰色邮件取消订阅请求。

### 软件许可协议

购买每份软件许可证都应签署思科最终用户许可协议和网络安全补充最终用户许可协议。

### 软件订用支持

所有思科电子邮件安全许可证都包含软件订用支持，此支持对于保证业务关键应用持续可用、高度安全，并且始终保持最佳性能非常重要。利用这项支持，您可以在所购买软件订用的整个有效期内使用下列服务。

- 软件更新和重要升级：确保应用以最新功能在最佳状态下运行。
- 思科技术支持中心：提供快速、专业的支持服务。
- 在线工具：构建和扩展内部专业资源以及提高业务灵活性。
- 协作学习：提供额外的学习知识和培训机会。

## 思科服务

表 7 概括列出适用于思科电子邮件安全解决方案的思科服务。

表 7. 思科服务

服务	说明
<b>思科品牌服务</b>	<ul style="list-style-type: none"><li>借助思科安全规划和设计服务，您能够以具成本效益的方式快速部署强大的安全解决方案。</li><li>思科电子邮件安全配置和安装远程服务通过安装、配置和测试您的解决方案降低安全风险。</li><li>思科安全优化服务通过设计、性能调整和支持系统变更，让不断发展的安全系统能够应对新出现的安全威胁。</li></ul>
<b>协作与合作伙伴服务</b>	<ul style="list-style-type: none"><li>思科协作专业服务网络设备安全评估服务通过确定安全差距，确保您的网络环境始终固若金汤。</li><li>思科智能关怀服务利用思科安全情报进行主动监控，确保您的企业处于最佳运营状态。这些安全情报源于思科高度可靠的网络性能可视性。</li><li>思科合作伙伴还提供有关规划、设计、实施和优化生命周期的各类其他服务。</li></ul>
<b>思科融资</b>	Cisco Capital® 可根据业务需求定制融资解决方案，以便您可以更快速地获得思科技术和业务优势。

## 思科 SMARTnet 支持服务

为了从技术投资中获得最大收益，您可以为您的思科电子邮件安全设备购买思科 SMARTnet™ 服务。借助这项服务，您可以随时直接与思科专家联系、使用各种自助式支持工具，并迅速实现硬件更换，从而快速解决网络问题。有关详情，请访问 <http://www.cisco.com/go/smartnet>。

## 如何评估思科电子邮件安全设备 (ESA)

要想充分了解思科电子邮件安全设备 C 系列和 X 系列平台的优势，最好的办法就是参加[先试后买计划](#)。如需获取具有完整功能的评估设备，在您的网络中进行实际测试（可免费试用 45 天），请访问 <http://www.cisco.com/go/esa>。

## 如何评估思科云电子邮件安全服务

基于云的解决方案是一种可靠的全包式服务，可提供灵活的电子邮件安全部署模式。它可通过共同管理帮助您降低个人成本，且无需部署任何现场电子邮件安全基础设施。您的思科客户团队或经销商可以帮助您设置 45 天的免费评估。

## 如何评估思科电子邮件安全虚拟设备

1. 访问 <http://www.cisco.com/go/esa>。
2. 在右侧的“支持” (Support) 部分，点击“软件下载、版本和一般信息” (Software Downloads, Release, and General Information)。点击“下载软件” (Download Software)，然后点击任何型号所对应的链接，系统将显示可下载的虚拟机映像。您还会看到一个可下载的 XML 评估许可证。您需要下载其中一个映像以及该 XML 评估许可证。
3. 从 Cisco.com 下载以下文档：
  - a. [思科安全虚拟设备安装指南](#)
  - b. Cisco AsyncOS 9.5 for Email 的[版本说明](#)
4. 按照思科安全虚拟设备安装指南中的说明开始操作。请注意，思科内容安全虚拟设备评估不在思科 SMARTnet 服务范围内，因此不受支持。

## 保修信息

如需查看保修信息，请访问 Cisco.com 的[产品保修](#)页面。

## 为什么选择思科？

对您的网络而言，安全问题已变得前所未有地重要。由于威胁和风险一再出现，再加上人们对机密性和可控性的担忧，因此，必须确保安全，才能实现业务连续性、保护重要信息、维护品牌信誉。在您的网络中嵌入的思科集成安全解决方案可提高可视性和可控性，以确保您的业务不会中断。我们不仅具有市场领先地位、资历丰富、产品新颖，还能在整个攻击过程中（攻击前、攻击中和攻击后）提供高级威胁防御，这些优势可保证我们成为能够满足您的安全需求的最佳供应商。

## Cisco Capital

### 提供融资服务，助您实现目标

Cisco Capital 可帮助您获得所需的技术来实现目标并保持竞争力。我们可以帮助您减少资本支出、加速业务发展、并优化投资和投资回报率。借助 Cisco Capital 融资服务，您在购买硬件、软件、服务和第三方补充设备时将拥有更多灵活性。Cisco Capital 可以为您提供一种可预测的支付方式。Cisco Capital 目前已在 100 多个国家/地区推出融资服务。[了解详情](#)。

### 更多详情

更多详情，请访问 <http://www.cisco.com/go/emailsecurity>。如需试用最受欢迎的产品，请参阅[免费试用电子邮件安全产品的三种方式](#)。



美洲总部  
Cisco Systems, Inc.  
加州圣何西

亚太地区总部  
Cisco Systems (USA) Pte.Ltd.  
新加坡

欧洲总部  
Cisco Systems International BV  
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。地址、电话号码和传真号码均列在思科网站 [www.cisco.com/go/offices](http://www.cisco.com/go/offices) 中。

思科和思科徽标是思科和/或其附属公司在美国和其他国家或地区的商标或注册商标。有关思科商标的列表，请访问此 URL：[www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks)。本文提及的第三方商标均归属其各自所有者。使用“合作伙伴”一词并不暗示思科和任何其他公司存在合伙关系。(1110R)