2019 年度网络安全报告系列

请扫描二维码
获取更多安全资料

致电: 4006 680 680

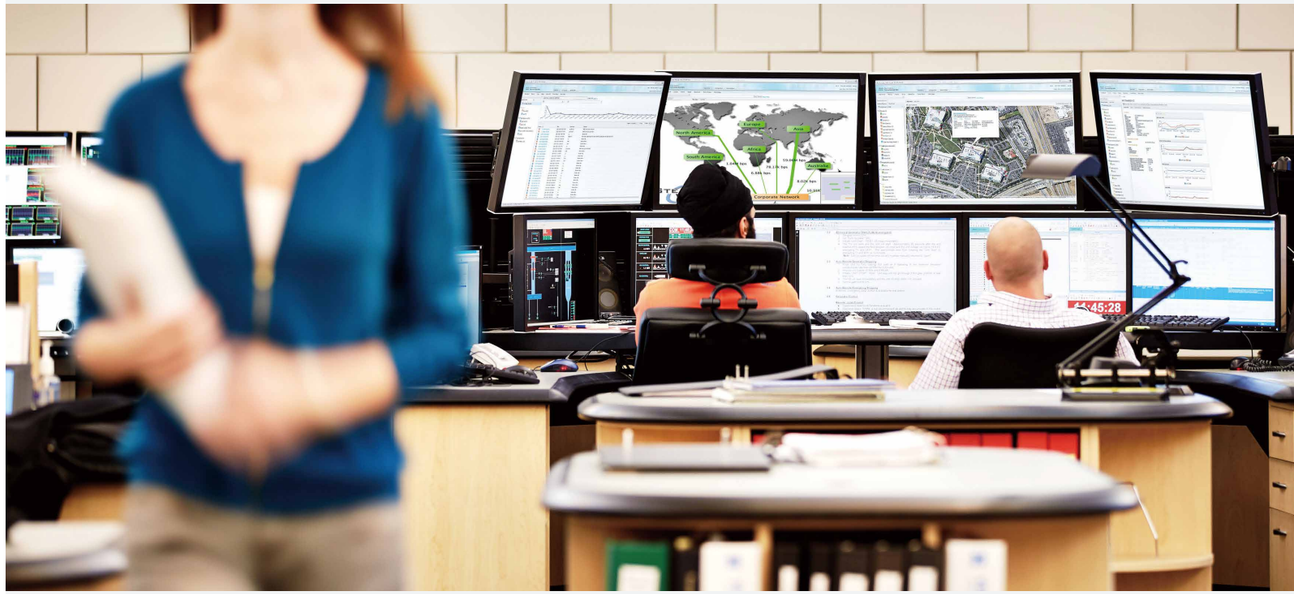
如需了解思科公司的更多信息，请浏览 http://www.cisco.com.cn

请扫描二维码
获取更多安全资料

思科网络安全解决方案综述

目录

思科网络安全解决方案综述



综述

当前企业面临的安全挑战

随着信息化技术的发展，用户的业务模型发生了很大的变化，云计算、BYOD以及虚拟化技术的大量应用，在提高了劳动生产效率的同时，也让我们传统的网络边界变得模糊，如何更好的实施控制和威胁防御，是网络安全面临的一个重大课题。

动态的零日威胁大量出现，即安全补丁与漏洞曝光的同一日内，针对该漏洞相关的恶意程序就会出现。而这种威胁往往具有很大的突发性与破坏性，对企业的网络安全和重要数据造成了越来越大的威胁。而近期加密勒索软件的频频曝光，也给我们的企业用户带来了更多遭受攻击的可能。

很多企业用户也为自己的网络选择了不少的网络安全技术，以期望能够保障整个网络的安全性，包括防火墙、防病毒、入侵防御等等，但这些技术在真正部署过程中，往往都是孤军奋战，没有形成一个体系架构，也没有全网统一的规划、分析和响应，更像一些碎片性的方案，达不到1+1〉2的效果。

了解碎片化安全方案的危险在哪里

@2019 思科及其子公司版权所有

思科关注威胁的网络安全模型

为了满足用户新的业务需要，应对最新的安全挑战，我们需要关注威胁的安全模型，主要包括三点：

1、覆盖攻击的整个过程

- 在攻击发生之前，能够全面的了解整个网络的状况，通过实施细粒度的安全控制策略以及对系统/主机/流量等的加固措施，提高系统对攻击的防御能力，进而最大限度减少攻击的可能性。
- 在攻击发生之中，需要采用智能分析和关联等技术，准确的检测出攻击所在，并且充分利用相关的设备和防御手段，对攻击进行阻挡和全面的防御。
- 在攻击发生之后，可以通过入侵事件关联分析、异常流量分析以及恶意软件防护的攻击跟踪追溯技术，准确的定位出攻击的范围以及影响，并且做出有效的响应和修复，最大限度减少攻击的危害。

2、涵盖网络/终端/移动设备/虚拟化平台/云平台等平台

- 随着用户业务模型的变化，我们需要在各个层面保障业务的安全性，包括网络/终端/移动设备/虚拟化平台/云平台，我们新的安全设备和软件，将会完全支持这些平台，应对用户多种环境下的安全需求。

3、持续的安全模型，非单个时间点的安全

- 整个安全模型是一个动态的，连续的过程，需要一个快速敏捷的安全，思科的解决方案可以随着用户环境的不断变化，实时的获取最新的情景信息，并且实时的进行攻击检测，安全策略的动态修改，保证用户网络的一个动态的安全性。

思科的网络安全解决方案将会专注于以下三个方面：

1、全面提高可见性 Visibility Driven

我们无法保护一个自己根本就不了解的网络。对网络的全面可知，是管理员做出正确的控制和防御策略的前提。利用思科的情景感知技术，管理员可以对企业网络的所有用户，移动终端，客户端应用程序，操作系统，虚拟机通讯，漏洞信息，威胁信息，URL 等相关信息实现全面的可见性。思科的众多的网络和网络安全组件都可以很好的支持情景感知技术。

2、关注威胁 Threat Focused

我们需要以威胁防御为中心，利用整合的多种网络安全技术，以及最新的云智能，关注攻击发生的整个过程，在攻击发生的各个阶段，全面的检查、理解和阻挡攻击，通过不断的完善自己的解决方案，来保护用户的网络，最快时间发现和解决网络中出现的安全事件，最大限度的减少恶意攻击带来的损失。

3、统一平台 Platform Based

网络安全，离不开网络，单单靠一些独立的安全平台，是没有办法组成一个有机的安全体系。思科将业界领先的网络基础架构平台和网络安全平台相结合，利用 SDN 以及 open API 等相应技术，在物理平台、虚拟平台以及云平台之上，提供了全面的安全服务，包括情景感知、内容感知、访问控制、应用识别、威胁控制等安全服务。通过 open API 技术，思科的网络安全服务可以与思科以及第三方的相应技术，实现完美的结合，实现了统一的安全防控和安全管理。

思科 Talos 团队

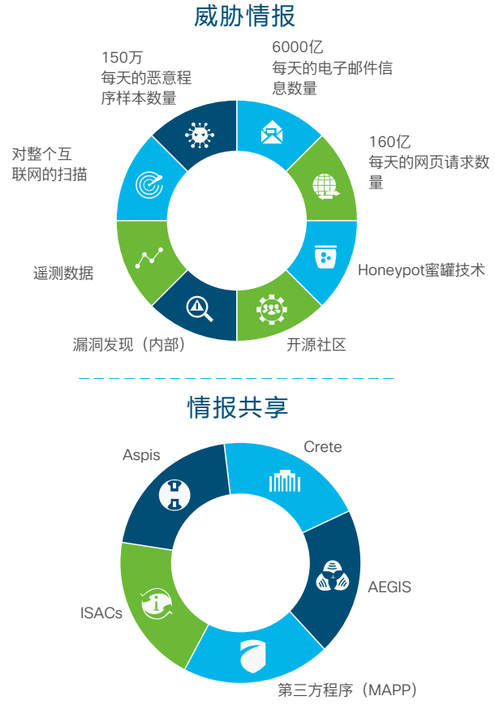
查看思科 Talos 团队
最新精彩见解

思科 Talos 团队介绍

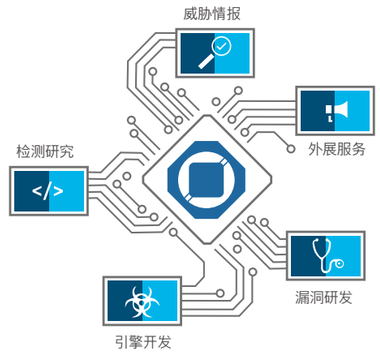
思科 Talos 团队由业界领先的网络安全专家组成，他们分析评估黑客活动，入侵企图，恶意软件以及漏洞的最新趋势。包括 ClamAV 团队和一些标准的安全工具书的作者中最知名的安全专家，都是思科 Talos 的成员。该团队的专长涵盖软件开发，逆向工程，漏洞分析，恶意软件的调查和情报收集等。思科 Talos 团队同时也负责维护Snort.org，ClamAV，SenderBase.org 和 SpamCop 中的官方规则集，同时得到了社区的庞大资源支持，使得它成为网络安全行业最大的安全研究团队。

思科 Talos 作为思科安全情报的主要发掘提供团队,为思科的安全研究和安全产品服务提供了强大的后盾支持,帮助思科的安全解决方案阻挡最新最复杂的攻击。

思科 Talos 威胁情报



思科 Talos 包括5个团队



超过250名
全职威胁情报
研究人员

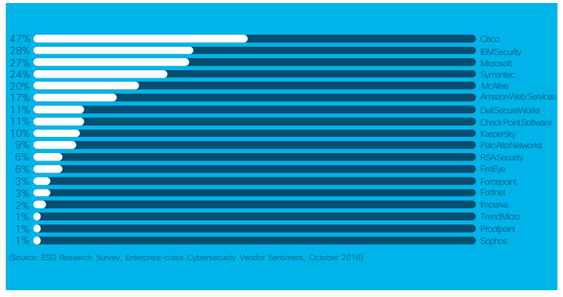
上百万个
遥测代理

4个
全球数据中心

超过100家
威胁情报合作
伙伴

1100个
威胁捕获程序

全球网络安全情报最佳提供商，思科位列第一



思科网络安全技术与平台介绍

思科以先进的安全模型作为指导，也给用户提供业界最为领先，最为全面的安全技术和解决方案，主要包括四个方面：下一代网络安全平台，高级威胁防御解决方案，内容安全解决方案和访问控制与策略服务解决方案。

网络安全平台（下一代防火墙/入侵防御）

Cisco 推出 ASA/Firepower 下一代网络安全平台，重新定义了下一代的防火墙概念：自适应，专注于威胁防御的统一安全平台。通过这个平台，可以给用户提供无以伦比的可见性，多层次的深度防御功能，并且降低安全成本和管理的复杂度。

ASA/Firepower 下一代安全平台的核心功能包括:

- 状态检测防火墙功能/NAT 地址转换功能
- IPSec VPN/SSL VPN 技术
- 全面的网络可见性，包括用户、应用、操作系统、漏洞等
- 新一代的入侵防御技术，提供业界最高的防护效率
- URL 过滤技术
- AMP 恶意软件防护技术

ASA/Firepower 下一代安全平台保障用户最优化网络性能:

- 与网络设备深度结合,保证整个系统的最大冗余性和最高性能
- Clustering 集群技术,实现了安全性能的 1+N 的冗余,按需增加以及多活数据中心情景下的安全多活
- 各种路由协议的广泛支持,以及对 Vxlan 等最新技术的支持,实现了安全的无处不在

ASA/Firepower 下一代安全平台实现了最优威胁防御，简化用户安全运维:

- 实现对内网每个终端/服务器的全面建模，如操作系统/漏洞/开放端口/应用/安全事件等等。
- 基于以上建模的动态自动安全策略推荐，帮助管理员自动配置最佳安全策略,减少人为错误。
- 威胁与终端信息结合，提供对安全事件的影响指数分析，使管理员可以专注于对我们影响最大的安全事件。
- 感染指数，将威胁按照终端汇总关联，快速发现内网中有问题的主机
- 可追溯的安全，提供恶意软件传播轨迹，快速发现内网中曾经错过的攻击。

具备 Firepower 服务的 ASA 防火墙

了解业内首款注重威胁防护的自适应下一代防火墙 (NGFW) 。该款产品专为威胁和高级恶意软件防护的新纪元而设计。具备 FirePOWER 服务的 Cisco® ASA 防火墙可在攻击前、攻击中和攻击后的整个攻击过程中提供集成的威胁防御。为什么呢？将 Cisco ASA 防火墙经验证的安全功能与业界领先的 Sourcefire® 威胁和高级恶意软件防护 (AMP) 功能结合到单个设备中。该解决方案独创性地扩展了 Cisco ASA 5500-X 系列下一代防火墙的功能，远非目前其他 NGFW 解决方案所能企及。无论是小型或中型企业，还是分布式企业或单个数据中心需要保护，具备 FirePOWER 服务的 Cisco® ASA 可以在 NGFW 解决方案中提供所需的规模和环境。

一流的多层防护

具备 FirePower 服务的Cisco ASA 将独特的、注重威胁防护的下一代安全服务带到 Cisco ASA 5500-X系列下一代防火墙及 Cisco ASA 5585-X 自适应安全设备防火墙之中。它可针对已知的高级威胁提供综合防护，包括对针对性恶意软件攻击与持续性恶意软件攻击的防护。CiscoASA是全世界部署最为广泛的企业级状态防火墙。具备 FirePower 服务的 Cisco ASA 具有以下综合功能:

- 站点到站点和远程接入 VPN 以及高级群集可提供高安全性、高性能访问和高可用性，以确保业务连续性。
- 精细的应用可视性与可控性 (AVC) 支持超过 4000 项基于应用层和风险的控制，这些控制可调用定制的入侵防御系统 (IPS) 威胁检测策略，从而优化安全效力。
- 业内领先的具备 FirePOWER 下一代 IPS(NGIPS) 的 Cisco ASA 可提供高效的威胁防护以及对用户、基础设施、应用及内容的完全情景感知，从而能够检测多途径威胁并实现防御响应的自动化。
- 基于信誉和类别的 URL 过滤功能可提供针对可疑网络流量的综合报警和控制功能，并可对超过80个种类中的数亿个 URL 执行策略。
- AMP 可提供业内领先的漏洞检测效力、低总拥有成本及一流的保护价值，从而帮助您发现、了解并制止其他安全层遗漏的恶意软件和新兴威胁。

具备 FirePOWER 服务的 Cisco ASA： 关键安全功能

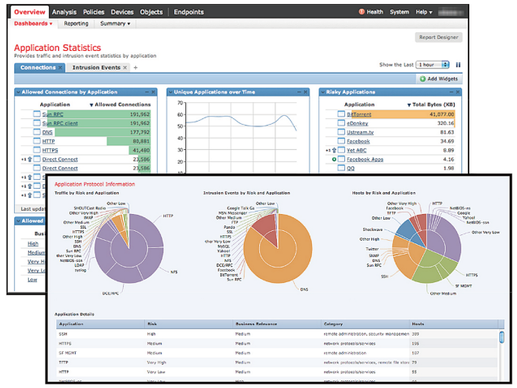
前所未有的网络可视性

具备 FirePOWER 服务的 Cisco ASA 防火墙可通过 Cisco Firepower Management Center (以前叫 FireSIGHT Management Center)管理中心进行集中管理，可为安全团队提供对网络中活动的全面可视性与可控性。此类可视性包括用户、设备、虚拟机之间的通信、漏洞、威胁、客户端应用、文件和网站。整体的可执行危害表现 (IoC) 与详细的网络和终端设备事件信息相关联，可提供针对恶意软件感染的进一步可视性。通过对整个 NGFW 部署无可匹敌的可视性与可控性，思科的企业级管理工具可帮助管理员降低复杂性。Cisco Firepower Management Center 管理中心还可提供包含恶意软件文件轨迹的内容感知功能，可帮助确定感染范围并确定根本原因，从而加快补救速度。

思科安全管理器可提供可扩展的集中网络运营工作流管理。在使用 Cisco Firepower Management Center 管理中心时，该管理器集成了一整套强大的功能，包括策略和对象管理、事件管理、报告以及针对 Cisco ASA 防火墙功能的故障排除。

对于包括中小型企业部署的本地 On-Device 管理，思科自适应安全设备管理器 (ASDM) 7.3.x 提供访问控制和高级威胁防御管理。ASDM V 7.3.x 提供了增强型用户界面，可快速查看相关趋势并可细分以进行进一步分析。

Cisco Firepower Management Center 管理中心：直观的概括性控制面板和详细的细分控制面板



更低的成本和复杂性

具备 FirePOWER 服务的 Cisco ASA 采用集成的防范进行威胁防御，从而降低了资本和运营成本以及管理复杂性。它可以流畅地与现有 IT 环境、工作流和网络交换矩阵相集成。该设备系列具有高度可扩展性，最高速度可达多千兆，并能在物理和虚拟环境中的分支机构、互联网边缘和数据中心之间实现统一、强劲的安全防护。

借助 Cisco Firepower Management Center 管理中心，管理员可简化运营，以关联威胁、评估其影响、自动化调整安全策略并轻松地将用户身份归于安全事件。Cisco Firepower Management Center 管理中心可持续监控网络的实时变化。它能够自动评估新威胁，以确定哪些威胁会对您的企业造成影响。然后，它能够重点围绕补救做出响应，并根据威胁变化的状况改变网络防御措施。它还能自动执行策略调整等关键安全活动，为您节省时间和精力，并确保防御和应对措施始终处于最佳状态。

Cisco Firepower Management Center 管理中心可通过 eStreamer API 轻松地与第三方安全解决方案相集成，从而简化运营工作流并匹配现有的网络交换矩阵。

具备 FirePOWER 服务的 Cisco ASA 的功能和优势

功能	优势
下一代防火墙	业内首款以对抗威胁为中心的 NGFW；可通过单个设备提供 ASA 防火墙功能、高级威胁防护及高级漏洞检测与补救。
久经验证的 ASA 防火墙	借助 Cisco AnyConnect® VPN 丰富的路由、状态化防火墙、网络地址转换及动态群集，实现高性能、高度安全性和可靠的接入
市场领先 NGIPS	针对已知及未知威胁提供一流的威胁防御和减缓功能
高级恶意软件防护	实施检测、阻止、跟踪、分析并补救，以保护企业免于遭受针对性恶意软件攻击和持续性恶意软件攻击
完全情景感知	基于对用户、移动设备、客户端应用、虚拟机间的通信、漏洞、威胁及 URL 的完整可视性进行策略执行
应用控制与 URL 过滤	可（针对应用、地理位置、用户、网站）进行应用层控制，且能够基于定制应用和 URL 执行使用策略并定制检测策略
企业级管理	可针对已发现的主机、应用、威胁及危害表现，提供控制面板和详细报告，从而实现综合可视性
简化的运营自动化	通过威胁关联、影响评估、安全策略自动调整及用户识别，降低运营成本和管理复杂性
针对特定用途、可扩展	采用高度可扩展且最高速度可达多千兆的安全设备架构；物理和虚拟环境中的小型办公场所、分支机构、互联网边缘和数据中心之间可实现统一、强劲的安全防护
On-Device 管理	通过小规模的部署，帮助中小型企业简化高级威胁防御管理工作

远程接入 VPN	它可将企业手提电脑之外的安全企业网络访问扩展到个人移动设备，无论身在何处；支持 Cisco AnyConnect 安全移动解决方案，其中包含细化的应用级别 VPN 功能以及本地 Apple iOS 和 Android VPN 客户端
站点到站点 VPN	保护整个分布式企业和分支机构的通信，包括 VoIP 和客户端服务器应用数据
集成无线接入	集成 Wi-Fi 可用于桌面设备外形 (ASA 5506W-X)，适合在紧凑型和简化型小型办公场所进行部署
坚固型外形	经过特殊设计的坚固型模型 (ASA 5506H-X) 适合在极端环境条件下使用，并且可用于重要基础设施和控制网络应用
第三方技术生态系统	采用开放式 API，支持第三方技术生态系统与现有客户工作流相集成
与 Snort 和 OpenAppID 的集成	针对社区资源接入，与 Snort 和 OpenAppID 进行开放源安全集成，且能够轻松定制安全策略，以快速处理新的特定威胁和应用
综合安全情报 (CSI)	无与伦比的安全和网络信誉情报提供实时的威胁情报和安全防护

产品性能和规格

具备 FirePOWER 服务的 Cisco ASA 5500-X

功能	具备 FirePOWER 服务的 Cisco ASA 5506-X	具备 FirePOWER 服务的 Cisco ASA 5506W-X	具备 FirePOWER 服务的 Cisco ASA 5506H-X	具备 FirePOWER 服务的 Cisco ASA 5508-X	具备 FirePOWER 服务的 Cisco ASA 5516-X	具备 FirePOWER 服务的 Cisco ASA 5525-X	具备 FirePOWER 服务的 Cisco ASA 5545-X	具备FirePOWER 服务的Cisco ASA 5555-X
最大应用控制 (AVC) 吞吐量	250 Mbps	250 Mbps	250 Mbps	450 Mbps	850 Mbps	1,100 Mbps	1,500 Mbps	1,750 Mbps
最大应用控制 (AVC) 和 NGIPS 吞吐量	125 Mbps	125 Mbps	125 Mbps	250 Mbps	600 Mbps	650 Mbps	1,000 Mbps	1,250 Mbps
最大并发会话数	20000; 50000	20000; 50000	50000	100000	250000	500000	750000	1000000
每秒最大新连接数	5000	5000	5000	10000	20000	20000	30000	50000
支持的应用	3000 以上							
URL 类别	80+							
归类的 URL 数量	2.8 亿以上							
集中配置、登录、监控和报告	多设备思科安全管理器 (CSM) 和 Cisco Firepower Management Center 管理中心							
On-Device管理	ASDM 7.3 以上					ASDM		

