金融行业网络安全解决方案

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。

思科勒索软件防御解决方案

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

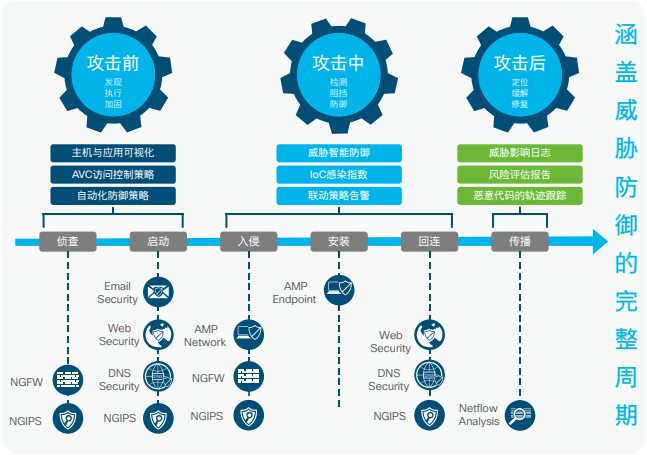
使用更有效的安全方法降低勒索软件风险

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：

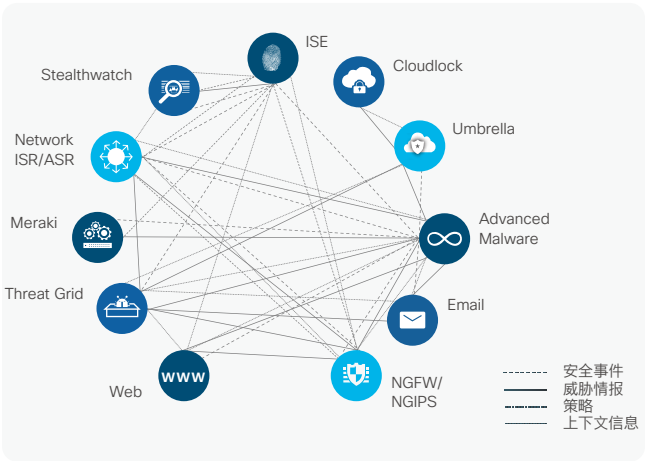
- NGFW 与 NGIPS 在互联网出口检测并阻挡恶意勒索软件的进入
- 面向终端的思科高级恶意软件防护 (AMP) 可以阻止勒索软件在终端上打开
- 配备高级恶意软件防护 (AMP) 的思科邮件安全可阻止垃圾邮件和网络 钓鱼邮件以及恶意邮件附件和 URL
- Web 安全网关拦截钓鱼网站的访问
- 思科 Stealthwatch 能够实现网络可视化与异常行为分析，通过与现有的网络基础设施配合，检测终端 C&C 连接行为，并且可以与ISE 联动实现对网络进行动态分段阻止勒索软件内部扩散
- Umbrella (OpenDNS) 服务切断恶意域名解析，在 DNS 层实现预先阻止勒索软件
- 针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

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

免费试用思科邮件安全方案

免费为您的网络进行安全检查

致电: 4006 680 680

北京
北京市朝阳区建国门外大街2号
北京银泰中心银泰写字楼C座7-10层

邮编：100022
电话：（8610）85155000
传真：（8610）85155960

上海
上海市长宁区红宝石路500号
东银中心A栋21-25层

邮编：201103
电话：（8621）22014000
传真：（8621）22014999

广州
广州市天河区珠江新城珠江
东路6号周大福金融中心24层
03-06室
邮编：510620
电话：（8620）85193000
传真：（8620）85193008

成都
成都市滨江东路9号B座
香格里拉中心办公楼12层

邮编：610021
电话：（8628）86961000
传真：（8628）86961003

武汉
湖北武汉市江岸区京汉大道
1398号企业天地2号11楼
11-08、11-09、11-10单元

邮编：430014
电话：（8627）8229 2500
传真：（8627）8316 2650

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