Cisco ASA 5500-X 系列下一代防火墙

功能	具备 FirePOWER 服务的 Cisco ASA 5506-X	具备FirePOWER 服务的Cisco ASA 5506W-X	具备 FirePOWER 服务的 Cisco ASA 5506H-X	具备FirePOWER 服务的Cisco ASA 5508-X	具备FirePOWER 服务的Cisco ASA 5516-X	具备FirePOWER 服务的Cisco ASA 5525-X	具备FirePOWER 服务的Cisco ASA 5545-X	具备FirePOWER 服务的Cisco ASA 5555-X
状态检测吞吐量（最大1）	750 Mbps	750 Mbps	750 Mbps	1 Gbps	1.8 Gbps	2 Gbps	3 Gbps	4 Gbps
状态检测吞吐量（多协议2）	300 Mbps	300 Mbps	300 Mbps	500 Mbps	900 Mbps	1 Gbps	1.5 Gbps	2 Gbps
三重数据加密标准/高级加密标准(3D ES/AES) VPN 吞吐量	100 Mbps	100 Mbps	100 Mbps	175 Mbps	250 Mbps	300 Mbps	400 Mbps	700 Mbps
用户/节点	不限	不限	不限	不限	不限	不限	不限	不限
IPsec VPN 对等点	10; 50	50	50	100	300	750	2500	5000
思科云网络安全用户	275	275	275	565	2000	4000	5000	6000
Cisco AnyConnect 高级版/Apex VPN 对等点 (已包含; 最大	50	50	50	100	300	750	2500	5000
虚拟接口 (VLAN)	5; 30	5; 30	30	50	100	200	300	500
安全情境（已包含；最大）	不适用	不适用	不适用	2; 5	2; 5	2; 20	2; 50	2; 100
高可用性	需要Security Plus许可证；主用/备用	需要Security Plus许可证；主用/备用	主用/备用	主用/主用和主用/备用	主用/主用和主用/备用	主用/主用和主用/备用	主用/主用和主用/备用	主用/主用和主用/备用
集成无线Access Point	不适用	无线 a/b/g/n, 无线n最大支持 54Mbps 吞吐量	不适用	不适用	不适用	不适用	不适用	不适用
扩展槽	不适用	不适用	不适用	不适用	不适用	1 个接口卡	1 个接口卡	1 个接口卡
用户可访问的闪存插槽	否	否	否	否	否	0	-	0
USB 2.0 端口	USB端口类型“A”, 高速 2.0	USB端口类型“A”, 高速 2.0	USB端口类型“A”, 高速 2.0	USB端口类型“A”, 高速 2.0	USB端口类型“A”, 高速 2.0	2	2	2
集成 I/O	8个1GB以太网(GE)	8 x 1GE	4 x 1GE	8 x 1GE	8 x 1GE	8 GE 铜缆	8 GE 铜缆	8 GE 铜缆
扩展 I/O	不适用	不适用	不适用	不适用	不适用	6 GE 铜缆或 6 GE SFP	6 GE 铜缆或 6 GE SFP	6 GE 铜缆或 6 GE SFP
专用管理端口	是(将与 FirePOWER 服务共享），10/100/1000	是(将与 FirePOWER 服务共享），10/100/1000	是(将与 FirePOWER 服务共享），10/100/1000Base-T, 100Base-FX, 1000Base-X	是(将与 FirePOWER 服务共享），10/100/1000	是(将与 FirePOWER 服务共享），10/100/1000	是（1 GE）	是（1 GE）	是（1 GE）

思科网络安全解决方案综述

Firepower 2100/4100/9300 系列下一代防火墙

Cisco Firepower 2100/4100/9300 NGFW 设备使用 Cisco Firepower 威胁防御软件映像。这些设备还可以支持思科自适应安全设备 (ASA) 软件映像。Cisco Firepower 管理中心（原来的 Firepower Management Center）提供 Cisco Firepower NGFW 以及 Cisco Firepower NGIPS 和思科 AMP 的统一管理。此外，优选 Cisco Firepower 设备
上还提供直接源自思科的 Radware DefensePro 分布式拒绝服务 (DDoS) 缓解功能。

Cisco Firepower 2100 系列设备

Cisco Firepower 2100 系列包括四个专注于威胁防御的 NGFW 安全平台，可持续提供高级威胁卓越的防御性能。通过独立的多核CPU架构可以同时提供优化的状态防火墙、加解密以及威胁检测功能。其最大吞吐量从 1.9 Gbps 到 8.5 Gbps 以上，可应对从互联网边缘到数据中心等各种使用案例。

Cisco Firepower 4100 系列设备

Cisco Firepower 4100 系列包括四个专注于威胁防御的 NGFW 安全平台。其最大吞吐量从 35 Gbps 到 75 Gbps 以上，可应对从互联网边缘到数据中心等各种使用案例。它们可提供卓越的威胁防御能力以及更快的响应速度，同时占用空间却更小。

Cisco Firepower 9300 设备

Cisco Firepower 9300 是可扩展（超过 1 Tbps）运营商级模块化平台，专为要求低（少于 5 微秒分流）延迟和超大吞吐量的运营商、高性能计算中心、数据中心、园区、高频交易环境等打造。Cisco Firepower 9300 通过 RESTful API 实现分流、可编程的安全服务协调和管理。此外，它还可用于兼容 NEBS 的配置中。

性能规范和功能亮点

通过 Firepower 威胁防御映像实现的性能规范和功能亮点

功能	Cisco Firepower 型号											
	2110	2120	2130	2140	4110	4120	4140	4150	带 1 个 SM-24 模块的 9300	带 1 个 SM-36 模块的 9300	带 1 个 SM-44 模块的 9300	带 3 个集群 SM-44 模块的 9300
最大吞吐量：FW + AVC	2.0Gbps	3Gbps	4.75Gbps	8.5Gbps	12 Gbps	20 Gbps	25 Gbps	30 Gbps	30 Gbps	42 Gbps	54 Gbps	135 Gbps
最大吞吐量：AVC + IPS	2.0Gbps	3Gbps	4.75Gbps	8.5Gbps	10 Gbps	15 Gbps	20 Gbps	24 Gbps	24 Gbps	34 Gbps	53 Gbps	133 Gbps
最大并发会话，带 AVC	100万	120万	200万	300万	900万	1500万	2500万	3000万	3000万	3000万	3000万	6000万
每秒最大新连接数，带 AVC	12,000	16,000	24,000	40,000	68,000	120,000	160,000	200,000	120,000	160,000	300,000	900,000
应用可视性与可控性 (AVC)	标准，支持 4000 多个应用，以及地理定位、用户和网站											
AVC：为自定义开放源码应用检测器提供 OpenAppID 支持	标准											
思科安全情报	标准，具有 IP、URL 和 DNS 威胁情报											
Cisco Firepower NGIPS	适用；可以被动检测终端和基础设施以获得威胁关联和危害表现 (IoC) 情报											
面向网络的思科 AMP	适用；可以检测、阻止、跟踪、分析和遏制有针对性和持续性的恶意软件，轻松应对攻击中和攻击后整个攻击过程。也可以选择将威胁关联与面向终端的思科 AMP 集成											
思科 AMP Threat Grid 沙盒	可用											
URL 过滤：类别	80 以上											
URL 过滤：按 URL 分类	2.8 亿以上											

自动化威胁源和 IPS 签名更新	是：源自 Cisco Talos (http://www.cisco.com/c/en/us/products/security/talos.html) 的业内领先的综合安全情报 (CSI)
第三方和开放源生态系统	与第三方产品集成的开放式 API；面向新威胁和特定威胁的 Snort® 和 OpenAppID 社区资源
集中管理	Firepower 管理中心执行集中配置、日志记录、监控和报告
高可用性和集群	主用/备用；还支持 Cisco Firepower 9300 机箱内部集群
VLAN - 最大	1024

Cisco Firepower 2100/4100/9300 设备运行 ASA 映像时的性能和功能。

Cisco Firepower 型号												
功能	2110	2120	2130	2140	4110	4120	4140	4150	带1个 SM-24 模块的 9300	带1个 SM-36 模块的 9300	带1个 SM-44 模块的 9300	带3个 SM-44 模块的 9300
状态检测防火墙吞吐量（最大值）	3 Gbps	6 Gbps	10Gbps	20 Gbps	35 Gbps	60 Gbps	70Gbps	75 Gbps	75 Gbps	80 Gbps	80 Gbps	234 Gbps
状态检测防火墙吞吐量（多协议）	1.5 Gbps	3 Gbps	5 Gbps	10 Gbps	15 Gbps	39 Gbps	40 Gbps	50 Gbps	50 Gbps	60 Gbps	60 Gbps	130 Gbps
并发防火墙连接数	100万	150万	200万	300 万	1000万	1500万	2500万	3500 万	5500万	6000万	6000万	7000万
防火墙延迟 (UDP 64b, 微秒)	NA	NA	NA	NA	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5
每秒新连接数	18,000	28,000	40,000	75,000	150,000	250,000	350,000	800,000	800,000	1200,000	1800,000	4000,000
IPSEC VPN 吞吐量	500Mbps	700Mbps	1 Gbps	2 Gbps	8 Gbps	10 Gbps	14 Gbps	15 Gbps	15 Gbps	18 Gbps	20 Gbps	60 Gbps
IPsec/Cisco AnyConnect/ Apex 站点间 VPN 对等点数	1,500	3,500	7,500	10,000	10,000	15,000	20,000	20,000	20,000	20,000	20,000	60,000
VLAN 的最大数量	400	600	750	1024	1024	1024	1024	1024	1024	1024	1024	1024
安全情景 (包括；最大值)	2；25	2；25	2；30	2；40	10；250	10；250	10；250	10；250	10；250	10；250	10；250	10；250
高可用性	VPN 集群和负载均衡、机箱间集群	VPN 集群和负载均衡、机箱间集群	VPN 集群和负载均衡、机箱间集群	VPN 集群和负载均衡、机箱间集群	主用/主用和主用/备用	主用/主用和主用/备用	主用/主用和主用/备用	主用/主用和主用/备用	主用/主用和主用/备用	主用/主用和主用/备用	主用/主用和主用/备用	主用/主用和主用/备用
集群	NA	NA	NA	NA	最多 16 个设备	最多 16 个设备	最多 16 个设备	最多 16 个设备	最多 5 个设备，每个设备有 3 个安全模块	最多 5 个设备，每个设备有 3 个安全模块	最多 5 个设备，每个设备有 3 个安全模块	最多 5 个设备，每个设备有 3 个安全模块
可扩展性	VPN 集群	VPN 集群	VPN 集群和负载均衡、机箱间集群	VPN 集群和负载均衡、机箱间集群	VPN 集群和负载均衡、机箱间集群	VPN 集群和负载均衡、机箱间集群	VPN 集群和负载均衡、机箱间集群	VPN 集群和负载均衡、机箱间集群	VPN 集群和负载均衡、机箱内部集群、机箱间集群	VPN 集群和负载均衡、机箱内部集群、机箱间集群	VPN 集群和负载均衡、机箱内	VPN 集群和负载均衡、机箱内部集群、机箱间集群

硬件规格

Cisco Firepower 2100 系列硬件规格

Cisco Firepower 型号				
功能	2110	2120	2130	2140
尺寸（长 x 宽 x 高）	1.73 x 16.90 x 19.76 英寸（4.4 x 42.9 x 50.2 厘米）			
外形（机架单元）	1RU			
安全模块插槽数	不适用			
I/O 模块插槽数	不适用		1	
集成I/O	12 个 10/100/1000 Base-T以太网铜缆端口，4个1G SFP以太网光口		12 个 10/100/1000 Base-T以太网铜缆端口，4个10G SFP+以太网光口	
网络模块数	不适用		8 个 10 千兆以太网增强型小型封装热插拔 (SFP+) 网络模块	
最大接口数	最多 16 个千兆以太网接口（12 x 1G RJ-45，4 x 1G SFP）		最多 24 个千兆以太网接口（12 x 1G RJ-45，4 x 10G SFP+，8 x 10G SFP+）	
集成网络管理端口数	最多 24 个 10 千兆以太网 (SFP+) 接口；最多 8 个 40 千兆位以太网接口 (QSFP+) 接口，带 2 个网络模块			
串行端口	1 个 RJ-45 控制台			
USB	1 个 USB 2.0 （500mA）			
存储	1 X 100 GB，1个MSP扩展模块	1 X 100 GB，1个MSP扩展模块	1 X 200 GB，1个MSP扩展模块	1 X 200 GB，1个MSP扩展模块

硬件规格

Cisco Firepower 4100 系列硬件规格

Cisco Firepower 型号				
功能	4110	4120	4140	4150
尺寸（长 x 宽 x 高）	1.75 x 16.89 x 29.7 英寸（4.4 x 42.9 x 75.4 厘米）			
外形（机架单元）	1RU			
安全模块插槽数	不适用			
I/O 模块插槽数	2			
管理引擎	Cisco Firepower 4000 管理引擎，包含 8 个 10 千兆以太网端口和 2 个用于 I/O 扩展的网络模块 (NM) 插槽			
网络模块数	• 8 个 10 千兆以太网增强型小型封装热插拔 (SFP+) 网络模块 • 4 个 40 千兆以太网四通道 SFP+ 网络模块 • 8 个 千兆同轴，FTW (fail to wire) 网络模块			
最大接口数	最多 24 个 10 千兆以太网 (SFP+) 接口；最多 8 个 40 千兆位以太网接口 (QSFP+) 接口，带 2 个网络模块			
集成网络管理端口数	1 个千兆以太网铜缆端口			
串行端口	1 个 RJ-45 控制台			
USB	1 个 USB 2.0			
存储	200 GB	200 GB	400 GB	400 GB

Cisco Firepower 9300 硬件规格

Cisco Firepower 型号	
尺寸（长 x 宽 x 高）	5.25 x 17.5 x 32 英寸（13.3 x 44.5 x 81.3 厘米）
外形	3 个支架单元 (3RU)，适用于标准的 19 英寸（48.3 厘米）方孔机架
安全模块插槽数	3
网络模块插槽数	2 个（在管理引擎内）
管理引擎	Cisco Firepower 9000 管理引擎，包含 8 个 10 千兆以太网端口和 2 个用于 I/O 扩展的网络模块插槽
安全模块数	• RAID-1 配置下，Cisco Firepower 9000 安全模块 24，带有 2 个 SSD • RAID-1 配置下，Cisco Firepower 9000 安全模块 36，带有 2 个 SSD
网络模块数	• 8 个 10 千兆以太网增强型小型封装热插拔 (SFP+) 网络模块 • 4 个 40 千兆以太网四通道 SFP+ 网络模块 • 2 个 100 千兆以太网四通道 SFP28 网络模块（双宽度，占用两个网络模块槽位）
最大接口数	最多 24 个 10 千兆以太网 (SFP+) 接口；最多 8 个 40 千兆位以太网接口 (QSFP+) 接口，带 2 个网络模块
集成网络管理端口数	1 个千兆以太网铜缆端口（在管理引擎中）
串行端口	1 个 RJ-45 控制台
USB	1 个 USB 2.0

Radware DefensePro DDoS 攻击缓解

目前，在Cisco Firepower 4100 和 9300 上，思科直接提供和支持 Radware DefensePro DDoS 攻击缓解功能。Radware 的 DefensePro DDoS 攻击缓解功能是屡获殊荣的实时边界攻击缓解解决方案，可保护组织不受到新出现的网络和应用威胁攻击。它可以保护应用基础设施不会发生网络和应用中断（或者减速），帮助组织防范可用性攻击，持续打赢安全保卫战。

系统检测并缓解了以下攻击：

- SYN 泛洪攻击
- 网络 DDoS 攻击，包括 IP 泛洪、ICMP 泛洪、TCP 泛洪、UDP 泛洪和 IGMP 泛洪
- 应用 DDoS 攻击，包括 HTTP 泛洪和 DNS 查询泛洪
- 异常泛洪攻击，例如非标准和畸形数据包攻击

Radware DDoS 攻击缓解：保护集

Radware DDoS 攻击缓解包含受专利保护的、基于行为的自适应实时签名技术，该技术实时检测和缓解零日网络和应用DDoS攻击。它消除了人为干预的需求，在受到攻击时不阻止合法用户流量。

思科网络安全解决方案综述

Cisco® Catalyst® 6500/6800 系列 ASA-SM 模块

Cisco®Catalyst® 6500/6800 系列 ASA-SM 模块提供了能够与 Cisco Catalyst 65006500/6800 系列交换机无缝集成的出色技术，可为客户带来卓越的安全性、可靠性。基于 Cisco ASA 平台（业内使用最广泛的防火墙）的ASA-SM模块，通过刀片式架构满足当前用户不断增长的处理性能需求。

ASA-SM 模块有助于轻松的在现有网络基础设施中添加完善的防火墙能力，只需将 ASA-SM 模块插入当前 Catalyst 6500/6800 系列交换机中的一个空插槽中即可，无需额外的机架空间、线缆、电源或物理接口。此外，它还能够与机箱内的其它模块协同工作，以便在整个机箱内实现更加强大的安全性，并有效提升每个端口的安全性。通过使用现有的基础设施来提供网络安全服务，ASA-SM 模块可提供出色的投资回报，并极大地简化维护和管理。

特性和优势

ASA-SM模块可帮助客户提高网络和应用保护方面的效率。该模块针对 Cisco Catalyst 6500/6800 系列提供了卓越的投资保护，并有助于降低网络的总体拥有成本 – 降低运营成本，同时应对无形的机会成本。该模块可通过下列优势实现这一点：

- **无缝集成**
  ASA-SM 模块可与 Cisco Catalyst 6500/6800 系列交换机无缝集成。只需将 ASA-SM 模块插入当前 Catalyst 6500/6800 系列交换机中的一个空插槽中，即可获得完善的防火墙能力。由于该模块可直接插入到当前交换机的空插槽中，因此无需占用机架空间；所有接口均是虚拟的，所以无需管理物理接口；该模块使用现有交换机接口，无需重新布线。因此，安装和配置所需的时间显著缩短，从而极大地简化安全服务的添加。相反，在现有网络内添加用于防火墙服务的专用设备，需要大量的人力资源和成本。

- **简化维护和管理**
  ASA-SM 模块可与 Catalyst 6500/6800 系列机箱轻松集成，从而与交换机使用相同的接口和管理软件。事实上，该模块可成为交换机的一部分，因此不会增加交换机管理和维护方面的时间、人力和成本。从本质上来说，向现有基础设施添加高性能网络安全服务，比管理和维护独立的安全设备要更加轻松。

- **最低的环境成本**
  作为 Cisco Catalyst 6500/6800 系列交换机完整集成的组件，ASA-SM 模块可利用交换机的电源和散热资源。另外，它的功耗显著低于其它竞争对手的模块解决方案。冗余 ASA-SM 模块可在最小的电源上运行，最大功耗只有 352.8瓦或 8.4安（@42V）。

下表列出了Cisco Catalyst 6500/6800 系列 ASA-SM 模块的关键特性

特性	描述
性能	
最大防火墙吞吐量	20 Gbps
多协议防火墙吞吐量	16 Gbps
并发连接	10,000,000
每秒新建连接数	300,000
虚拟防火墙个数	最大支持250个（需购买license，默认支持2个）
每台交换机支持最大 ASA-SM 模块数	4个
VLAN 数	1000
高可用性	A/A、A/P
NAT 转换	1000万
透明模式 VLAN	16 对
最大安全策略数	2百万

虚拟化安全平台 ASAv

您需要一种既能满足数据中心的部署和性能需求，又能以较低的成本提供企业级安全性的防火墙。思科 ASAv 虚拟设备便是秉持这一理念设计而成。ASAv 具有多种规格和性能级别，可满足您的网络环境、预算条件和不断变化的安全需求。所有型号都可提供经过验证的安全保护，安全性与世界上许多最大型的、最注重安全的企业采用的网络保护相同。ASAv 还可以在不影响安全性的情况下，为您提供利用各种应用和设备所需的可控性和可视性。

功能和优势

面向企业、运营商和数据中心的思科 ASAv 系列虚拟设备可通过以下途径保护关键资产：

- 出色的状态防火墙服务，可为企业提供所需的精细控制，来安全地利用各种应用和设备
- 通过一系列由思科智能运营中心 (SIO) 支持的基于云和基于软件的集成僵尸网络流量过滤器，提供广泛且深入的网络安全保护
- 高性能 VPN 和全天候远程访问
- 能够快速轻松地启用更多安全服务，响应不断变化的需求

思科ASAv5/ASAv10/ASAv30/ASAv50

思科 ASAv5/ASAv10/ASAv30/ASAv50 虚拟设备集合了业界部署最广泛的状态检测防火墙与一套完整的 IPSec 和 SSLVPN 服务，提供不打折扣的全面安全保护。这些设备可提供多种安全服务，并在整个组织内实现一致的安全实施。除了全面的状态检测防火墙功能之外，思科 ASAv5/ASAv10/ASAv30/ASAv50 还具有通过 VPN 提供安全连接的可选功能。

思科 ASAv5/ASAv10/ASAv30/ASAv50 虚拟安全设备是 ASA5500-X 系列的组成部分，该系列采用与其他 ASA 系列防火墙相同的经过验证的安全平台，可提供卓越的性能和无与伦比的运营效率。思科 ASAv5/ASAv10/ASAv30/ASAv50 专用于在虚拟基础设施中实现高效部署，可与多个虚拟交换机配合使用，并实现跨物理和虚拟安全设备的无缝策略实施。思科 ASAv 系列与其他虚拟设备的不同之处在于，它能够使用以下技术将本地流量可视性与深入的全球网络情报相结合，提供端到端网络情报，以满足快速发展的需求：

功能	思科 ASAv5	思科 ASAv10	思科 ASAv30	思科 ASAv50
状态检测吞吐量（最大1）	100 Mbps	1 Gbps	2 Gbps	10 Gbps
状态检测吞吐量（多协议2）	50 Mbps	500 Mbps	1 Gbps	5 Gbps
3DES/AES VPN 吞吐量3	30 Mbps	125 Mbps	1 Gbps	3 Gbps
用户/节点数	不限	不限	不限	不限
IPsec VPN 对等点	50	250	750	10,000
Cisco Cloud Web Security 用户	250	1000	5000	没有测试
高级 AnyConnect VPN 对等端	50	250	750	10,000
并发连接数	100,000	100,000	500,000	2000,000
每秒新连接数	8000	20,000	60,000	120,000
虚拟接口 (VLAN)	25	50	200	1024
安全上下文（包括数/最大数）	不可用	不可用	不可用	不可用
高可用性	主用/备用			
虚拟机支持	VMware ESX/ESXi 5.5, 6.0 KVM Hyper-V: Windows Server 2012 R2 (Not supported for ASAv50)			
vCPU	1	1	4	8
内存	1 GB最小 1.5 GB	2 GB	8 GB	16 GB
磁盘最小容量	8 GB	8 GB	16 GB	16 GB

思科网络安全解决方案综述

虚拟化安全平台 NGFWv

Cisco Firepower NGFWv 可以部署在虚拟化环境，私有云，公有云以及混合云环境，支持 Vmware、KVM、Amazon Web Services（AWS）以及 Microsoft Azure 环境。用户通过部署 NGFWv 可在 SDN 环境中提供快速部署和灵活的业务编排；此外，NFV 的部署也可以有效降低开销。

功能	NGFWv
最大吞吐量: FW + AVC	1.2Gbps
最大吞吐量: AVC + IPS	1.1Gbps
最大并发会话，带 AVC	10万
每秒最大新连接数，带 AVC	10,000
Cisco FDM管理（本地管理）	支持（只支持VMware）
应用可视性与可控性 (AVC)	标准，支持 4000 多个应用，以及地理定位、用户和网站
AVC：为自定义开放源码应用检测器提供 OpenAppID 支持	标准
思科安全情报	标准，具有 IP、URL 和 DNS 威胁情报
Cisco Firepower NGIPS	适用；可以被动检测终端和基础设施以获得威胁关联和危害表现 (IoC) 情报
面向网络的思科 AMP	适用；可以检测、阻止、跟踪、分析和遏制有针对性和持续性的恶意软件，轻松应对攻击中和攻击后整个攻击过程。也可以选择将威胁关联与面向终端的思科 AMP 集成
思科 AMP Threat Grid 沙盒	可用
URL 过滤：类别	80 以上
URL 过滤：按 URL 分类	2.8 亿以上
自动化威胁源和 IPS 签名更新	是：源自 Cisco Talos (http://www.cisco.com/c/en/us/products/security/talos.html)的业内领先的综合安全情报 (CSI)
第三方和开放源生态系统	与第三方产品集成的开放式 API；面向新威胁和特定威胁的 Snort® 和 OpenAppID 社区资源
集中管理	Firepower 管理中心执行集中配置、日志记录、监控和报告
高可用性和集群	主用/备用；ESXi和KVM

Firepower NGFWv虚拟化平台操作系统需求

平台支持	Vmware，KVM，AWA，Azure
最小系统需求：Vmware	4 vCPU 8-GB memory 50-GB disk
最小系统需求：KVM	4 vCPU 8-GB memory 50-GB disk
支持的 AWS 实例	c3.xlarge
支持的 Azure 实例	Standard_D3
管理选项	Firepower Management Center Cisco Defense Orchestrator Firepower Device Manager (VMware)

工业安全设备 ISA3000

产品概述

思科® 工业安全设备是真正的工业设备，基于经验证的企业级安全性提供面向 OT 的保护。

ISA 3000 是一个 DIN 导轨安装式加固型设备，具有四个数据链路，可为最恶劣和最苛刻的工业环境提供最广泛的访问、威胁及应用控制。

ISA 3000 系列秉承了 IE 4000 交换机硬件设计的工业成就，添加了 Cisco ASA 和 SourceFire 软件的经验证的安全性。ISA 3000 可为您的网络现代化项目提供安全保障。它还在不影响工业生产实践的前提下，提供融合 IT 和 OT 安全的可视性。构建该安全设备是为了抵御极端环境、反映工业设计，同时符合整体 IT 网络设计、合规性及性能要求。

对于那些需要使用强化产品的工业以太网的应用情况，ISA 3000 系列是理想选择。具体情况包括公共事业、制造业、能源和流程控制、智能交通系统 (ITS)、石油和天然气野外现场、城市监控项目和采矿业。由于单个设备能够同时跟踪可疑文件传播、线圈设定点、异常流量模式及特权升级，因此安全性和可视性达到空前水平。思科安全网络产品组合的这一工业元素与其他工业级思科解决方案相辅相成，可以让您全面了解本地单元与 IT 世界、外部供应商或承包商活动之间的交互。

ISA 3000 可通过用户友好的机上系统管理员或公司范围内的安全管理进行管理，提供以工业为中心、开箱即用的配置及简化的操作可管理性。这些高度可定制的管理选项使本地操作感知得以简化，IT/OT 安全融合得以提高，进而使工业功能和 IT 功能必然混合。

功能和优势

功能	优势
强大的工业设计	• 专为恶劣的环境和苛刻的温度范围（-40°C 至 70°C）而构建。 • 每个 ISA 3000 都具有共形涂层。 • 针对振动、冲击、浪涌及电气噪音进行了强化。 • 四个 1 千兆以太网上行链路端口提供多个灵活设计选项。（4 个铜质或 2 个铜质/2 个光纤） • 符合有关自动化、ITS 和变电站环境的多种行业规范。 • 提高工业系统和设备的正常运行时间、性能和安全性。 • 紧凑的 DIN 导轨单元设计与工业 LED 功能，使监控更加容易。 • 无风扇、对流冷却，无活动部件，耐久性更强。 • IEEE 1588v2 PTP（支持电源配置文件和默认配置文件）。 • 警报 I/O 用于监控和向外部设备发出信号。（未来版本支持） • SD 卡用于配置备份和启动。（未来版本支持）
方便易用的 GUI 设备管理器	• 设备上的管理功能可使本地感知得到即刻控制。 • 多设备管理可同时处理数百台设备。 • 用户特定访问和控制定制。
流量连续性/保护	• 全“带外遥控”流量绕开铜缆端口。 • 默认被动部署学习模式。 • 可进行软件更新而不损失流量。 • 连接限制可以防止 DOS 产生流量。 • 延迟检测和缓解功能。 • 服务质量策略

功能	优势
经验证的、可扩展的访问控制	• 执行 ISA-95/IEC 62264 细分需求 • 全面状态检测 • 第 2 层和第 3 层防火墙操作模式 • 可下载访问控制列表 • 基于身份的访问控制策略 • 用户/用户组 • 策略型路由 ACL • 扩展 ACL • WebVPN ACL • 动态 ACL • TrustSec ACL
不打折扣的威胁检测	• 经过第三方测试验证的为最有效的威胁检测 • 超过 25,000 个规则，可随时随地提供最广泛的保护 • 数百个以工业为中心的规则。 • 工业设备利用保护规则 • 协议滥用识别 • 保护基于 Web 的控制系统 • 网络行为分析 • 被动设备发现
应用控制	• 所有 DMZ 基础设施的可视性与可控性 • 工业应用的可视性与可控性 • 单个协议命令和值的可视性与可控性
远程访问支持/控制	• 通过 Cisco AnyConnect 执行网络访问控制 • 身份服务引擎支持 • 站点间 VPN • 远程接入 VPN • 无客户端的 SSL VPN 功能 • 思科安全桌面 • 支持 Citrix 和 VMware 无客户端连接
DMZ 基础设施	• DNS 服务 • DHCP 服务 • AAA 支持 • IP 路由

适合工业环境的理想加固型设备

思科工业安全设备 3000 系列提供:

- 从单元和变电站级一直到 ISP 连接的控制访问。
- 灵活的企业级远程访问。
- 提供 DNS 和 DHCP 等基本网络基础设施服务。
- 从交换机、路由器、操作系统、计算基础设施到工业控制系统，对每一个网络和计算级别提供无可比拟的威胁防范。
- 比工业领域中的其他服务提供更多的流量连续性安全级别。
- 为工业和企业领域的每一级应用提供应用可视性与可控性。

Firepower7000/8000 系列下一代入侵防御平台

根据 NSS Labs 的测量结果，Sourcefire FirePOWER 设备为威胁检测效率、检测吞吐量 和价值等方面制定了行业标准。为保持在此领域的领导地位，全新 FirePOWER 8300 设 备在检测吞吐量方面较之市场领先的 8200 系列（最高 60 Gbps）增加了 50%，吞吐量 可堆叠到 120 Gbps 以上!

8000 系列设备建立在灵活的企业安全架构的基础之上，该架构能够运行应对当今不断 变化的威胁形势所需的安全解决方案。这些设备可以作为单独的下一代入侵防御系统 (NGIPS)、下一代防火墙 (NGFW) 或高级恶意软件防护 (AMP) 系统部署。凭借在单一设备上同时运行这些安全解决方案的独特优势，您的安全投资在未来也能发 挥价值。随着您的网络和安全需求发生变化，FirePOWER 架构设施的保护类型也会随 之变化。

与大多数高端安全设备的固定端口配置不同，8000 系列设备采用模块化配置，因此您可 以选择和更改设备的接口数量和类型。8000 系列设备中插入了各种网络模块 (NetMod)， 可用于自定义接口配置来满足您的网络要求。非旁路网络模块（用于被动或出故障时自 动关闭的部署方式）和具有集成式出故障时自动打开/旁路功能的网络模块（用于内嵌式 部署）提供以下选项:

FirePOWER 8000 设备

型号	8350	8360	8370	8390
性能和功能 IPS 吞吐量	15 Gbps	30 Gbps	45 Gbps	60 Gbps
型号吞吐量	30 Gbps	60 Gbps	90 Gbps	120 Gbps
模块化接口	任意组合中最多 7 个模块	任意组合中最多 6个模块	任意组合中最多5个模块	任意组合中最多4个模块
监控接口（可配置的旁路）	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (2) 10 Gbps SR; (2) 10 Gbps LR	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (2) 10 Gbps SR; (2) 10 Gbps LR	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (2) 10 Gbps SR; (2) 10 Gbps LR	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (2) 10 Gbps SR; (2) 10 Gbps LR
监控接口（非旁路）	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (4) 10 Gbps SR; (4) 10 Gbps LR	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (4) 10 Gbps SR; (4) 10 Gbps LR	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (4) 10 Gbps SR; (4) 10 Gbps LR	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (4) 10 Gbps SR; (4) 10 Gbps LR
管理接口	RJ45	RJ45	RJ45	RJ45
管理接口速度	10/100/1000	10/100/1000	10/100/1000	10/100/1000
一般延迟	小于 150 微秒	小于 150 微秒	小于 150 微秒	小于 150 微秒
内存 (RAM)	128GB	256GB	384 GB	512 GB
无人值守管理	支持	支持	支持	支持
堆叠式	最多可以添加 3 个堆叠套件，堆叠总大小为 4 个 - 60 Gbps IPS	最多可以添加 2 个堆叠套件，堆叠总大小为 4 个 - 60 Gbps IPS	最多可以添加 1 个堆叠套件，堆叠总大小为 4 个 - 有关详情请参阅 8390 任意组合中最多 4 个模块	完全堆叠。无法进一步扩展。
FirePOWER™	**支持**	**支持**	**支持**	**支持**
双电源	**支持**	**支持**	**支持**	**支持**
硬盘驱动器	固态	固态	固态	固态
冷却风扇	6	12	18	24

思科网络安全解决方案综述

FirePOWER 8000 设备

型号	8120	8130	8140
性能和功能			
IPS 吞吐量	2Gbps	4 Gbps	6 Gbps
型号吞吐量	4 Gbps	8 Gbps	10 Gbps
模块化接口	支持 - 任意组合中最多 3 个模块	支持 - 任意组合中最多 3 个模块	支持 - 任意组合中最多 3 个模块
监控接口（可配置的旁路）	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (2) 10 Gbps SR; (2) 10 Gbps LR	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (2) 10 Gbps SR; (2) 10 Gbps LR	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (2) 10 Gbps SR; (2) 10 Gbps LR
监控接口（非旁路）	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (4) 10 Gbps SR; (4) 10 Gbps LR	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (4) 10 Gbps SR; (4) 10 Gbps LR	(4) 1 Gbps 铜缆; (4) 1 Gbps 光纤; (4) 10 Gbps SR; (4) 10 Gbps LR
管理接口	RJ45	RJ45	RJ45
管理接口速度	10/100/1000	10/100/1000	10/100/1000
一般延迟	小于 150 微秒	小于 150 微秒	小于 150 微秒
内存 (RAM)	24GB	24GB	24GB
无人值守管理	支持	支持	支持
堆叠式	否	否	最多可以添加 1 个堆叠套件，堆叠 总大小为 2 个 -12 Gbps IPS
FirePOWER™	支持	支持	支持
双电源	支持	支持	支持
硬盘驱动器	固态	固态	固态
冷却风扇	10	10	10

Firepower 7000 系列

型号	7010	7020	7030	7110	7115	7120	7125
性能和功能							
IPS 吞吐量	50Mbps	100Mbps	250Mbps	500Mbps	750Mbps	1Gbps	1.25Gbps
FirePOWER™	**支持**	支持	支持	支持	**支持**	支持	支持
模块化接口	否	否	否	否	支持-8 SFP插槽	否	支持-8 SFP插槽
监控接口	(8) 1 Gbps 铜缆;	(8) 1 Gbps 铜缆;	(8) 1 Gbps 铜缆;	(8) 1 Gbps 铜缆; 或（8）1Gbps 光纤SR	(12) **共计-**（4） 1 Gbps **铜缆;** （8）SFP**插槽**		(12) 共计-（4） 1 Gbps 铜缆; （8）SFP插槽
可编程的出故障时自动打开的接口	支持	支持	支持	**支持**	支持；（4） 1 Gbps 铜缆	支持	支持；（4） 1 Gbps 铜缆
管理接口	RJ45	RJ45	RJ45	RJ45	RJ45	RJ45	RJ45
管理接口速度	10/100/1000	10/100/1000	10/100/1000	10/100/1000	10/100/1000	10/100/1000	10/100/1000
一般延迟	小于150微秒	小于150微秒	小于150微秒	小于150微秒	小于150微秒	小于150微秒	小于150微秒
内存（RAM ）	4GB	4GB	4GB	16GB	16GB	16GB	16GB
无人值守管理	支持	支持	支持	支持	支持	支持	支持
堆叠式	否	否	否	否	否	否	否
双电源	否	否	否	支持	支持	支持	支持
冷却风扇	2	2	2	5	5	5	5

统一管理平台 Firepower Management Center 管理中心

Cisco Firepower Management Center 管理中心可提供关于网络资源变更和操作变更的被动发现实时信息，从而可为做出明智决策提供完全的情景依据。在选择 Cisco Firepower Management Center 管理中心设备时，应考虑环境中受监控的传感器设备和主机的数量，以及所要分析或存储的预期安全事件。所有配置均可提供以下管理功能：

- 集中的设备、许可证、事件和策略管理
- 基于角色的管理（基于管理员角色或用户组的分段或单独视图及职责）
- 带有定制和基于模板的报告的可定制控制面板
- 针对一般信息和焦点信息的综合报告和报警
- 在超链接表格、图形和图表中显示事件和情景信息
- 网络行为和性能监控
- 稳健的高可用性选项，有助于避免出现单点故障
- 关联和补救功能，可实现实时威胁响应
- 可与第三方解决方案和客户工作流（如防火墙、网络基础设施、日志管理、安全信息和事件管理 [SIEM]、故障通知单和补丁管理）集成的开放式 API
- 除了提供广泛的情报外，Cisco Firepower Management Center 管理中心还可提供深入的详情，包括：
- 趋势和高级统计：帮助经理和高层主管及时了解某个时间点的安全状况及其变化情况（改善或恶化）
- 事件详情、合规性和调查分析：帮助了解整个安全事件过程中发生的所有情况，以便增强防御措施、加强漏洞控制，并为执法和诉讼提供协助
- 工作流：轻松导出数据，以提升事件响应水平，从而改善响应管理

无与伦比的可视性和见解

下表展示了 Cisco Firepower Management Center 管理中心如何针对多数传统安全技术无法检测到的威胁途径，提供全面的情景感知。

Cisco Firepower Management Center 管理中心：完全堆叠可视性

类别	Cisco Firepower Management Center 管理中	典型的 NGIPS	典型的下一代防火墙
威胁	是	是	是
用户	是	是	是
Web 应用	是	否	是
应用协议	是	否	是
文件传输	是	否	是
恶意软件	是	否	否
命令和控制服务器	是	否	否
客户端应用	是	否	否
网络服务器	是	否	否
操作系统	是	否	否
路由器和交换机	是	否	否
移动设备	是	否	否
打印机	是	否	否
VoIP 电话	是	否	否
虚拟机	是	否	否

安全管理自动化，实现动态防御

Cisco Firepower Management Center 管理中心可持续监控网络的实时变化。它能够自动评估新威胁，以确定哪些威胁会对您的企业造成影响。然后，它能够重点围绕补救做出响应，并根据变化的状况，改变网络防御措施。它还能自动执行策略调整等关键安全活动，为您节省时间和精力，并确保防御和应对措施始终处于最佳状态。

部署模式的选择

Cisco Firepower Management Center 管理中心可按物理或虚拟设备方式进行部署。物理部署的 Cisco Firepower Management Center 设备能够支持最大限度的可集中管理的传感器和事件存储。虚拟部署的 Cisco Firepower Management Center 设备能够确保对现有基础设施调配的便利性。它们可通过 VMware vSphere 调配进行轻松部署，并可在 VMware 基础设施内部进行部署，以保护物理网络中的资产。Firepower Management Center 版虚拟设备可在 VMware vSphere，KVM，Amazon Web Services 上托管。

思科网络安全解决方案综述

Cisco Firepower Management Center 管理平台：

性能和功能	FMC 750	FMC 1000	FMC 2000	FMC 2500	FMC 4000	FMC 4500	FMCv
最大可管理设备	10	50	250	300	500	750	25 10 2
最大IPS Events	2000万	6000万	6000万	6000万	30000万	30000万	5000万

高级威胁防御平台

思科 AMP 恶意软件防护平台

针对实际情况的漏洞防御、检测、响应和补救

优点

- 通过无与伦比的全球威胁情报加强一线防御
- 深入了解危害的起源和影响范围
- 快速检测、响应和补救恶意软件
- 避免昂贵的重复感染和补救方案
- 随时随地保护 - 网络、终端、移动设备、电邮、网络 - 攻击前、攻击中和攻击后

当今的高级恶意软件隐蔽、持久并且可规避传统的防御。安全团队面临着如何阻止这些攻击的挑战，因为他们的安全技术并不提供必要的可视性与可控性，所以其无法在损害形成之前快速检测并消除威胁。

组织遭受攻击，安全漏洞总是会占据新闻头条。现今，全球的黑客群体正在不断制作出高级恶意软件并通过各种攻击媒介侵入组织。这种多层面的定向攻击甚至可以规避最佳时间点检测工具。这些工具在网络入口点检查流量和文件，但难以检查出设法规避初始检查的威胁活动。这使得安全专业人员对于潜在危害的影响范围一无所知，无法在恶意软件造成明显损害之前快速响应并对其进行遏制。
思科高级恶意软件防护（AMP）是一个能够解决高级恶意软件整个生命周期问题的安全解决方案。它不但可预防漏洞，还可提供可视性与可控性，从而在威胁规避了一线防御后将其快速检测出并进行遏制和补救 - 所有这些都是具有成本效益的且不会影响运营效率。

思科高级恶意软件防护概览

AMP是情报驱动的、集成式企业级高级恶意软件分析和保护解决方案。您可以在攻击整个过程（攻击前、攻击中和攻击后）中为组织获取全面的保护。

- 攻击前，AMP使用来自思科综合安全情报的全球威胁情报、Talos 安全情报和研究小组以及 AMP Threat Grid 的威胁情报源，来加强防御并防范已知和新兴的威胁。

- 攻击中，AMP 结合使用情报和已知文件签名，以及 Cisco AMP Threat Grid 的动态恶意软件分析技术，来识别并阻止违反策略的文件类型、漏洞尝试及尝试渗入网络的恶意文件。

- 攻击后，或者，文件最初检查之后，该解决方案将超越时间点检测功能（即进行不止一次的检测）并持续监控和分析所有文件活动和流量（无论如何处置），以搜索任何恶意行为的迹象。如果未知或之前被视为“良性”处置的文件开始出现不良行为，AMP 将对其进行检测并立即向安全团队发出警报，提示出现危害迹象。然后，它会提供卓越的可视性，以供深入了解恶意软件的起源、受影响的系统以及恶意软件正在执行的操作。它还提供各种控件，以便迅速响应入侵，并且只需单击几下即可进行补救。这使得安全团队能够获得所需的深入可视性和可控性，以快速检测出攻击、确定受影响范围并在恶意软件造成损害之前并对其进行遏制。

全球威胁情报和动态恶意软件分析

AMP 的构建基于无与伦比的安全情报和动态恶意软件分析。思科综合安全情报生态系统、Talos 安全情报和研究小组以及 AMP Threat Grid 威胁情报源代表了行业领先的实时威胁情报和大数据分析集合。然后，此数据将从云推送至 AMP 客户端，以便您通过最新的威胁情报，主动防范威胁。组织将获益于：

- 每天110万传入恶意软件示例
- 全球有160万个传感器
- 每天100TB的数据
- 130亿网络请求
- 600位工程师、技术人员和研究人员
- 全天候运行

AMP 对照此强大、情景丰富的知识库关联文件、行为、遥测数据和活动以快速检测恶意软件。安全团队受益于 AMP 的自动化分析，节省了搜索漏洞活动时间并随时拥有最新的威胁情报，可以快速了解、优先处理和阻止复杂的攻击。

我们 Threat Grid 技术与 AMP 相集成，还可以：

- 按照标准格式提供的高度准确和情景丰富的情报源与现有安全技术无缝集成
- 每月对照 350 多个行为指标对数百万示例进行分析，可生成数十亿标样
- 简单易懂的威胁指数，帮助安全团队确定威胁的优先级

AMP 使用所有这些情报和分析告知您安全决策或自动代表您采取措施。例如，借助不断更新的情报，系统可以阻止已知恶意软件和违反策略的文件类型，动态地将已知恶意的连接放入黑名单，并阻止从那些被归类为恶意的网站和域下载文件。

持续分析和追溯性安全

大多数基于网络和终端的防恶意软件系统仅在文件穿过控制点进入您的扩展网络时检查文件。这也是分析终止的地方。但是，恶意软件比较复杂并且擅长规避初始检测。休眠技术、多态、加密和使用未知协议是恶意软件用于遮蔽自身的一些方法。您无法防范您看不到的事物，这也是大多数安全漏洞产生的原因。安全团队在入口点看不到威胁且在事后无视它的存在。他们不具备可供快速检测或遏制威胁的可视性，不久之后，恶意软件实现了目标，损害也已经造成。

CiscoAMP 则不同。AMP 系统认识到时间点、主动检测和拦截方法并不是百分百有效，因此即使通过了初始检测，之后也会持续分析文件和流量。AMP 监控、分析并记录终端、移动设备上以及网络中的所有文件活动和通信，以便快速找到显露出可疑或恶意行为的隐蔽威胁。一旦出现麻烦，AMP 就会通过追溯方式向安全团队发出警报并提供有关威胁行为的详细信息，以便您可以回答重要的安全问题，例如：

- 恶意软件来自何处？
- 进入的方法和进入点是什么？
- 它在何处以及哪些系统受到影响？
- 威胁的目的是什么以及它正在做什么？
- 如何阻止威胁并消除根本原因？

使用此信息，安全团队能够及时了解情况并使用 AMP 的遏制和补救功能采取措施。通过 AMP 中易于使用的、基于浏览器的管理控制台，管理员只需单击几下，即可通过阻止文件在另一个终端上再次执行来遏制恶意软件。而且，由于AMP知晓文件曾经去过的所有地方，因此它可以将文件从内存中去除并将其与所有其他用户隔离。在恶意软件入侵时，安全团队不再需要重新映像整个系统以消除恶意软件。那样做需要耗费时间、资金和资源，并且会中断关键业务功能。采用 AMP 后，恶意软件补救类似一个外科手术，不会对 IT 系统或业务造成相关的间接损害。

这就是持续分析、持续检测和追溯性安全功能的强大所在 - 能够记录系统中每个文件的活动。并且，如果认为“良性”文件变“坏”了，则能够对其进行检测并回退历史记录以查看该威胁的起源和其显露的行为。然后，AMP 会为您提供内置响应和补救功能以消除威胁。AMP 还会记住其所见内容（从威胁的签名到文件的行为），并将这些数据记录在 AMP 的威胁情报数据库中以进一步加强一线防御，因此该文件及类似的文件将无法再次规避初始检测。

现在，安全团队具备了必要的深入可视性和可控性，可以快速、有效地检测攻击并发现隐蔽的恶意软件；了解并确定受影响范围；在恶意软件（甚至是零日攻击）造成任何损害之前快速将其遏制并补救；并防止类似的攻击发生。

主要特性

AMP的持续分析和追溯性安全功能的实现皆是因为以下这些强大特性：

- 危害表现(IoC)：文件和遥测事件进行关联并作为潜在活动漏洞优先处理。AMP 可自动关联多个来源的安全事件数据（例如入侵与恶意软件事件），以帮助安全团队将事件关联到更大规模的协同攻击并优先处理高风险事件。
- 文件信誉：高级分析和综合情报相结合，以确定文件是安全还是具有恶意，从而进行更为准确的检测。
- 动态恶意软件分析：高度安全的环境可帮助您执行、分析和测试恶意软件，以发现之前未知的零日威胁。AMP解决方案中集成了 AMP Threat Grid 的沙盒与动态恶意软件分析技术，因此可以根据更大的一组行为指标进行更为全面的分析。
- 追溯性检测：如果文件处置在扩展分析之后发生了变化，AMP 会发出相关警报，以便您知晓并了解规避了初始防御的恶意软件。
- 文件轨迹：文件在您环境中的传播会随着时间推移得到持续跟踪，以实现可视性并缩短确定恶意软件影响范围的时间。
- 设备轨迹：持续跟踪设备上和系统级的活动和通信，以在损害后快速了解导致损害的根本原因以及事件历史记录。
- 弹性搜索：跨文件、遥测以及综合安全情报数据的简单无界搜索可帮助您快速了解暴露给IoC或恶意应用的上下文和范围。
- 感染率：显示组织内已执行的所有文件，并按感染率从最低到最高排序，以帮助您发现之前未检测到但被少量用户看到的威胁。您可能不希望自己的扩展网络上存在只有少数用户执行但可能具有恶意的文件（例如一个定向高级持续威胁）或可疑应用。
- 终端IoC：用户可以提交其自己的IoC以捕捉定位攻击。这些终端IoC允许安全团队对特定于其环境中应用的鲜为人知的高级威胁执行更为深入调查。
- 漏洞：显示列出您系统上存在漏洞的软件、包含该软件的主机以及最可能受到损害的主机的列表。凭借我们的威胁情报和安全分析，AMP可识别易受恶意软件攻击的软件和潜在的漏洞，为您提供按优先顺序排列的需要修补的主机列表。
- 爆发控制：实现对可疑文件或爆发的掌控，无需等待内容更新即可修复感染。
- 在爆发控制功能中：
  - 简单自定义检测可以跨所有或选定系统，快速阻止特定文件
  - 高级自定义签名可以阻止多态恶意软件系列
  - 应用阻止列表可以强制执行应用策略或遏制受危害应用用作恶意软件网关并终止再次感染循环
  - 自定义白名单，有助于确保安全、自定义或关键任务型应用无论如何都可继续运行
  - 设备流关联将在源头阻止恶意软件回调通信，尤其针对公司网络之外的远程终端

部署选项让保护无处不在

网络犯罪分子通过各种入口点向组织发起攻击。为了真正有效地捕获隐蔽攻击，组织需要尽可能多地了解各种攻击媒介。因此，AMP 解决方案可部署在整个扩展网络中的不同控制点。组织可以按照满足自身特定安全需求的方式在所需地点部署此解决方案。选项包括：

产品名称	
面向终端的 Cisco AMP	使用 AMP 的轻型连接器保护 PC、Mac、移动设备和虚拟环境，对用户的性能不会产生任何影响。
面向网络的 Cisco AMP	部署 AMP 作为与 Cisco FirePOWER™ NGIPS 安全设备集成的基于网络的解决方案。
FirePower平台和具有 FirePOWER 服务的 ASA 上的 Cisco AMP	部署集成到 Cisco FirePower和 ASA 防火墙中的 AMP 功能。
Cisco AMP 私有云虚拟设备	部署 AMP 作为本地气隙解决方案，专门针对具有限制使用公共云的高隐私要求的组织。
CWS、ESA 或 WSA 上的 Cisco AMP	对于思科云网络安全 (CWS)，电邮安全设备 (ESA) 或网络安全设备 (WSA) 而言，可以启用 AMP 功能以提供追溯功能和恶意软件分析。
Cisco Meraki MX上的AMP	在Meraki MX安全网关上部署AMP，可以在云端安全管理平台上启用高级恶意威胁防御能力。
Cisco AMP Threat Grid	AMP Threat Grid 与 Cisco AMP 集成，提供增强的动态恶意软件分析。它还可以部署为独立动态恶意软件分析和威胁情报解决方案。

Threat Grid 恶意软件分析平台

为了对抗恶意软件和高级威胁，您必须拥有最佳安全工具。思科® 高级恶意软件防护 (AMP) Threat Grid 设备在单个设备中集成了两种领先的恶意软件防护解决方案：统一恶意软件分析和情景丰富的情报。借助该产品，安全专业人员可以主动防御网络攻击并实现快速恢复。

产品概述

AMP Threat Grid 设备可提供内部部署高级恶意软件分析功能，其中包含深度的威胁分析和丰富的内容。它支持组织上传恶意软件样本，从而有助于组织实现合规性并遵循政策限制。来自 AMP Threat Grid 的联合数据会形成单向连续数据流，可在提供所需恶意软件防护的同时，帮助确保遵守组织要求。

通过 AMP Threat Grid 设备，您可以使用高度安全的专有静态和动态分析技术来分析任何样本。它将结果与上百万个其他经分析的恶意软件人为因素相关联，从而全面地了解恶意软件攻击、活动及其分布的相关信息。安全团队可以对照其他上百万个样本，快速地关联所观察到的活动和特征的单个样本，以便透过历史和整体情景全面地了解其行为。此功能可帮助您有效抵御针对性攻击和来自高级恶意软件的威胁。AMP Threat Grid 的详细报告（包括已发现的重要行为表现以及威胁分数评分）可帮助您快速确定高级攻击的优先级，并从中恢复。

特性和优势

AMP Threat Grid 设备的特性和优势。

特性	优势
用户处部署设备	提供安全且高度可靠的内部部署静态和动态恶意软件分析功能。能够轻松与现有安全基础设施集成。可为恶意软件分析结果提供安全的用户内部部署存储。
高级分析	提供关于恶意软件行为的全面安全见解，以及与 AMP Threat Grid 庞大数据库中的样本源和相关行为对应的直接链接。支持轻松访问所有信息和分析结果，以进行进一步调查。
高级行为指标	可高度准确且切实有效地分析800多种高级行为表现，而且误判率非常低。通过涵盖大量恶意软件系列和 恶意行为的高级静态和动态分析生成全面的威胁表现。围绕威胁提供最广泛的情景，帮助快速且自信地做出决策。
威胁分数	通过专有分析和算法自动得出威胁分数，其中会综合考虑已观察到的行为的可信度和严重性、历史数据、频率，以及聚类的表现和样本。设备将按可信度确定威胁优先级，以反映每个样本的恶意行为级别。增强威胁优先级的确定，从而为恶意软件分析人员、事件响应人员、安全工程团队以及使用 AMP Threat Grid 数据源的产品提高效率和准确性。
便于集成的 API	利用现有的安全和网络基础设施，简化并快速实现威胁情报的运营化。通过AMPThreat Grid的REST API可实现快速轻松的集成。该设备还提供面向各种第三方产品的集成指南，包括网关、代理，以及安全信息和事件管理 (SIEM) 平台。

全面的内部部署恶意软件分析

对于受合规性和政策限制而无法将样本上传到云端的组织，AMP Threat Grid 可提供专用设备，用于在 AMP Threat Grid 联合威胁情报的全力支持下实现本地恶意软件分析。AMP Threat Grid 可提供有关恶意软件攻击、活动和分布的全局信息。它每月会分析数百万个样本，并生成数TB恶意软件分析信息，形成切实有效且内容丰富情报。

安全团队可以快速参照数百万个其他样本对单个恶意软件样本中观察到的活动和特征进行关联分析，从历史和全局角度全面了解其行为，从而有效地防范针对性攻击和来自高级恶意软件的更广泛威胁。AMP Threat Grid 的详细报告能够识别关键行为威胁表现并给出威胁分数，从而帮助快速而精确地确定高级攻击的优先级，并从中恢复。分析功能包括：

- 可提供对恶意软件行为的全面理解的动态和静态分析引擎
- 有关所有恶意软件样本活动（包括网络流量）的详细分析报告
- 专为安全运营中心 (SOC) 分析人员、恶意软件分析人员和事故
- 调查人员而设计的用户界面工作流程

思科网络安全解决方案综述

Stealthwatch 流量可视与安全平台

StealthWatch® 系统可提供行业领先的网络可视性和安全情报，帮助提高威胁检测、事件响应和调查分析的速度和精确度。

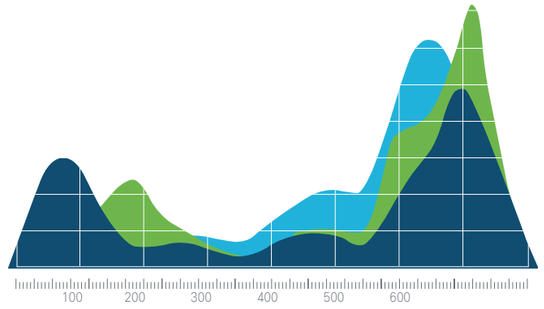
该系统能够利用 Netflow 和现有基础设施中的其他遥感勘测数据，以具有成本效益的方式将整个网络转化为一个传感器网。它能够检测各种异常流量和行为，包括零日恶意软件、分布式拒绝服务 (DDoS) 攻击、内部威胁和高级持久性威胁 (APT)。StealthWatch 的 Web 界面十分直观。它通过单一视图展示流量在网络中的横向移动。而且，它的信息情报和警告功能非常先进。这个简单、精致且功能强大的平台可全面增强可用性、安全分析和早期威胁检测。

优势

通过独特的网络流量视图和分析，StealthWatch 可在以下方面带来显著改善：

- 实时威胁检测
- 事件响应和调查分析
- 网络分段
- 网络性能和容量规划
- 满足监管要求的能力

- 流量组成分解
- 基于 Point-of-ViewTM 技术的可自定义用户界面
- 支持多千兆和大规模多协议标签交换 (MPLS) 网络环境
- 高级流可视化
- 强大的可扩展性
- 合并的内部和外部监控
- 容量规划与历史流量趋势分析
- WAN 优化报告
- 差分服务代码点 (DSCP) 带宽使用
- 蠕虫传播可视化
- 适合高速网络的内部安全功能



StealthWatch Management Console

StealthWatch Management Console 为不同的 IT 组提供单一观测点，用于查看整个网络中所有活动的情景信息。简单的概览界面使操作人员能够快速找到故障并做出适当响应。

控制台的容量决定可以分析和呈现的 Netflow 数据量，以及可部署的 StealthWatch FlowCollector 的数量。控制台可通过硬件设备或虚拟机两种形式提供。
StealthWatch Management Console 的主要功能包括：

- 用户身份跟踪
- 灵活的部署选项，包括虚拟设备
- 快速根本原因分析和故障排除
- 相关流图
- NAT 拼接
- 自定义控制面板
- 自定义报告
- 自动拦截、修复和速率限制
- 应用、服务、端口、协议、主机、对等设备和会话的“主要排名”报告

StealthWatch Management Console 的主要优势

优势	说明
实时更新数据	为同时监控数百个网段上的流量提供数据流，以便您发现可疑的网络行为。此功能在企业层面上尤其重要。
检测安全威胁并确定优先级的功能	通过单一控制中心提供以下能力：快速检测安全威胁并确定优先级、精确查找网络错用行为和性能欠佳之处，以及管理整个企业的事件响应。
网络分组	创建网络分组和关系映射，轻松查看组织的流量状态。运营和安全团队能够在几秒钟内精确找到需要关注的方面。
图形表示	以整洁、易于理解的格式展现网络状态。
快速评估安全状态	在主控制面板上显示多个警报类别，使操作人员能够快速评估组织的安全状态。
StealthWatch 设备管理	配置、协调和管理 StealthWatch 设备，包括 FlowCollector、FlowSensor 和 IDentity 设备
使用多种类型的流数据	使用多种类型的流数据，包括 Netflow、Internet Protocol Flow Information Export (IPFIX) 和 sFlow。这使您能够以具有成本效益的方式获得基于行为的网络保护。
可扩展性	支持最苛刻的网络需求。在速度极高的环境中保持出色表现，并且能够保护可通过IP访问的每个网络部分（无论大小如何）。
交付方法选择	您可以订购 Appliance Edition，这是一款可扩展的设备，适合任何规模的组织。或者，您可以订购 Virtual Edition。此版本可执行与 Appliance Edition 相同的功能，但运行于虚拟环境中。
增强网络管理	通过趋势分析、防火墙和容量规划以及性能监控增强网络管理。
处理 APT、恶意软件和内部威胁	提供防御持续演进的威胁所需要的深入可视性和情景。这包括从蠕虫、病毒和其他恶意软件，到针对性攻击、DDoS 尝试、内部威胁和 APT 在内的所有安全威胁。所提供的信息还包括各种警报，以及安全人员快速采取决定性措施以降低潜在损害所需的情景信息。
网络事务审计跟踪	提供所有网络事务的完整审计跟踪，提高调查分析研究的效率。
实时可自定义关系流图	提供组织流量当前状态的图形视图。管理员可根据位置、功能或虚拟环境等任何标准轻松构建网络图。通过在两组主机之间创建连接，操作人员能够快速分析在它们之间传输的流量。然后，只需选择有问题的数据点，即可更加深入地洞察在任意时间点发生的情况。

StealthWatch Management Console VM 版

型号	支持的 FlowCollector 的最大数量	流存储容量
StealthWatch Management Console VE	最多 5 台	1 TB

StealthWatch Management Console 硬件版规格

型号	处理器	内存	磁盘阵列	硬盘	存储容量	接口		
SMC-2200	2x 2.4 Ghz E52680 v4-cache 14c/35MB	32G DDR4 (16x) 512GB total	RAID-6	8x 1.2TB 10K	7.2TB	X520 dual Fiber port 10G SFP+		

StealthWatch FlowCollector

StealthWatch FlowCollector 跨物理和虚拟环境提供网络可视性和安全情报，帮助提高事件响应能力。
从网络收集的 Netflow 遥感勘测数据量由已部署 FlowCollector 的容量决定。可以安装多个 FlowCollector。FlowCollector 可通过硬件设备或虚拟机两种形式提供。

StealthWatch FlowCollector 的主要优势

优势	说明
更丰富的流情景	从代理服务器采集 URL 和代理用户数据，并将其与对应的网络流数据相关联。
更好的流量可视性	针对经过 Web 代理的指定网络会话，提高 StealthWatch 系统的可视性。
SLIC 威胁源监控	自动将来自代理记录的 URL 数据与 StealthWatch Labs Intelligence Center (SLIC) 威胁源进行比较。
调查支持	人工调查控制台内的数据。
增加精确度	为 StealthWatch 系统提供情景数据，提高安全事件的精度。
关联代理和流数据	从代理服务器采集 URL 和代理用户数据，并将其与对应的网络流数据相关联。系统会自动将这些信息与 SLIC 威胁源进行比较。此外，这些信息也用于为通过控制台手动执行的调查提供支持。
可视性	允许组织查看与代理会话另一端关联的已转换地址，消除网络上的盲点。
威胁检测	采集代理记录并将其与流记录相关联，提供每个流的用户应用和 URL 信息，从而提高情景感知能力。此过程可以增强组织精确找到威胁的能力，缩短平均知道时间 (MTTK)。
应急响应	提供关于流经代理服务器的 Web 流量的附加情景，实现更精确的故障排除、事件响应和调查分析。
实时流量分析	为计费、带宽记帐和网络性能故障排除提供实时流量分析。
流流量监控	同时监控数百个网段上的流流量，这样您就能发现可疑的网络行为。此功能在企业层面上尤其重要。
确定安全问题的根本原因	在几秒钟内隔离根本原因，更快速地响应安全事件。
切实可行的见解	无需成本昂贵的探测，即可提供切实可行的性能分析。
长期数据保留	允许组织和机构长期保留大量的数据。
多种类型的流数据	使用多种类型的流数据（Netflow、IPFIX 和 sFlow），提供具成本效益的、基于行为的网络保护。
可扩展性	在速度极高的环境中保持出色表现，并且能够保护可通过 IP 访问的每个网络部分（无论大小如何）。
重复数据删除与拼接	执行重复数据删除，任何穿过多个路由器的流仅计数一次。然后，可以将流信息拼接在一起以全面了解网络事务。
在分布于不同地区的网络上实现端到端可视性	汇聚来自多个网络或网段的高速网络行为数据，提供端到端保护，改善分布于不同地区网络的性能。
交付方法选择	您可以订购 Appliance Edition，这是一款可扩展的设备，适合任何规模的组织。 或者，您可以订购 Virtual Edition。此版本可执行与 Appliance Edition 相同的功能，但运行于虚拟环境中。该解决方案可以根据所分配资源进行动态扩展。

StealthWatch FlowCollector VM 版

型号	最大每秒Flow数	最大Flow Exporter	流存储
FlowCollector for NetFlow	3,000	1,000	1.0 TB
FlowCollector for sFlow	3,000	1,000	1.0 TB

StealthWatch FlowCollector 硬件版规格（按型号）

型号	处理器	内存	磁盘阵列	硬盘	存储容量	接口
FC-4200	2x 2.4 Ghz E52680 v4-cache 14c/35MB	32GB DDR4 (16x) 512GB total	RAID-6	8x 1.2TB 10K	7.2TB	X520 dual Fiber port 10G SFP+
FC-5200 Engine	2x 2.4 Ghz E52680 v4-cache 14c/35MB	16G DDR4 (16x) 256GB total	RAID-6	6x 300GB 10K	1.2TB	X520 dual Fiber port 10G SFP+
FC-5200 DB	2x 2.4 Ghz E52680 v4-cache 14c/35MB	32GB DDR4 (16x) 512GB total	RAID-10	16x 1.2TB 10K	9.6TB	X520 dual Fiber port 10G SFP+

StealthWatch FlowSensor

FlowSensor 是一个组件，用于为不支持 Netflow 的交换和路由基础设施片段生成 Netflow 数据。它还可以在各种环境下工作，在这些环境中，重叠监控解决方案更加适合IT机构的运营模式。FlowSensor 能够为不启用思科基于网络的应用识别 (NBAR) 的环境提供第 7 层应用信息。

FlowSensor 提供网络和服务器性能指标的全面可视性。它将深度数据包检测 (DPI) 和行为分析结合在一起，识别应用和协议，从而优化安全性、网络运营和应用性能。

从网络生成的 Netflow 数据量由已部署 FlowSensor 的容量决定。可以安装多个 FlowSensor。FlowSensors 可通过硬件设备或监控虚拟机环境的软件两种形式提供。

StealthWatch FlowSensor 的主要功能包括:

- 第7层应用情景
- 流可视性
- Netflow 生成
- 虚拟环境可视性
- 针对当前威胁进行实时更新
- 计算TCP连接的往返时间(RTT)和服务器响应时间(SRT)

StealthWatch FlowSensor 的主要优势

优势	说明
第 7 层应用可视性	通过收集应用信息以及数据包层的性能统计数据，提供真正的第 7 层应用可视性。
数据包层性能和分析	通过收集应用信息以及数据包层的性能统计数据，提供真正的第 7 层应用可视性。
网络异常警报	指出任何异常网络行为并立即发送警报和情景情报，使安全人员能够快速采取行动，降低损害。
降低成本	在几秒内识别和隔离问题或事件的根本原因，提高运营效率，降低成本
交付方法选择	您可以订购 Appliance Edition，这是一款可扩展的设备，适合任何规模的组织。或者，您可以订购 Virtual Edition。此版本可执行与 Appliance Edition 相同的功能，但运行于虚拟环境中。

StealthWatch FlowSensor VM 版

型号	最大网络流量	网络监控接口
Flow Sensor Virtual Appliance	N/A	N/A

思科网络安全解决方案综述

StealthWatch FlowSensor 硬件版规格

型号	处理器	内存	磁盘阵列	硬盘	存储容量	接口
FS-2200	2x 2.2 Ghz E52650 v4-cache 12c/30MB	16G DDR4 (16x) 256GB total	RAID-6	6x 300GB 10K	1.2TB	i350 quad port 1G Copper RJ-45 + I350 dual port Fiber 1G SFP
FS-3200	2x 2.2 Ghz E52650 v4-cache 12c/30MB	16G DDR4 (16x) 256GB total	RAID-6	6x 300GB 10K	1.2TB	X520 dual Fiber port 10G SFP+
FS-4200	2x 2.2 Ghz E52650 v4-cache 12c/30MB	16G DDR4 (16x) 256GB total	RAID-6	6x 300GB 10K	1.2TB	Napatech quad port Fiber 10G SFP+

StealthWatch UDP Director

UDP Director® 可简化在整个企业内收集与分发网络数据和安全数据。通过从多个位置接收重要的网络和安全信息，然后将信息转发到单一数据流并再转发到一个或多个目标，有助于降低网络路由器和交换机的处理压力。

StealthWatch UDP Director 的主要优势

优势	说明
减少意外停机和服务中断	仅在 UDP Director 2000 设备上提供 UDP Director 高可用性。UDP Director 1000 设备不支持 UDP Director 高可用性。
简化网络安全与监控	UDP Director 汇聚 Netflow、sFlow、syslog 和 Simple Network Management Protocol (SNMP) 信息并为其提供单一的标准化目标。这样，它可以显著简化大型企业内多种类型网络和安全数据的集成。UDP Director 设备可以从任何无连接 UDP 应用接收数据，然后将数据重新传输到多个目标，还可以根据需要复制数据。
支持任何无连接 UDP 应用	从多个路由器发送的 tFlow 记录可以复制到多个 Netflow 收集器。这种灵活性不需要在 Netflow 导出设备配置中设置许多 Netflow 目标规范。从多个路由器和交换机发送的 sFlow 样本可以复制到多个 sFlow 收集器上。至于 Netflow 示例，这种用法不需要在 sFlow 导出设备配置中设置多个 sFlow 目标规范。系统日志消息可以自动复制到多个系统日志收集器中。来自路由器、交换机和其他网络设备的 SNMP 陷阱可以自动收集并分布到多个 SNMP 管理站。
可将 UDP 数据从任意来源定向到任意目标	从任何无连接 UDP 应用接收数据，然后重新将数据传输到多个目标，还可以根据需要复制数据。
不需要重新配置基础设施	将点日志数据（Netflow、sFlow、系统日志、SNMP）定向到单一目标，添加或删除新工具时，无需重新配置基础设施。
提供详细的流统计	使用详细的流统计功能，帮助组织估算其环境中的每秒流数 (fps)，确定其监控要求。
缩短网络基础设施的配置时间	简化网络安全与监控
减少带宽	减少网络日志数据重复，降低 WAN 带宽使用量
减少服务中断	减少意外停机和服务中断

UDP Director VM 版规格

型号	最大输入(pps)	最大输出(pps)	监控接口
UDP Director Virtual	15,000	3,000	N/A

StealthWatch FlowSensor 硬件版规格

型号	处理器	内存	磁盘阵列	硬盘	存储容量	接口
UDPD-2200	2x 2.2 Ghz E52650 v4-cache 12c/30MB	16G DDR4 (16x) 256GB total	RAID-6	6x 300GB 10K	1.2TB	i350 quad port 1G Copper RJ-45 + I350 dual port Fiber 1G SFP

内容安全平台

ESA电子邮件安全平台

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。

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。下表概括列出思科电子邮件安全解决方案的主要功能。

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。

思科网络安全解决方案综述

主要功能

容量	说明
全球威胁情报	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： ·每天 100 太字节 (TB) 的安全情报 ·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） ·1.5 亿个终端 ·每天 130 亿个网络请求 ·全球 35% 的企业邮件流量 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馈送给安全设备，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。
垃圾邮件拦截	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。 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。
灰色邮件检测和安全取消订阅	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。 安全取消订阅解决方案具有以下优势 ·防御伪装成取消订阅链接的恶意威胁 ·为管理所有订阅提供统一界面 ·邮件管理员和最终用户可以更好地了解此类邮件
高级恶意软件防护	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 AMP Threat Grid 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。
病毒爆发过滤器	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，系统会通过思科网络安全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。
Web 互动跟踪	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： ·点击恶意 URL 次数排名靠前的用户 ·最终用户点击数排名靠前的恶意 URL ·日期/时间；重写原因；对 URL 采取的操作 管理员还可以反向跟踪所有包含特定 URL 的邮件。
出站邮件控制	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。

卓越的性能	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。
DLP	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。
较低的成本	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。
灵活部署	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，您便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。 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。 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。您可以使用思科内容安全管理设备或思科内容安全管理虚拟设备来轻松管理自定义部署。
满足您业务需求的解决方案	思科云电子邮件安全解决方案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。 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。 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。

产品规格

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 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 C190	1.2 TB (600 x 2)	有 (RAID 1)	8 GB DDR4 内存	1 个 1.9GHz CPU（六核）

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。

思科电子邮件安全设备的硬件规格

型号	ESA C690	ESA C690X	ESA C390	ESA C190
机架单元 (RU)	2RU	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）	1.7 x 19 x 31 英寸（4.3 x 48.3 x 78.7 厘米）	1.7 x 19 x 31 英寸（4.3 x 48.3 x 78.7 厘米）
直流电源选项	是	是	否	否
远程重新通电	是	是	是	否
冗余电源	是	是	是	是（配件选项）
热插拔硬盘	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	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
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	否	否

思科电子邮件安全虚拟设备规格

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

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。

WSA Web 安全平台

在我们高度互联且日益移动化的环境中，复杂的威胁越来越多，这就要求我们使用最佳组合的安全解决方案。思科保障网络基础设施所有层的安全，包括提供强大的保护、完全控制和企业所需的投资价值。我们还提供一系列多方面的网络安全部署选项，以及市场领先的全球威胁情报。思科 WSA 使用性能优越的专业设备简化安全部署。此外，通过思科网络安全虚拟设备 (WSAV)，企业还可以随时随地根据需要快速轻松地部署网络安全措施。

思科 WSA 是首个结合先进防御措施的网络安全网关之一，可帮助组织应对日益严重的挑战来保护和控制 Web 流量。它不仅在部署上更加简单快捷，而且可帮助减少维护需求、缩短延迟时间并降低运营成本。借助“一次性设置”技术，当初始自动策略设置生效后，您的员工即可抽身去做其他事情。每3到5分钟，自动安全更新就会推送到网络设备。思科 WSA 不仅具有灵活的部署选项，还可以与现有的安全基础设施集成，因此能够帮助您满足快速变化的安全需求。
随着视频和其他富媒体的增多，流量已变得难以预测，导致超额和性能下降等问题发生。在解决这些问题和其他问题时，管理员（尤其是跨国组织中的管理员）还需要在购买和安装硬件时面临较长的交付期问题、远程安装难题、海关关税和其他物流问题。

思科 WSAV 允许管理员根据需要随时随地创建安全实例，大大降低了网络安全部署的成本，特别是在高度分布式网络中，尤为如此。思科 WSAV 是思科 WSA 的软件版本，运行在 VMware ESXi 或 KVM 虚拟机监控程序和思科统一计算系统 TM（思科UCS®）服务器之上。购买任意思科电子邮件或网络安全软件捆绑包后，您便会获得思科 SMAV 的无限制许可证，以及相应的 SMA 软件许可证。

借助思科 WSAV，管理员无需进行能力规划，即可对峰值流量做出快速响应。您不必购买和运输设备；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。

功能和优点：

Talos 安全情报	受世界上最大的威胁检测网络支持，可获得快速、全面的网络保护，不仅可视性最高，而且容量最大，可处理： ·每日100TB 的安全情报 ·160 万部已部署的安全设备，包括防火墙、IPS、网络和电子邮件设备 ·1.5 亿个终端 ·每天 130 亿个网络请求 ·35% 的全球企业电邮流量 通过全天候监测全球流量活动，分析异常现象、发现新威胁，并监控流量趋势。Talos 能持续生成新的规则，以便每 3 到 5 分钟将更新馈送到 WSA，从而有助于防止零小时攻击。同时，它还能先于同类竞争产品数小时或数天提供业界领先的威胁防御。
思科网络使用控制	将传统的 URL 过滤与动态内容分析相结合，以降低合规性、责任和工作效率风险。思科不断更新的 URL 过滤数据库中包含超过 5000 万个屏蔽站点，与众不同的是，它还涵盖已知网站。动态内容分析 (DCA) 引擎能够实时准确地识别 90% 的未知 URL；它不仅可以扫描文本、对文本进行相关性评分、计算模型文档接近度，还能返回最接近的类别匹配。管理员还可以选择特定类别的智能 HTTPS 检查。
高级恶意软件防护	高级恶意软件防护 (AMP) 是附加的许可功能，所有思科 WSA 客户均可使用。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。它使用了思科和 Sourcefire® 技术所支持的庞大的云安全情报网络。AMP 向思科 WSA 中提供的恶意软件检测和拦截功能增添增强型文件信誉功能、详细的文件行为报告、持续文件分析和追溯性判定警报。思科 AMP Threat Grid 通过本地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。第 4 层流量监测器通过检测并拦截间谍软件“回拨”通信，来持续扫描所有活动。通过跟踪所有网络应用，第 4 层流量监测器可以有效地阻止试图绕过常用的网络安全解决方案的恶意软件。它可以动态地将已知恶意软件域的 40 地址添加到要拦截的恶意实体清单。
感知威胁分析	思科认知威胁分析是一种基于云的解决方案，可以缩短在网络内部发现威胁的时间。它通过使用行为分析和异常检测，来识别恶意软件感染的症状或数据泄露，从而应对基于外围的防御的漏洞。您只需向您的网络安全解决方案添加附加许可证，即可使用思科感知威胁分析功能。您可以在获得随着不断变化的威胁形势一起发展的优异保护的同时，降低复杂性。
应用可视性与可控性 (AVC)	轻松地控制数百个 Web 2.0 应用和 150,000 多个微应用的使用。借助粒度策略控制，管理员一方面可以允许使用 Dropbox 或 Facebook 等应用，另一方面又可以阻止用户上传文档或点击“赞”按钮等活动。通过 WSA，您可以查看整个网络中的活动。新变化：客户可以按用户、组和策略部署自定义的带宽和时间配额。

防数据丢失 (DLP)	通过为基本 DLP 创建基于上下文的规则来防止机密数据从网络中泄露出去。思科 WSA 还使用互联网内容修改协议 (ICAP) 与第三方 DLP 解决方案进行集成，以便执行深度内容检测和 DLP 策略。思科 WSA 还支持安全 ICAP，从而能够加密 WSA 与第三方 DLP 解决方案之间交换的流量。
漫游用户保护	思科 WSA 可通过与 Cisco AnyConnect® 安全移动客户端进行集成来保护漫游用户。这样一来，即可启动将流量重定向回本地解决方案的 VPN 隧道，从而为远程客户端提供网络安全保护。Cisco AnyConnect 技术会先对流量进行实时分析，随后再确定是否允许访问。 此外，思科 WSA 还与思科身份服务引擎 (ISE) 相集成。通过这一重要的增强功能，客户现在可以通过请求获得思科 WSA 的 ISE 的强大功能。借助思科 ISE 集成，管理员可以根据思科 ISE 在单点登录过程中收集的配置文件或成员信息，在思科 WSA 中创建策略。
集中管理和报告	获得有关威胁、数据和应用的有价值情报。思科 WSA 提供易于使用的集中式管理工具来控制运营、管理策略及查看报告。 思科 M 系列内容安全管理设备提供了跨多个设备和多个位置（包括虚拟实例在内）的中央管理和报告功能。 思科® 网络安全报告应用是一个用于提供报告的解决方案，它可以快速为思科网络安全设备 (WSA) 和思科云网络安全 (CWS) 解决方案生成的日志建立索引，并对之进行分析。此工具可为具有较高流量和存储需求的客户提供可扩展的报告。报告管理员可通过此工具收集有关 Web 使用情况和恶意软件威胁的详细见解。
灵活的部署	思科 WSAV 的功能与思科 WSA 几乎完全相同，不同之处仅在于前者增添了虚拟部署模式（包括即时自助服务调配），不仅更方便您使用，而且还可以节省更多成本。获得思科 WSAV 许可证后，企业无需网络连接，即可将许可证应用于本地新存储的思科 WSAV 虚拟映像文件，从而部署网络安全虚拟网关。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网络安全网关。 您可以在同一部署中运行硬件和虚拟机。因此，小型分公司或远程场所无需在其所在地点安装和支持硬件，即可获得与思科 WSA

产品规格

思科 WSA 的性能规格

	型号	磁盘空间	RAID 镜像	内存	CPU
大型企业	S690	4.8 TB （8 块 600 GB SAS 硬盘）	有 (RAID 10)	64 GB DDR4 内存	2 个，2.5 GHz，24 核
大型企业	S690X	9.6TB （16 块 600 GB SAS 硬盘）	有 (RAID 10)	64 GB DDR4 内存	2 个，2.5 GHz，24 核
中型办公室	S390	2.4 TB （4 块 600 GB SAS 硬盘）	有 (RAID 10)	32 GB DDR4 内存	1 个，2.4 Ghz，8 核
中小企业和分支机构	S190	1.2TB （2 块 600 GB SAS 硬盘）	有 (RAID 1)	8 GB DDR4 内存	1 个，1.9 Ghz，6 核

*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。

思科 WSA 的硬件规格

	思科 S690	思科 S690X	思科 S390	思科 S190
硬件平台				
外形规格	双机架单元	双机架单元	单机架单元	单机架单元
尺寸	3.4x19x29 英寸	3.4x19x29英寸	1.7x19x31英寸	1.7x19x31英寸
冗余电源	是	是	是	是（配件选项）
远程电力循环	是	是	是	否
直流电源选项	是	是	否	否

热插拔硬盘	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	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
光纤选项	是，独立 SKU 6 端口千兆 Base-SX 光纤：WSA-S690-1G 6 端口万兆 Base-SR 光纤：	是，独立 SKU 6 端口千兆 Base-SX 光纤：WSA-S690-1G 6 端口万兆 Base-SR 光纤：	否	否

思科 WSAV 规格

Web 用户	型号	磁盘	内存	核心
少于 1000	S000v	250 GB	4 GB	1
1000-2999	S100v	250 GB	6 GB	2
3000-6000	S300v	1024 GB	8 GB	4

服务器		虚拟机监控程序	
思科 UCS		ESXi 5.0、5.1 和 5.5	vmware KVM
Red Hat Enterprise Linux 7.0		KVM：QEMU 1.5.3	
Ubuntu 14.04.1 LTS		KVM：QEMU 2.0.0	

部署

思科 WSA 是一种转发代理，可以采用显式模式（代理自动配置 [PAC] 文件、Web 代理服务器自动发现 [WPAD]、浏览器设置）或透明模式（网络高速缓存通信协议 [WCCP]、策略型路由 [PBR]、负载均衡器）进行部署。与 WCCP 兼容的设备（如 Cisco Catalyst® 6000 系列交换机、思科 ASR 1000 系列汇聚多业务路由器、思科集成多业务路由器和思科 ASA 5500-X 系列下一代防火墙）可以将 Web 流量重新路由到思科 WSA。

思科 WSA 可以代理 HTTP、HTTPS、SOCKS、本地 FTP 和 FTP over HTTP 流量，以便提供各种附加功能（如数据丢失保护、移动用户安全和高级可视性与可控性）。

访问控制与策略平台

ISE 统一策略管理平台

产品概述

思科® 身份服务引擎 (ISE) 可帮助 IT 专业人员应对企业移动性挑战，并为不断发展的网络提供涵盖整个攻击过程的保护。Cisco ISE 是市场领先的安全策略管理平台，它能以统一且自动化的方式实现高度安全的访问控制，帮助实施基于角色的网络访问及网络资源访问。它提供出色的用户可视性和设备可视性，可实现简化的企业移动性体验。它采用基于思科平台交换网格（pxGrid）技术的集成生态系统合作伙伴解决方案共享至关重要的情景数据，可更快地识别和缓解威胁，并采取补救措施。

移动性企业环境中的安全性

企业网络已不再局限于安全防火墙所保护的范围内。当今的员工需要使用比以往更多的媒介（包括个人笔记本电脑、平板电脑和智能手机），从家庭网络和移动网络访问企业资源。显然，移动性可能使网络遭受极具破坏性的攻击和数据泄露，并由此给组织造成巨大的经济损失。但是当今的移动员工需要随时随地工作，以保持竞争力和工作效率。在这种扩展网络的复杂性不断增加的同时，“物联网”逐渐兴起，各种支持网络功能的设备连接至私有和公共网络，导致无法识别网络安全威胁并采取补救措施的潜在影响急剧增加。

此外，IT 专业人员必须在更紧张的预算内支持企业移动性计划，同时遵守政府、行业和其他合规性要求。要满足这些要求乃至更多要求，就必须清楚地了解网络访问并严格实施访问控制。安全点解决方案通常被大量分布并部署在整个企业网络中。这类解决方案侧重于在威胁出现时识别威胁，或在发生泄露或攻击后协助进行取证调查。将防止受影响的设备或用户访问网络放在首位的安全解决方案通常涉及复杂、耗时且昂贵的部署。随着您的网络不断发展和扩展，这些互无联系的安全点解决方案无法足够快地进行相应的扩展。必须对不断发展的移动性企业环境采用一种兼顾管理性和安全性的新方法。这种方法便是思科身份服务引擎 (ISE)。

功能和优势

Cisco ISE 为实现网络访问安全提供了一种更全面的方法，它具有以下特性：

- 可准确识别每一位用户和每一台设备
- 使所有设备的自注册和调配变得简单
- 提供集中的情景感知型策略管理来控制用户访问 - 覆盖任何人、任何时间，以及任何设备
- 提供有关已连接用户和设备的更深入的情景数据，以便更快地识别和缓解威胁，并采取补救措施

在网络中运营时，客户可通过部署 Cisco ISE 获得下表所示的优势。

客户可以获得的主要优势

Cisco ISE 的优势	
强大的设备分类	Cisco ISE 提供业内首款集成的设备分析器，该分析器不仅能够识别每个终端，将终端与其用户或功能及其他属性（包括时间、位置和网络）相匹配，而且能创建情景身份，从而使 IT 能够精确控制允许访问网络的人员和允许访问的内容。自动设备馈送服务会实时更新 Cisco ISE，以确保新设备在上市后能够尽快得到识别。

Cisco ISE 的优势

广泛的策略实施	Cisco ISE 使组织能够轻松且非常灵活地定义访问策略规则，以满足企业不断变化的业务要求。例如，在 Cisco ISE 中，IT 管理员可以定义策略来区别对待访客用户和访客设备与注册用户和注册设备。访客用户可能会获得整个网络的有限访问权限，注册用户则能获得其相应策略指定的访问权限。此外，Cisco ISE 中的策略可保证只有注册用户的受信任设备或合规设备才能访问网络。Cisco ISE 会根据用户或设备的情景身份向网络进入点发送高度安全的访问规则，这样， IT 人员就可以在用户或设备尝试访问网络的任何位置确保策略实施的一致性。
简化的访客体验	Cisco ISE 提供开箱即用的访客管理和自注册功能，十分方便。管理员可使用动态的可视化工具在几分钟内自定义访客门户，该工具可实时预览访客所看到的门户屏幕和所要经历的步骤，以便准确展示设置的变化会如何影响到用户。Cisco ISE 支持完全自定义访客页面（包括广告、横幅、主题和品牌）、全面管理访客帐户和到期日期，以及全面审核整个网络中的访客帐户和活动。Cisco ISE 支持所有可能的访客工作流程类型（从热点接入，到员工发起的采用短信确认方式的访客接入），使访客接入变得十分轻松。
自助式设备自注册	Cisco ISE 使 IT 人员可以灵活决定如何实施企业的自带设备 (BYOD) 或访客策略。Cisco ISE 为用户提供自助式注册门户，以便根据 IT 自动定义的业务策略注册和调配新设备。这样一来，IT 能够实现自动化的设备调配、分析和安全评估来满足符合安全策略的需要，同时确保极致简化，让员工可在无需 IT 帮助的情况下将设备接入网络。
安全合规性	单一管理控制台简化了所有公司网络中的策略创建、可视性和报告，对审计要求、监管要求， 以及 IEEE 802.1X 标准的联邦政府强制性准则的合规性验证将变得简单轻松。
自动化的设备合规性检查	Cisco ISE 使用 Cisco AnyConnect® 4.0 Unified Agent 提供设备安全状态检查和补救选项。Cisco AnyConnect® 4.0 Unified Agent 还提供用于检查台式机和笔记本电脑的高级 VPN 服务，并支持与市场领先的面向移动设备的企业移动性管理 (EMM) 解决方案相集成。此功能有助于确保用户的设备既安全又符合策略要求。
可靠的随时随地访问	Cisco ISE 可实时调配有关网络接入设备的策略，使移动用户或远程用户能够通过无线连接获得与有线连接一致的服务访问体验。
运营效率	Cisco ISE 可提供自注册和安全自动化、集中策略控制、可视性、故障排除以及与 Cisco Prime™ 解决方案集成，有助于大幅减少 IT 和服务中心在解决用户和网络安全问题上所需的时间。
嵌入式实施	大多数思科交换机和无线控制器中都内置设备传感功能，可在进入点将分析信息扩展到整个网络，而无需购买和管理重叠设备或更换基础设施。

Cisco ISE 的优势

使用 Cisco TrustSec® 策略网络功能将策略从接入扩展到数据中心	Cisco ISE 是适合独特的 Cisco TrustSec 网络技术的策略管理点，它提供策略定义的网络分段，以消除网络安全的复杂性。借助 Cisco TrustSec 技术，用户可以使用基于角色的访问策略，根据业务规则轻松地以符合逻辑的动态方式对其网络进行分段，而不是管理多个 VLAN 或不断变化的网络架构，从而在不断变化的扩展网络上轻松实现高度安全的访问。
多供应商基础设施支持	Cisco ISE 可与符合 RADIUS 和 IEEE 802.1X 标准的多供应商基础设施互通。思科及其合作伙伴可提供最佳实践指导以及详细的实际设计指南。企业客户可结合使用 Cisco ISE 与思科设计的网络基础设施及 Cisco TrustSec 技术，以便从其网络中获取更丰富的情报，并获得更强的网络可视性。
Cisco pxGrid 情景共享	Cisco ISE 可从整个网络中收集动态的情景数据，并利用 Cisco pxGrid 技术（一个强大的情景共享平台）与外部和内部生态系统合作伙伴解决方案共享有关已连接用户和设备的更深层次的情景数据。Cisco ISE 网络和安全合作伙伴通过使用单个 API 来利用这些数据，以改善其各自的网络接入功能，并使其解决方案能够更快地识别和缓解网络威胁，并采取补救措施。
广泛、集成的合作伙伴生态系统	Cisco ISE 拥有最广泛的合作伙伴生态系统。合作伙伴使用 Cisco pxGrid 改善其终端设备漏洞补救、网络取证调查和网络单点登录 (SSO)。EMM、安全信息和事件管理 (SIEM) 以及威胁防御 (TD) 的集成技术合作伙伴均利用 Cisco ISE 提供的深入情景身份感知功能，来应对比他们可以单独应对的使用案例更多的使用案例，从而更有效地履行其职责。利用 Cisco ISE，合作伙伴平台可深入挖掘思科网络基础设施，并对用户和设备执行网络操作（例如隔离智能手机或笔记本电脑，以及阻止网络访问）。

Cisco ISE 通过提供全面的策略管理、简化的设备自注册过程、可与合作伙伴共享的丰富情景数据以及动态的策略实施，来帮助确保高度安全的有线、无线和 VPN 接入，从而增强企业的能力。

功能	优势
业务策略实施	提供一个基于规则的、属性驱动的策略模型，用以创建具有业务相关性的灵活访问控制策略。 通过从预定义字典（包括用户和端点身份、安全状态验证、身份验证协议、分析身份或其他外部属性来源的信息）中提取属性，从而创建精细策略。也可动态创建属性，并保存属性以备日后使用。 可与多种外部身份库（例如 Active Directory、LDAP、RADIUS、RSA OTP 以及用于身份验证和授权的证书授权）集成。
访问控制	使用 Cisco TrustSec 技术支持的网络设备的高级功能提供各种访问控制选项，包括可下载访问控制列表 (dACL)、VLAN 分配、URL 重定向、指定的 ACL 和安全组标签 (SGT)。

功能	优势
访客生命周期管理	提供简化的全新体验，以支持和自定义访客网络接入。凭借对热点接入、终端发起的接入、自助式接入及其他许多接入工作流程提供的内置支持，ISE 使用户可以轻松地在几分钟内创建公司品牌（带有广告和促销信息）的访客体验。新的访客管理工作中心提供实时的可视化流程，将您的设计效果展现在您的眼前。时间限制、帐户到期日期和短信验证提供额外的安全控制，全面的访客审计可以在您的网络中跟踪访问，以满足安全和合规性要求。
简化的设备自注册过程	使用主题提供可完全自定义的品牌用户体验。提供开箱即用的工作流程，这些工作流程可引导用户完成自注册过程，并向最终用户提供其各自的自助服务门户，用于添加和管理其设备。为标准的 PC 和移动计算平台提供自动化的 Supplicant 调配和证书注册。通过精简设备自注册过程减少 IT 服务中心支持请求，并为用户提供更安全的访问和更轻松、更透明的体验。
AAA 协议	使用标准的 RADIUS 协议进行身份验证、授权和记账 (AAA)。支持多种身份验证协议，包括（但不限于）PAP、MS-CHAP、可扩展身份验证协议 (EAP)-MD5、受保护的 EAP (PEAP)、通过安全隧道的 EAP 灵活身份验证 (FAST) 以及 EAP 传输层安全 (TLS)。Cisco ISE 是唯一支持机器与用户凭证的 EAP 链路的 RADIUS 服务器。
内部证书授权	在 Cisco ISE 内为组织提供易于部署的内部证书授权，以简化个人设备的证书管理，而不会显著增加外部证书授权申请的复杂性。Cisco ISE 提供用于管理终端设备及其证书的单一控制台， 能够通过基于标准的在线证书状态协议 (OCSP) 检查证书状态，并且可在设备失窃时自动吊销证书。内部证书授权支持独立和从属（即与您现有的企业 PKI 一起）部署。
设备分析	附带了适用于各种终端（如 IP 电话、打印机、IP 摄像机、智能手机和平板电脑）的预定义设备模板。此外，管理员还可以创建属于自己的设备模板。端点连接至网络时，这些模板可用于自动检测、分类和关联管理员定义的身份。管理员还可以根据设备类型关联端点特定的授权策略。 Cisco ISE 通过被动网络监控和遥感勘测来收集终端属性数据，具体方式包括直接查询实际终端，或者通过 Cisco Catalyst® 交换机上的设备传感器从思科基础设施进行查询。 Cisco ISE 传感技术包含 Cisco Catalyst 交换机具有的由基础设施驱动的终端传感功能。利用这项功能，交换机能够快速收集终端属性信息，然后使用标准 RADIUS 将此信息传送至 Cisco ISE，以便执行终端分类和基于策略的实施。这种基于交换机的传感功能可更有效地分发终端信息，从而改善可扩展性、可部署性和分类时间。
设备配置文件馈送服务	Cisco ISE 提供的业内首个设备配置文件馈送服务支持开箱即用的分析技术，方法是为来自多家供应商的各种支持 IP 的设备自动更新思科已验证的设备配置文件。馈送服务还提供了一种机制，合作伙伴和客户可通过该机制共享各自的自定义配置文件信息，以便思科审核和重新分发。由于这些自动更新功能，企业可在用户尝试连接到网络时检测所有最新的设备。这不仅使紧跟不断出现的大量新设备变得更加简单，而且能大幅减少 IT 管理员的支持任务。
终端状态	验证连接网络的 PC 和移动设备的终端状态评估。通过基于客户端的永久代理或临时网络代理进行操作，以验证终端是否符合企业的状态策略。可创建强大的策略，包括（但不限于）使用当前的定义文件变量（版本、日期等）、注册表（项、值等）和应用来检查是否有最新的操作系统补丁、防病毒软件包和反间谍软件包。此外，Cisco ISE 还支持自动补救 PC 客户端和定期重新评估，以确保终端未违反公司策略。

功能	优势
Cisco pxGrid 和 ISE 生态系统	Cisco pxGrid 是 Cisco ISE 内的一个强大的情景共享平台，它将 Cisco ISE 收集的更深层次的情景数据提供给外部和内部的生态系统合作伙伴解决方案，以便这些解决方案在在整个网络中更快地执行其功能。从终端漏洞评估到网络单点登录，利用简单的统一框架的 Cisco ISE 生态系统合作伙伴的名单不断扩大。
ISE 生态系统：EMM 集成	EMM 集成使 Cisco ISE 能够与 Cisco EMM 技术合作伙伴解决方案连接，从而帮助确保正在尝试连接至网络的移动设备之前已经向 EMM 注册，并且符合企业策略。它还有助于用户对其设备采取补救措施。合规性检查包括（但不限于）检查设备加密、PIN 锁和越狱状态。
ISE 生态系统：SIEM 和 TD	通过与 Cisco ISE 集成，SIEM 和 TD 合作伙伴可获悉有关用户及设备身份、网络授权级别以及安全状态的 Cisco ISE 情景信息，进一步增加他们对整个网络的安全事件的可视性。出现这种变革后，合作伙伴能够从数月的取证事件追查到异常设备，从中获得实时可视性，并制定可直接从管理员面板内部执行的安全措施。
ISE 生态系统：控制/SCADA 运营和安全策略集成	实现高度安全地访问和管理控制以及监控与数据收集 (SCADA) 网络设备。Cisco ISE 为控制和 SCADA 策略管理器提供情景和控制，
ISE 生态系统：简化的网络故障排除和取证调查	允许数据包捕获系统使用 Cisco ISE 收集的情景数据将用户、设备和用户角色与捕获的数据包数据关联。由于数据包捕获对于调查威胁和网络问题至关重要，因此将情景数据与数据包捕获相关联可简化网络故障排除和加快取证调查。
ISE 生态系统：终端漏洞补救集成	了解如何在网络漏洞报告上确定优先顺序以及确定优先顺序的对象非常困难。将来自 Cisco ISE 的情景数据与漏洞报告共享可更好地识别和优先处理需要调查的终端漏洞，并帮助用户采取措施以便快速补救。
ISE 生态系统：基于风险的自适应身份验证和单点登录	启用情景驱动的用户身份验证和网络应用授权。可根据 Cisco ISE 提供的联合身份、身份验证风险因素和情景数据组合来精细策略，减少甚至完全消除身份验证挑战。随着员工用来访问企业资产的移动设备数量激增，用户身份验证（虽然对安全至关重要）变得极其繁琐。此集成使用户能够对企业资产透明地进行身份验证，而无需重复挑战，同时根据风险级别阻止对云资产的访问。
广泛的森域 Active Directory 支持	Cisco ISE 提供对 Microsoft Active Directory (AD)域的全面身份验证和授权。它可以将多个分散的域分组到逻辑组，以简化配置复杂的 AD 拓扑，从而支持不断变化的业务环境。Cisco ISE 还支持灵活的身份改写规则，以便实现顺利过渡和集成。 支持 Microsoft AD 2003、2008、2008R2、2012、2012R2。
终端保护服务	使管理员能够对网络中存在入侵风险的终端快速采取纠正操作（隔离、解除隔离或关机）。这样有助于减少网络危险，增强安全性。

功能	优势
集中管理	包括具有监控、报告和故障排除功能的内置网络控制台，用于帮助服务中心和网络操作人员快速识别和解决问题。提供所有服务的全面历史和实时报告、所有活动的记录以及连接至网络的所有用户和终端的实时控制面板指标。
平台选择	可作为物理或虚拟设备使用。具体包括两个物理平台以及一个基于 VMware ESX 或 ESXi 的设备。物理和虚拟设备都可用来构建 Cisco ISE 集群，以便为较大型的组织服务，并提供关键企业业务系统所需的必要扩展、冗余以及故障转移能力。

Anyconnect 统一安全客户端

AnyConnect 利用思科身份服务引擎 (ISE) 提供具有情景感知功能且简单的安全策略综合实施方法。

还可以使用它来辅助实施面向终端的思科高级恶意软件防护 (AMP) 的部署。 其 AMP 支持功能将终端威胁防范扩展到支持 VPN 的终端或所有使用思科 AnyConnect 服务的位置。

新的思科 AnyConnect 4.2 是 Windows 和 Mac OS X 平台上的网络可视化模块。 管理员现在可以监控终端应用的使用情况，从而发现潜在的行为异常并制定出更明智的网络设计决策。 这些使用数据可与越来越多支持互联网协议信息输出 (IPFIX) 的网络分析工具共享。

AnyConnect 安全移动客户端在整个扩展网络内提供可视性和可控性，阻止受到危害的终端获取关键资源的访问权限。 它具有以下特点：

- 调整隧道协议以采用最有效的方法
- 提供第 2 层高级访问功能，为并发设备和用户验证提供便利
- 远程向平板电脑和智能手机授予选定企业应用程序的访问权限
- 将服务器作为代理，跨有线网络、无线网络和 VPN 提供一致且高度安全的终端访问
- 提供可选的 Web 安全和高级恶意软件威胁防御
- 监控终端应用使用情况，帮助揭示可疑行为

您可以通过适用于移动平台的 Cisco AnyConnect® 安全移动客户端保护员工的智能手机和平板电脑，客户端可供 Apple iOS 6.0+、Android 4.0+ 以及精选的 Amazon Kindle 和 Fire Phone 设备使用。适用于移动平台的 Cisco AnyConnect 安全移动客户端从智能手机和平板电脑提供可靠且易于部署的加密网络

Cisco AnyConnect 安全移动解决方案的功能

功能	说明
统一终端合规性	Cisco AnyConnect ISE 代理可以在整个有线、无线及 VPN 环境中为 Cisco ISE 提供统一的终端状态检查和修复。作为终端状态检查主要源头的服务，可检查操作系统级别、最新病毒防护更新以及其他资源，以增强终端的安全功能和合规性。此外，终端状态也可通过与 ASA 相结合 Cisco Hostscan 来获得。

功能	说明
高度安全的网络访问	Cisco AnyConnect Cisco Network Access Manager 提供卓越的连接功能，支持管理员控制终端可以连接的网络或资源。它提供的 IEEE 802.1X 请求方可以与 MACsec IEEE 802.1AE 等独特加密技术一起，配置为身份验证、授权和统计 (AAA) 功能的一个部
网络安全	Cisco AnyConnect 内置的另一个模块，可通过现场思科网络安全设备(WSA) 或基于云的思科云网络安全 (CWS) 产品来实现网络安全。将网络安全与 VPN 访问相结合，管理员可以为所有最终用户提供全面的安全移动性，这对于自带设备 (BYOD) 部署至关重要。企业可以选择能防止网络遭受恶意软件攻击并控制和确保安全使用网络的部署。
无客户端访问	Cisco 自适应安全设备 (ASA) 提供通过各种浏览器跨多个平台实现的 SSL 连接。Cisco ASA 支持管理员提供对非受管终端的无客户端 VPN 访问，还可以提供对各种基于 Web 和 TCP/IP 的应用的访问。这些都是通过改写器、插件或智能隧道，使用浏览器嵌入式 SSL 技术提供的，同时还能确保精细的访问控制和端到端安全性。
虚拟桌面基础设施 (VDI) 访问	Cisco ASA 可以高度安全地终止 VDI 会话，而且能实现对虚拟应用和桌面的透明访问。为移动设备、笔记本电脑和桌面设备提供对虚拟资源的客户端和无客户端访问。由高度安全远程访问提供强大支持的虚拟资源访问不受特定厂商约束，可受益于为虚拟资源和传统资源定义的单一访问策略。
移动设备支持	随着自带设备工作 (BYOD) 潮流的兴起，管理员需要支持最终用户使用个人移动设备远程访问公司网络，从而帮助其提高工作效率。在如今多样化工作人员最常用的设备上，均可部署 Cisco AnyConnect。经过挑选的企业移动应用，通过每个应用专配 VPN，可以透明地实现基于设备或由设备驱动的高度安全的远程访问。全新的每应用专配 VPN 功能可防止未经批准的应用访问机密业务资源，从而进一步减小了恶意软件通过远程访问进行入侵的风险并降低了带宽成本。

总结

思科的以威胁防御为中心的方法降低了复杂性，提供全面的可见性和可控性，在攻击发生的整个过程（攻击发生之前，之中和之后）提供先进的威胁防御。思科是唯一的能够在连续攻击发生的各个阶段，都可以提供领先的安全产品的厂商。许多思科的安全产品也都在各自细分技术领域处于领先者的位置。在过去的两年中，思科安全投入了数十亿美金，完成了对 Sourcefire, ThreatGRID, Neohapsis, OpenDNS 和 Lancope 等的收购和整合，大大加强和丰富了自身的整体网络安全解决方案。

思科安全服务概览

安全服务可帮助您从自己的网络安全计划和技术投资中获取最大回报。 使用安全服务的组织可以获得顾问和技术专家的帮助，从而为自己的员工提供最新的知识和能力支持。安全服务还有助于缩短威胁检测和响应时间。此外，通过降低复杂性，您还可以提高适应不断变化的业务优先级的能力。

安全服务：

为新数字经济保驾护航

思科安全事件响应服务

如今，网络攻击空前活跃，而安全人才却日益短缺，这让许多组织难以抵御网络威胁。《思科 2015 年年度安全报告》中指出，只有50%的首席信息安全官真正认为“能够轻松确定感染的范围，加以遏制，防止事态进一步扩大”。

快速、全面的响应

如果您的组织遇到网络相关事件（无论是机密数据泄露，还是因蠕虫影响到运营），思科安全事件响应服务团队会快速调集相关资源，该团队可对实际情况做出分类，然后定制相应的响应计划，从而确定攻击来源，界定事件范围，有效遏制攻击，并找出根本原因，以确保企业尽可能快速有效地恢复正常运营。

威胁不同，响应方式也有所不同

不同的组织遇到的威胁和事件也情况各异，思科安全事件响应服务团队首先向您发起响应服务启动呼叫，对当前状况进行分类，然后与您一起确定当前可以立即采取的措施，并确定所需的其他思科资源和工具。我们会在24小时内派出技术人员，为您提供现场服务。技术人员还将负责与整个安全事件应急响应服务团队联络，确保充分利用思科资源（包括思科Talos 团队）来解决您的问题。

我们的优势

- 即时联系富有经验的事件响应专家（他们长年从事于解决各类事件）
- 久经考验的方法、独一无二的情报和经验丰富的团队，让人满意的响应结果
- 解决事件中使用各种思科工具套件（面向终端的AMP、FirePOWER IDS、Stealthwatch 等）增强对威胁的可视性，更快速、全面了解网络中所有威胁
- 毫无阻碍地使用配套服务（例如渗透测试、第三方评估、网络分段等），更全面实施补救并提高恢复能力

我们的方法

- **分类：** 评估当前状况，确定制定和启动响应策略的最佳方式
- **协调：** 跟踪响应状态和未完成的行动项目，并根据需要更新计划，确保事件得到谨慎处理
- **调查：** 运用多种措施确定攻击范围，包括部署必要的工具；审查日志源，分析规律和问题所在；执行必要的调查分析；对恶意软件进行反向工程
- **遏制：** 隔离并消除攻击者的后续攻击行为
- **监控：** 在合约期内开发签名，并对网络环境进行持续监控，确保网络长期保持健康状态
- **补救：** 根除恶意软件以及攻击者埋下的其他工具和工件
- **漏洞会诊：** 在需要时，思科安全时间应急响应服务团队会与我们的危机沟通团队进行内部合作，委派合适的沟通专家参与事件处理，避免采用“一刀切”的方法
- **最终报告：** 服务结束时，我们会提供一份报告（内容包括事件摘要、回顾、调查结果和建议）

思科安全优化服务

随着网络边界逐渐消失，安全关注点也有所变化。如何确定迁移到云的安全风险？随着越来越多的设备访问您的网络，您的安全策略是否充分而有效？您如何对 网络进行更改，而不影响到可靠性或安全性？在 IT 资源紧张的情况下，如何应对这些变化？ 思科® 安全优化服务可帮助您应对这些挑战。

全方位服务管理风险和威胁

我们全面的服务将战略、评估、支持和培训活动集于一身。我们持续的支持可帮助您发展并改善您的安全状态、安全策略，以及安全基础设施的有效性。我们将帮助您将获得丰富的知识和最佳实践，并以安全方式实施安全新技术（例如云和虚拟化），并协助您管理风险和威胁，帮助您满足不 断发展的合规性要求。

业务目标驱动解决方案

思科安全优化服务专注于以下方面：

- **提高安全性** - 发现存在于您的安全和网络基础设施中的漏洞，帮助您实现预期的保护级别。
- **合规策略** - 随着您陆续添加新应用和新技术，不断改进网络安全解决方 案，同时确保始终遵守相关政策和法规。
- **公共云** - 了解当您的员工、应用和数据连接到第三方云时，您需要进行哪些更改来提高安全性。
- **分支机构** - 在您的不同位置之间高度安全地传输支付处理数据或其他 数据。
- **以新的方式更安全地工作** - 在员工使用社交网络和协作、即时消息、屏 幕共享、网络会议和共享工作空间时，保护信息和关键数据。
- **移动性** - 让用户能够随时随地从任何设备更安全地访问数据。

我们的优势

- 通过识别您的安全和网络基础 设施中的漏洞，提高安全性。
- 随着您陆续添加新应用和新技术，不断改进网络安全解决方案，同时确保始终遵守相关政策和法规。
- 在您的不同位置之间高度安全地 传输支付处理数据或其他数据。
- 支持您的员工访问并与第三方云协作，同时保护信息和关键数据。
- 让用户能够随时随地从任何设 备更安全地访问数据。

我们的方法

我们的团队将与您共同制定一份端到端安全架构视图。我们将与您密切合作，确定改善系统设计、发现安全漏洞、减少性能问题，以及支持新业务 要求的最佳方法。我们还将帮助您以更安全的方式实施新技术。 思科安全优化服务将在以下四个方面为您提供支持：

1.战略和规划： 我们推荐风险管理战略和安全策略，以便您在保护公司资 源的同时，能够支持您的客户、供应商和员工在任何地点使用任何设备 进行高度安全的访问。

2.定期评估： 我们会开展评估并分析安全漏洞，以便为您提供关于如何解 决这些漏洞的建议。

3.持续的优化支持： 我们会在您制定及验证安全计划的过程中，持续为您 提供专家意见。

4.持续的知识传授： 我们会提供非正式的培训课程，帮助您的 IT 员工学习 安全知识。 思科为您提供对您的安全环境执行全面且权威的测试所需的专业知识和全 球覆盖能力。您将从最大的全球最佳实践和验证设计数据库（基于内部思 科资源和专业知识）中获益。 我们将凭借丰富的安全专业知识和广泛的合作伙伴生态系统，帮助您成功管理风险。

实践出真知-思科电子靶场 CyberRange (安全训练营)

仅有安全硬件和软件产品不足以阻挡目前最先进的攻击，现代网络防御要求安全人员具备检测和瓦解复杂威胁的经验与专业知识。Cisco® Cyber Range 服务能够帮助安全人员获得应对现代网络威胁所需验。根据实际情况，Cyber Range 提供一个虚构的对战模拟环境，可让安全人员扮演攻击者和防御者的角色，从而了解最新的安全漏洞破解方法以及如何利用高级工具和技术来缓解和根除威胁。

Cisco Cyber Range 服务提供:

如果您的组织遇到网络相关事件（无论是机密数据泄露，还是因蠕虫影响到运营），思科安全事件响应服务团队会快速调集相关资源，该团队可对实际情况做出分类，然后定制相应的响应计划，从而确定攻击来源，界定事件范围，有效遏制攻击，并找出根本原因，以确保企业尽可能快速有效地恢复正常运营。

- 应对和防范简单及复杂网络攻击的实际经验，包括高级持久威胁 (APT)
- 领先的安全方法、运维和程序方面的更深入知识
- 部署行之有效的检测模式、利用最新安全工具和技术的高级技能
- 建立团队协作和责任管理，平衡工作负荷，将工作重点放在核心任务上

解决方案亮点

Cyber Range 是实际体验智能网络安全的一个平台，它是模拟典型企业客户的网络和应用的沙坑环境。该解决方案不仅重视技术，同时也兼顾人、技能、流程、数据以及连接到互联网的万事万物。

Cisco Cyber Range 服务基于以下组件构建:

基于运维主导的模式，汇集人、流程和技术的力量来应对网络威胁 在思科云智能安全服务的助力下，利用着重于威胁、可见性驱动和基于平台的工具

模拟 50 多种不同的攻击情形和 100 多种实际应用 不断更新最新的攻击和威胁情形

使用能在全球任何地方远程访问的虚拟环境

特性与优点

Cisco Cyber Range 服务模拟复杂的网络、服务器和应用基础架构环境。图 1 概要显示了 Cyber Range 环境。

应用与网络基础架构区代表典型的内部 IT 环境，模拟了互联网边界网关（网关块）、数据中心与应用服务（服务器块）以及本地与远程用户访问基础架构（用户块）。防御区代表安全运维中心。在防御区内，蓝色团队的成员可以访问一系列系统，以监控、应对和防范针对内部环境的威胁。攻击区代表外部环境。红色团队可以利用最新的工具和技术来攻击内部环境，包括通过网关块和从用户块攻击。监控区允许绿色团队（包括思科人员）控制和评估总体对战模拟。

- 基于运维主导的模式，汇集人、流程和技术的力量来应对网络威胁 在思科云智能安全服务的助力下，利用着重于威胁、可见性驱动和基于平台的工具
- 模拟 50 多种不同的攻击情形和 100 多种实际应用 不断更新最新的攻击和威胁情形
- 使用能在全球任何地方远程访问的虚拟环境

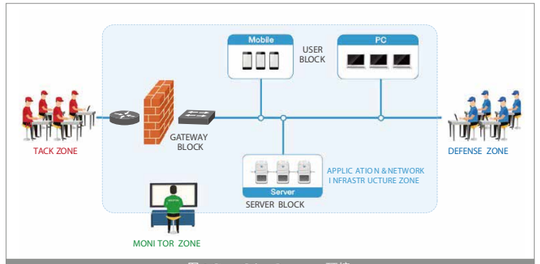


图 1 Cisco Cyber Range 环境

为什么要选择思科服务

Cyber Range 以许多重要方式模拟众多的基础架构服务以及攻击和防御功能。

- 架构设计验证
- 攻略创建和验证
- SOC 团队网络对战模拟练习和事件响应实践
- 某些技术的实操培训
- 威胁缓解流程验证
- 模拟新威胁（零天）或正在演变的威胁，以开发适当的缓解策略和方法

服务规格

Cyber Range 能够模拟众多的基础架构服务以及攻击和防御功能。表 1列出了标准服务。

表 1：服务功能

基础架构
• 有线、无线和远程接入 • 网络与路由 • 客户端模拟器 • 服务器模拟器 • 应用模拟器 • 流量生成

攻击
• 分布式拒绝服务 (DDoS) • 零天攻击 • 网络侦测 • 应用攻击 • 数据丢失 • 计算机恶意软件 • 移动设备恶意软件 • 越狱方法 • Botnet 模拟 • 开源攻击工具 • 虚拟网络攻击

防御
• 全局威胁智能 • 客户端端点安全性 • 防火墙、 IDS/IPS • 基于签名和基于行为的检测 • Web 和电子邮件代理 • 无线安全性 • 应用可见性与控制 • 遥测数据分析 • 身份与权限管理 • 安全与事件管理 • 调查工具 • 开源防御工具 • Cisco TrustSec ® • 软件定义的网络

更多信息

要详细了解 Cisco Cyber Range 服务，请与当地的客户代表联系或发送电子邮件至 cybersecurity-apjc@cisco.com

思科勒索软件防御解决方案

扫描二维码
了解思科勒索软件防御方案

扫描二维码
了解思科更多安全方案

什么是勒索软件？

勒索软件是指可加密个人计算机上文档、照片和音乐等信息的恶意软件或恶意代码。用户必须支付费用才能解密并赎回这些文件。

勒索软件的入侵方式主要分为：

利用网络钓鱼或垃圾邮件中的链接或打开附件

利用感染恶意软件的广告（恶意广告）潜入

使用漏洞攻击包（用于识别终端系统中软件漏洞的软件套件）控制系统进行攻击

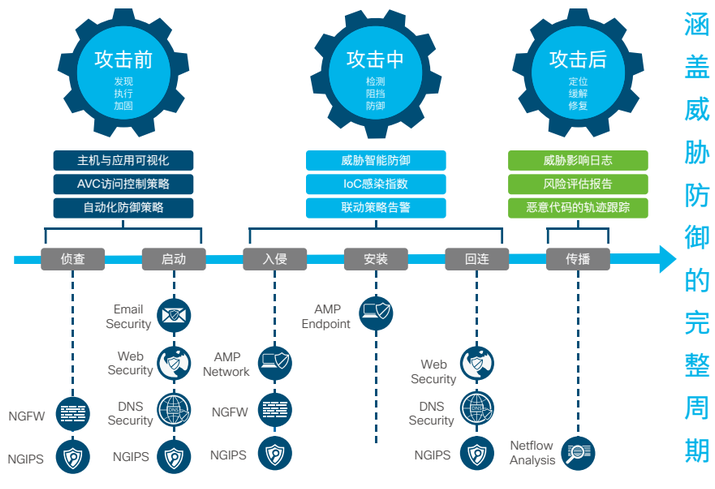
使用更有效的安全方法降低勒索软件风险

减少勒索软件感染的风险需要基于产品组合的方法，而不是单个产品，在威胁尝试植入前进行阻止，从而降低勒索软件感染的风险。

思科勒索软件防御利用思科安全架构来保护业务，其防御范围从网络扩展到 DNS 层、邮件以及终端。我们的解决方案由业界一流的 Talos 威胁研究提供支持，实现了针对勒索软件攻击的全面防御。

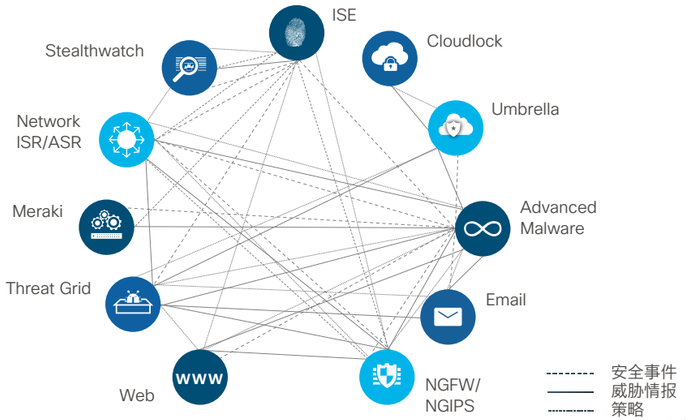
思科勒索软件防御之道：集成的架构和涵盖攻击前、中、后期全过程的解决方案

- NGFW 与 NGIPS 在互联网出口检测并阻挡恶意勒索软件的进入
- 面向终端的思科高级恶意软件防护 (AMP) 可以阻止勒索软件在终端上 打开
- 配备高级恶意软件防护 (AMP) 的思科邮件安全可阻止垃圾邮件和网络 钓鱼邮件以及恶意邮件附件和 URL
- Web 安全网关拦截钓鱼网站的访问
- 思科 Stealthwatch 能够实现网络可视化与异常行为分析，通过与现有的网络基础设施配合，检测终端 C&C 连接行为，并且可以与 ISE 联动实现对网络进行动态分段阻止勒索软件内部扩散
- Umbrella (OpenDNS)服务切断恶意域名解析，在DNS层实现预先阻止勒索软件
- 针对勒索软件，思科安全服务提供远程漏洞扫描和钓鱼软件模拟攻击测试等高级服务。



集成化防御架构，才能实现有效的安全

勒索软件会利用各种方式进行入侵，因此单点产品孤掌难鸣，必须采用一种集成化的防御架构方法才能遏制勒索软件的感染及扩散。
思科集成化防御架构由业界一流的思科 Talos 研究小组支持，包括了思科众多勒索软件防御工具，产品间实时共享安全事件，威胁情报，策略和情景信息，实现自动化联动协作，通过分层架构方法快速降低勒索软件的风险，实现有效的安全。



思科勒索软件防御方案促销包

Firepower NGFW/NGIPS和Email防护

- 识别终端主机的C&C连接
- 拦截含有恶意附件的邮件
- 识别或改写邮件的URL钓鱼链接
- 零日威胁爆发过滤
- 集成AMP防护

AMP高级恶意代码保护

- 利用云智能分析技术
- 恶意代码一旦被发现后，则实现后续的检测和拦截
- 对已知的恶意文件拦截最有效

StealthWatch

- 检测和发现感染主机与C&C僵尸网络的通信
- 对连接C&C的通信企图进行告警
- 借助网络设备作为探针来发现和降低风险

高级安全服务

- 远程漏洞扫描
- 钓鱼软件模拟攻击
- 勒索软件一日攻防演练

制造行业网络安全解决方案

了解智能制造整体安全解决方案

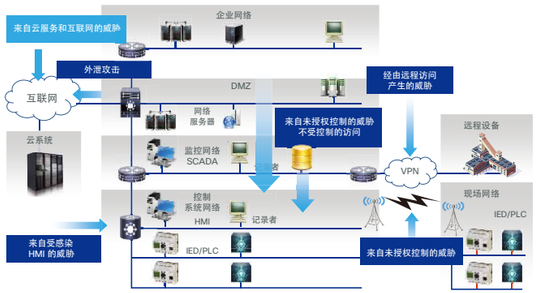
制造业是当下的“闪光”行业。“工业4.0”或“中国制造2025”从宏观的产业、政策层面不断为制造业发展而提供推动力，而万物互联 (IoE) 的技术和增长则在提高价值链效率、节省成本同时，也进一步成为现代制造业突飞猛进发展的强力“引擎”。

但正如硬币的两面一样，制造业的网络安全在如今也面临更大的威胁，随着制造商开始采用新技术标准，并努力融合 IT 和运营技术系统与组织孤岛之间的传统边界，这种威胁也会不断加剧，成为妨碍制造业创新发展的最大障碍。

工业自动化和控制系统面临威胁

传统工业控制系统中有很多系统在创建时并未考虑安全性，因而特别容易遭受网络威胁。由于这些系统与企业IT 技术融合和集成，新的攻击手段层出不穷。通过图1可以看到，在当今融合 IT 和 OT 网络、云计算、移动性和 IoT 平台盛行的时代，制造企业面临的威胁越来越多。

图 1. 制造商面临的威胁状况演变图



攻击者往往会瞄准那些能轻易被侵入的系统，例如工业自动化和控制系统 (IACS) 网络。从本质上讲，IACS 非常容易受到攻击，这些系统使用专有硬件和软件，传统工厂网络几乎没有（甚至完全没有）实施任何安全保护措施。随着制造商开始跨工厂实施 IoE 功能，并将工厂资产连接到更高级别的应用，这种易受攻击的情况也会加剧。

一次攻击可能导致损失数百万美元的故障停机、生产计划中断以及造价昂贵的机器设备损坏。在最严重的情况下，工人的健康或安全也可能受到威胁。甚至，会给制造企业带来错失创收和增加市场份额的机会。

整体策略

要在威胁愈加复杂、攻击手段成倍增加的环境下安全开展运营，现代制造商必须积极采用以威胁防护为中心的集成安全架构，覆盖攻击前，中，后的整个过程，构建连接基础设施、机器流程和人员的整体安全模式。

思科安全解决方案和服务旨在实现最佳的投资回报率和可衡量的业务成果，包括以下内容:

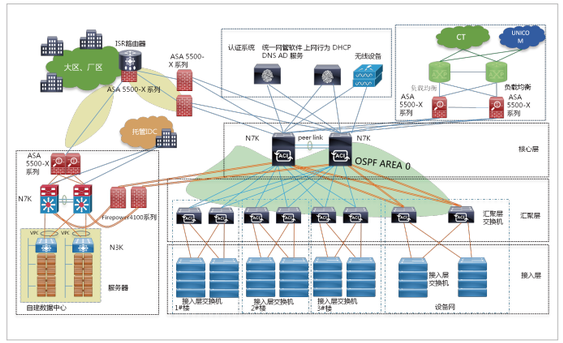
- 资产可视化和监控。思科能使企业识别和监控其网络中的所有资产和用户并为安全的远程访问奠定坚实的基础。
- 识别和访问管理。这些解决方案为供应商和承包商访问、设备加入合理化和动态策略实施提供便利。
- 工业 DMZ。思科的工业隔离区提供先进的外围网络缓冲区，在可信和不可信的网络之间执行数据安全策略。
- 网络地址转换 (NAT) 技术。这些 IP 解决方案精简了工厂范围内的机器设备网络，并提供额外的安全性，防止网络入侵。
- 工业网络安全服务。思科能分析网络风险、评估安全漏洞并设计和实施可减轻风险的网络及物理安全控制，借此帮助制造商保护工业资产和防止网络中断。
- 安全的运营托管服务。此项针对运营环境的模块化网络安全和合规解决方案可随企业需求的变化扩展，提供经济实惠的服务化交付选择。
- ICS 网络架构和设计服务。思科与制造商紧密合作，提供不仅能交付新一代安全性，而且能确保提升运营绩效和投资回报率的解决方案。

在如今万物互联的世界中，威胁状况不断发展变化，强大可靠的安全性对制造企业而言比以往任何时候都重要。由思科及其合作伙伴打造的互联工厂安全解决方案在这一新形势下设立了标准，制造商们正进入一个大胆尝试安全互联工厂的数字化新世界!

代表案例：农夫山泉股份有限公司

公司背景

- 农夫山泉股份有限公司是中国饮料20强之一，专注于研发、推广饮用天然水、果蔬汁饮料、特殊用途饮料和茶饮料等各类软饮料。
- 公司通过建设在八大优质水源地进行规模化生产，通过遍布全国的营销网络，将各产品分销至全国各地。



应用需求

- 农夫山泉未来不断新增业务应用以及对应IT架构，需防火墙具有可扩展性和高性能
- 在激烈竞争中，农夫山泉面对未知威胁日益增多，需要第一时间发现并实施处理
- 农夫山泉企业内部采购大量不同安全设备，需要彼此间快速协同和联动，降低管理复杂性

解决方案

- 思科 Firepower 4100 系列下一代防火墙为代表的安全解决方案
- 思科具备 Firepower 服务的 ASA 5500 系列下一代防火墙
- 思科 Talos 团队实时安全防护服务

公司收益

- 性能强劲，满足农夫山泉数据中心网络高吞吐/低延迟的需求。
- 专注于威胁防护， 为农夫山泉提供全方位的安全威胁防护
- 集成架构方案扩展性强，农夫山泉可以按需扩展，弹性增加更多新的安全防护功能， 节省投资
- 管理性强大，单一管理界面支持思科自身和第三方优秀安全解决方案的统一管理

金融行业网络安全解决方案

每个人都需要属于自己的银行

金融服务行业正经历巨大变化，金融服务专业人员需要在任何地方与客户合作；70% 以上的业务完全无需人工干预便可电子化完成。这些变化提升了数据、系统和网络的风险级别，网络犯罪通过恶意软件、钓鱼、勒索软件等方式进行攻击。

思科提供完善的金融行业网络安全解决方案，我们的方案由强大的思科 Talos 团队提供支持，可在全球不间断跟踪和监控威胁，并将该数据与我们的客户分享。最终实现最佳解决方案组合，全面保护业务和客户数据。

思科金融服务网络安全

这些解决方案满足了金融服务行业的需求，因为金融服务行业正转变为一种新的经营方式

我们的解决方案基于：

- 对安全领域的深入理解，让安全保护更有效的同时降低成本和复杂性。
- 我们帮助您改善自身的安全态势，并优化多供应商安全环境的效果。
- 弥补安全人才短缺的能力。思科可以提供所需的能力管理大型金融系统。

思科集成架构式安全解决方案旨在保护面向公司和客户的系统，防止遭受不断演变的安全威胁：

- Cisco Firepower NGFW 是行业首个专注于威胁的下一代防火墙 (NGFW)，其将部署数量最多的状态防火墙与应用程序控制、下一代入侵防护系统 (NGIPS) 以及高级恶意软件防护 (AMP)相结合。
- 思科网络威胁防御 使用自动化功能来检测、跟踪、发现和隔离高级威胁，并减少攻击可能性以及发现和修复的时间。Cisco Active ThreatAnalytics 将该功能以服务形式提供。
- Cisco Rapid Threat Containment 集成了思科身份服务引擎 (ISE) 和 Cisco TrustSec® 技术，以缓解并修复安全威胁。
- 身份和安全策略管理 可指定金融企业中不同职位人员和设备可以访问网络，以及可以执行哪些操作，控制对金融企业资源的访问。
- 网络可视性 思科提供网络可视性，例如在整个网络中启用流分析，可以更好地检测和规避内部威胁，例如僵尸网络、数据泄露和源自内部网络可以流量的其他攻击。
- 基于软件的细分 简化网络访问的配置，加快安全运营，并持续在网络的任何地方实施策略。
- 威胁情报 思科 Talos 团队能够通过对复杂系统进行智能大数据分析，为思科安全产品提供全面的威胁情报，为金融服务行业用户提供最为全面、实时的威胁防御。
- 安全服务 利用思科不同类型的安全服务，金融客户可以在遇到威胁和事件时，迅速得到思科服务团队的主动响应；发展并改善安全状态、安全策略，以及安全基础设施的有效性；通过电子靶场（Cyber Range）培训安全人员自身可以获得应对现代网络威胁所需的技能和经验，了解最新安全漏洞破解方法，如何利用高级工具和技术来根除威胁。

思科网络安全产品以及服务不仅在连续攻击的一个点上提供安全保护。它们会在每个事件期间、之前和之后保护您的组织。我们将这些解决方案与我们最好的高级服务结合起来，通过确定战略机遇来保护绩效，创造竞争优势，并从安全中获取长期可持续的商业价值，从而带来更好的结果。

代表案例：海银金融控股集团有限公司

公司背景

海银金融控股集团有限公司总部位于上海陆家嘴金融核心区。目前集团旗下拥有全资及控股子公司二十余家，员工人数约 5000 人，管理资产突破 1000 亿 人民币。集团业务已分布全球，海银通过资源整合优化打通投融资两端，建立一个由集团统一调配资源的运作体系，形成海银大金融的战略格局。

应用需求

- 集团将多家子公司业务进行统一调配资源的同时，也对数据中心进行集中化管理，各个子公司IT资源和业务应用都要求安全隔离。
- 海银集团化后面临更多数据生成、更多方式网络接入，需要更强大的整体防御能力支撑
- 作为金融行业对于客户商业信息异常敏感，需要从网络边界到网络内部，整体实现安全防御，并将安全防御覆盖到攻击的前、中、后全周期范围

> “思科的产品不仅满足海银集团对网络安全合规性的要求，对业务的持续稳定运行形成有效保障，为集团创造了一个安全规范的网络环境。”
>
> --海银金控 CIO

解决方案

思科 Firepower 4100 下一代防火墙产品为核心的集成架构式安全解决方案

- 思科 Firepower 4100 下一代防火墙虚拟化技术
- 思科具备 Firepower 服务的 ASA 5500 系列下一代防火墙
- 思科 ISE 身份认证服务引擎
- 思科 Talos 团队实时安全防护服务

公司收益

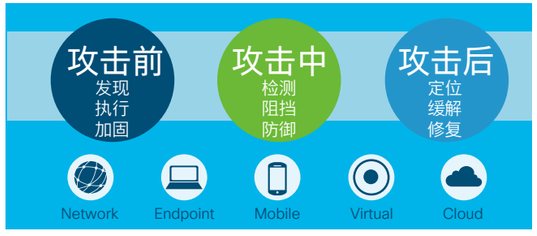
- 在数据中心多租户网络中保障业务数据的安全隔离，确保海银不同子公司多元化发展
- 全面的集成防护，在威胁发生之前就能快速发现，并自动操作隔离消除，提供全方位防护
- ISE 结合无线网络进行身份认证，让海银更灵活保护企业网络安全，消除未授权、有风险威胁用户隐患
- 在思科 Talos 团队服务支持下，第一时间响应最新威胁，实现快速精准防御

教育行业网络安全解决方案

在高等教育领域，网络威胁态势在不断发生变化，并日趋复杂和成熟，网络攻击正发展成为越来越复杂的以牟利为目的的行业，其中以勒索软件攻击更为典型。2017年的“永恒之蓝（Wannacry 勒索病毒）”的勒索软件，猖獗攻击国内各个高校，导致众多师生付赎金才能恢复被病毒加密的电脑文件，教学系统大面积瘫痪。这些威胁会严重干扰学生和教职员工的生活，学习，破坏学校等机构的可信度。

高校必须设法应对针对上述目标的威胁，维护有利于学习的网络环境。

覆盖整个攻击时间轴保护



- 在攻击发生之前，能够全面的了解整个网络的状况，通过实施细粒度的安全控制策略以及对系统/主机/流量等的加固措施，提高系统对攻击的防御能力，进而最大限度减少攻击的可能性
- 在攻击发生之中，需要采用智能分析和关联等技术，准确的检测出攻击所在，并且充分利用相关的设备和防御手段，对攻击进行阻挡和全面的防御
- 在攻击发生之后，可以通过入侵事件关联分析、异常流量分析以及恶意软件防护的攻击跟踪追溯技术，准确的定位出攻击的范围以及影响，并且做出有效的响应和修复，最大限度减少攻击的危害

在全周期的防御中，教育用户需要网络安全产品提供领先的威胁情报智能，有效保护自己网络。思科Talos团队能够通过对复杂系统进行智能大数据分析，为思科安全产品提供全面的智能的威胁情报，为用户提供最为全面、实时的威胁防御。

安全不仅是某一点的防范

安全需要无处不在，它不再是网络的某一点，而是网络中每个设备的基础和基本组件。教育机构必须在网络前端、互联网边缘直至接入层构建全面的安全性。

思科在解决方案中集成一致的安全实施。这些解决方案与现有的全数字化校园基础设施无缝结合，既涵盖个体需求，又能防御高级威胁，主要包括:

身份和安全策略管理

思科方案进行身份和安全策略管理，可指定哪些学生、访客、教职员工和设备可以访问网络，以及可以执行哪些操作，控制对校园资源的访问。

网络分段

思科可以基于安全策略进行网络微分段，控制访问权限并缩小受攻击面。

网络边界防御

思科可以通过 FirePower 下一代防火墙、入侵防御和 DDoS 防御，进行边界防护，规避损害网络性能和服务的尝试。

网络可视性

思科提供网络可视性，例如在整个网络中启用流分析，可以更好地检测和规避内部威胁，例如僵尸网络、数据泄露和源自内部网络的其他攻击。

终端安全

思科基于更快感知和更高准确性的智能威胁数据库，应对最复杂、最普遍的基于文件的安全威胁，保护终端安全。

远程访问控制

思科可以实施稳健的远程访问解决方案，确保学生和教职员工在家里访问系统时不会泄露敏感数据。

安全服务

利用思科不同类型的安全服务，高校可以在遇到威胁和事件时，迅速得到思科服务团队的主动响应；发展并改善安全状态、安全策略，以及安全基础设施的有效性；通过电子靶场（Cyber Range）培训服务安全人员自身可以获得应对现代网络威胁所需的技能和经验，了解最新安全漏洞破解方法，如何利用高级工具和技术来根除威胁。

代表案例：上海纽约大学

学校背景

上海纽约大学是世界一流大学美国纽约大学和中国著名高等学府华东师范大学在中国上海举办的具有独立法人地位的研究型大学，为中外合作大学联盟成员。该校与纽约大学阿布扎比分校、纽约大学纽约校区共同组成纽约大学全球系统中的三个具有学位授予权的门户校园。

应用需求

- 上海纽约大学需要多途径进行网络覆盖,包括有线和无线网络，对整体安全防范提出挑战
- 上海纽约大学要与纽约大学全球其他校区互联，进行网络互连的时候内部数据会产生泄露风险
- 学校建立了覆盖全校的高速网络，面对各种复杂的安全威胁，学校担心无法及时发现并处理
- 学校知名度高，每天大量本校职工、学生、教师、家长和其他访客在校园里面，缺乏行之有效的基于身份的网络访问控制手段

解决方案

采用思科全线网络安全产品和技术,来建设上海纽约大学的安全架构

- 通过 ASR 路由器和 DMVPN 与国外其他校区建立加密连接
- 互联网边界部署思科 Firepower 4100 系列下一代防火墙；数据中心部署 Firepower 4100 系列下一代防火墙
- 思科身份服务引擎(ISE)解决方 案用于访客的无线接入
- 终端设备部署了面向终端的高级恶意软件防护(AMP for Endpoint)，专门针对零日威胁和恶意代码实施安全防护
- 在核心、边界路由器上部署 ACL,进行严格访问控制
- 思科 Talos 团队实时安全防护服务

学校收益

- 上海纽约大学要与纽约大学全球其他校区互联，在符合纽约大学全球标准及进行网络互连的同时，在专线的基础上进行数据加密，严格保护内部数据安全
- 上海纽约大学要保证园区网络区域边界安全，需要对园区互联网边界、数据中心应用边界进行边界防护，同时针对互联网等复杂网络环境，通过部署思科 Firepower 下一代防火墙支持 NGIPS+AMP (高级恶意软件防护)功能实现对未知威胁的防护
- 针对学校职工、学生、校园访客等不同用户,进行不同等级、不同权限的身份验证以及访问控制授权要求

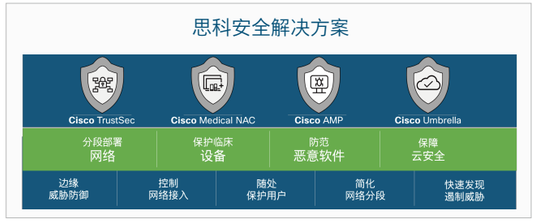
> “思科 AMP for Endpoints 和其他思科设备的深度融合，让上海纽约大学的安全防御 进入到一个新的阶段。让我们充满信心，脚踏实地去进行教育方面的创新研究。”
>
> --上海纽约大学CIO 常潘

医疗行业网络安全解决方案

随着医院信息化建设的不断深入，各级医院逐步建立部署了统一高效、资源整合、互联互通、信息共享、透明公开的医院信息系统。医院信息化飞速发展的同时，医院的业务系统面临的安全威胁也日益增长。

思科医疗网络与信息安全解决方案

传统的医疗网络是由多个物理隔离的网络组成的，这也有助于降低医院业务系统受到外部入侵的可能性。随着“互联网+ ”等战略实施以及越来越多外部信息互通的要求，医院内的HIS、PACS、LIS 等信息也越来越要求被第三方系统所访问以实现信息共享。



思科医疗网络与信息安全解决方案专注于医疗信息系统以下三方面:

全面提高可见性

我们无法保护一个自己根本就不了解的网络。对网络的全面可知，是医疗信息化管理员做出正确控制和防御策略的前提。利用思科的情景感知技术，管理员可以对医院内部网络的所有用户、移动终端、客户端应用程序、操作系统、虚拟机通讯、漏洞信息、威胁信息、URL 等相关信息实现全面可见性。思科众多的网络和网络安全组件都可以很好地支持情景感知技术。

关注威胁

我们需要以威胁防御为中心，利用整合的多种网络安全技术，以及最新的云智能，关注攻击发生的整个过程，在攻击发生的各个阶段，全面检查、了解和阻挡攻击，通过不断完善解决方案，保护医疗用户的网络，最快时间发现和解决网络中出现的安全事件，最大限度地减少恶意攻击带来的损失。

思科推出 Before-During-After 架构，覆盖攻击的整个过程

- 攻击发生前，能够全面了解整个网络的状况，通过实施细粒度的安全控制策略以及对系统/主机/流量等的加固措施，提高系统对攻击的防御能力，最大限度减少攻击可能性
- 攻击发生中，采用智能分析和关联等技术，准确地检测出攻击所在，并充分利用相关的设备和防御手段，对攻击进行阻挡和全面防御
- 攻击发生后，可通过入侵事件关联分析、异常流量分析以及恶意软件防护技术，准确定位出攻击范围及影响，并做出有效的响应和修复，最大限度减少攻击的危害

统一平台

网络安全，离不开网络，单单依靠独立的安全平台，无法组成一个有机的安全体系。思科将业界领先的网络基础架构平台和网络安全平台相结合，利用 SDN 以及 open API 等相应技术，在物理平台、虚拟平台、云平台上，提供全面的安全服务，包括情景感知、内容感知、访问控制、应用识别、威胁控制等安全服务。通过 open API 技术，思科的网络安全服务可与思科以及第三方相应技术，实现完美结合，进行统一安全防控和安全管理。

代表案例：北京贝瑞和康生物技术股份有限公司

公司背景

北京贝瑞和康生物技术股份有限公司是我国、乃至世界无创 DNA 产前检测领域的领导性企业，专注于样本采集运输、样本处理建库以及测序后数据分析等领域，发明大量专利性算法，在同行业中处于领先地位 。

> “以威胁为中心的集成式安全架构，给我留下了深刻的印象。这个架构完全不同于传统的安全方案，它更体现了强悍的性能、惊人的流量吞吐支持，以及融合架构式的快速威胁防护。包括它的弹性扩展能力，软件定义能力，更是颠覆了我们对安全防护产品的固有印象。这也保证公司能够将更多精力用于业务创新”
>
> --贝瑞和康 IT 总监

应用需求

- 内网因进行并行计算和高性能运算，进行基因测试应用，产生大量东西流量，普通防火墙无法正常承载公司业务扩展迅速，无法预料以后的数据增量，安全设备购买容易导致过度投资。
- 公司和第三方机构业务往来频繁，公司内部区域众多，容易受到各种威胁。
- 不同类型、不同品牌的安全设备并存且难以实现设备间联动协作，增加复杂性的同时并没有实现安全的有效性。

解决方案

思科 Firepower 4100 下一代防火墙产品为核心的集成架构式安全解决方案

- 思科 Firepower 4100 下一代防火墙
- 思科具备 Firepower 服务的 ASA 5500 系列下一代防火墙
- 思科 Talos 团队实时安全防护服务

公司收益

- 无惧数据中心的巨大数据流量，轻松实现检测和防护；同时对公司的办公楼层接入、网络管理与办公服务器区域等不同区域数据流量的实时全程安全防护
- 全局可视，快速洞悉安全威胁，哪怕是新出现的威胁风险，也能实现最短时间内的威胁检测发现
- 简单高效安全管理，让客户能够精简运营，并更加经济高效地满足企业用户的独特要求

思科安全荣誉

思科拥有业界最为全面的安全解决方案，涵盖了从网络安全、内容安全、高级威胁防御以及安全策略与访问控制等多个技术范畴，从应用场景上，也包括了像虚拟化、云、终端、网络、移动设备、工控网络等，真正实现了安全防护无处不在。

思科是整个安全设备市场领导者，占据全球30%以上的市场份额。思科的安全解决方案在 NSS LAB 多年的评测中，拥有最佳的安全防护效率。使用了思科的网络安全解决方案，也让我们的用户将对威胁的检测时间，从业界平均的100天以上，减少到了4.6个小时[1]，大大的加速了用户发现问题的进程，减少了因为恶意威胁造成的损失。

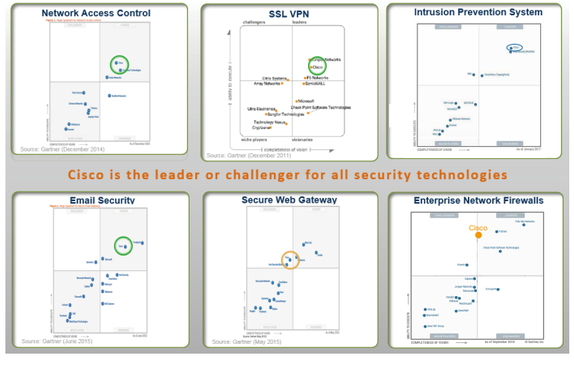
[1] 思科2018年度网络安全报告系列

思科安全产品在 Gartner 魔力象限中处于领导地位

Gartner®

在 Gartner 连续几年对安全产品的魔力象限评测中，思科的安全技术在各个领域的最新象限当中，都一直处于领导者的位置，包括：网络准入控制、SSLVPN、威胁防御、邮件安全、Web 安全和下一代防火墙。Gartner 也相当认可思科在近两年安全领域的努力，从整个公司层面获评正能量安全公司!

Gartner 在企业级防火墙产品的魔力象限评测中特别指出，思科企业级防火墙被认为具备最佳执行能力，同时在高级威胁防御方面，拥有其他友商无法比拟的优势（例如 AMP 和网络以及终端安全的深度集成），并提供完整解决方案。



2018 Gartner Peer Insights 客户首选企业网络防火墙

Gartner peerinsights customers' choice 2018

请扫码阅读详情

专业之选

思科荣获 Gartner Peer Insights 颁发的客户首选企业网络防火墙奖项。

思科荣膺 Frost & Sullivan 最高荣誉，引领全球防火墙市场

思科荣获 Frost & Sullivan 颁发的 2018 年全球网络防火墙市场的市场领导者奖。Frost & Sullivan 将防火墙市场领导者定义为 “能够识别市场中的各种需求并不断推动其防火墙平台发展以满足当前和未来需求的企业”。这一领导者奖项是对思科在市场上提供最佳下一代防火墙、成为客户首选安全合作伙伴这一承诺的认可。

Frost & Sullivan 表示：思科防火墙可以满足各种不同用户的需求。思科 “是在整体市场中唯一排名位居前四的供应商，同时也是全部四个业务规模细分市场（中小型商业机构、大型商业机构、企业和大型企业）中排名位居前三的供应商 - 切实证明了思科有效调整其防火墙产品线以满足广大客户的各种需求的能力。

思科的 5500-X、2100、4100 和 9300 系列下一代防火墙可提供多种不同的吞吐量和使用案例。客户可以选择在本地或云端部署和管理防火墙。无论使用案例如何，思科皆可提供适合您的最佳下一代防火墙。

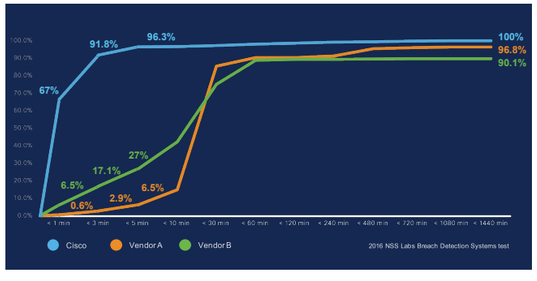
NSS Labs 漏洞检测系统(BDS)测试

在2016年度NSS Labs漏洞检测系统（BDS）测试中，思科安全解决方案连续第三年处于领先地位，对恶意软件、漏洞攻击和逃避技术的检测率均达到100%。

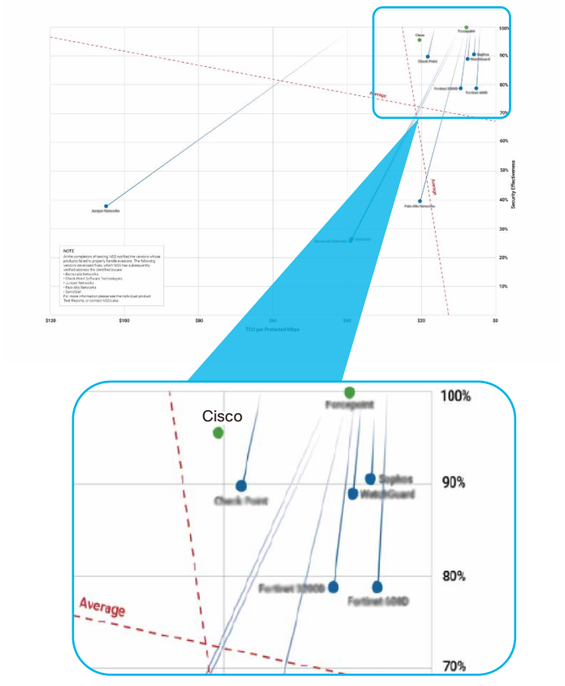
产品				漏洞检测率		NSS 的吞吐量测试结果	
具备 NGIPS v6.0 和高级恶意软件防护的思科 Firepower 8120				100.0%		1,000 Mbps	
误报率	路过式漏洞攻击	社交媒体漏洞攻击	HTTP 恶意软件	SMTP 恶意软件	离线感染	逃避技术	稳定性与可靠性
0.33%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	通过

面对不断演进的攻击，检测安全实践的有效性尤为重要。思科一直致力于减少“检测时间（Time to Detect，即TTD）”，即减少发生威胁到发现威胁之间的时间差。缩短检测时间，对于限制攻击者的操作空间和最大限度减少入侵造成的损失至关重要。

在2016年度NSS Labs漏洞检测系统（BDS）测试中，思科安全解决方案实现了在所有待测产品中最快的检测速度，3分钟内就可以检测出91%以上的威胁。



NSS Labs 2017下一代防火墙(NGFW）安全价值图



NGFW在互联网出口检测并阻挡恶意勒索软件的进入：思科下一代防火墙（NGFW）产品凭借出色的自适应能力，采用威胁防御为核心的设计架构，能够在攻击发生的整个过程提供威胁保护。在 NSS Labs 最新发布的2017下一代防火墙（NGFW）安全价值图（Security Value Map）中，思科下一代防火墙 Firepower 处于领导者位置。

Cisco Identity Services Engine (ISE)

ISE 被《SC 杂志》评为“2018 年最佳 NAC 解决方案”
今天的员工、访客需要通过更多的设备，访问更多的网络资源，随着网络扩展，这一切将变得更加复杂，如何让人们访问正确的网络资源和应用程序，维护设备和行为可见性，控制风险的复杂性变得越来越复杂，未能识别、修复的安全威胁越来越多，潜在影响呈指数增长。

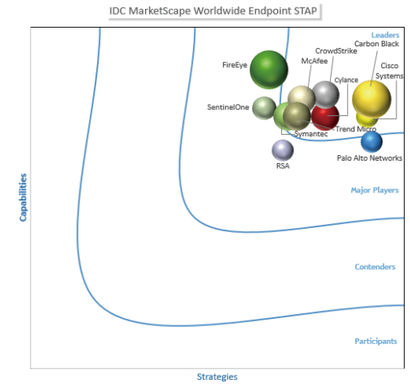
思科ISE 可使企业更加轻松进行访客访问和管理，利用 移动和桌面访客门户，企业只需几分钟即可完成访问权限的创建，全面管理访客访问的各个方面。

与此同时思科ISE对于自带设备和企业移动设备的简化让人印象深刻，ISE 提供开箱即用的自助式设备自行激活和管理设置，十分易于使用。

ISE通过集中和统一网络访问策略管理，提供高度安全的无差异访问体验：无论最终用户是采用有线连接、无线连接还是 VPN 连接，都能安全且一致地连接到企业网络。

利用 ISE，客户可以创建基于角色的灵活访问控制策略，从而在不增加复杂性的情况下实现动态的分段访问。基于终端身份进行流量分类的功能，确保客户在更改策略后无需重新设计网络。
同时借助与合作伙伴解决方案共享情景数据，可加快识别、遏制和修复网络威胁的速度，并通过执行ISE身份引擎中的访问策略变更来遏制威胁，从而阻止威胁在整个网络中的蔓延。

IDC：2017 终端安全市场领导者



面向终端的思科 AMP 在2017年终端安全 IDC Marketscape 报告中荣膺“领导者”，充分肯定了思科 AMP 高级恶意软件防护在攻击防御、监测和响应中的领先技术和卓越表现。

思科 AMP (高级恶意软件防护) 技术，提供基于网络和终端的恶意软件防护，超越了单纯时间点检测方法，可在攻击的整个过程（攻击前、攻击中和攻击后）对文件和流量进行持续分析，能够回溯并跟踪文件的传播活动和通信，有助于实现追溯性安全，帮助用户了解感染或威胁的完整范围，确定根本原因并进行防御。

面向终端的思科 AMP 获得 NSS Labs“推荐级”殊荣

查看为什么面向终端的思科 AMP 首次参评便获得 “推荐级”殊荣，在效力和最低总拥有成本 (TCO) 方面均名列前茅。

请扫码阅读详情

思科邮件安全连续第三年被 Radicati 评为电子邮件网关的市场领导者

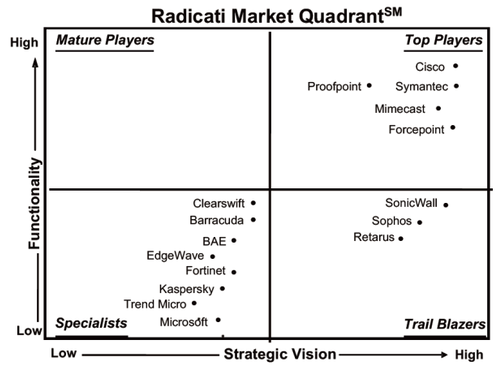


Figure 3: Secure Email Gateway Market Quadrant, 2018[8]

思科邮件安全可以在整个攻击过程中通过简单，开放，自动化和有效的安全性保护组织免受勒索软件，电子邮件欺骗，网络钓鱼，高级恶意软件和其他威胁的侵害。思科邮件安全产品包括：云邮件安全（CES），邮件安全设备（ESA），虚拟邮件安全设备（ESAv）和混合部署(Cloud and On-Premises)

思科StealthWatch 加密流量分析技术荣获 WITAwards 2017年度「技术变革」大奖

思科 StealthWatch 加密流量分析技术可以在无需对加密流量解密的情况下，运用网络感知分析方法识别隐藏在加密流量中的恶意软件。该系统针对加密流量内部的元数据进行机器学习算法分析，准确定位加密流量中的恶意模式，实现更快更精准的判断，帮助企业快速确定可能受到感染的设备和用户，最终提升企业面对安全事件时的响应速度和水平。准确率 超过99.997%。