



思科安全解决方案助力海银洞悉威胁，守护客户的信任



“对于金融属性的公司来讲，客户选择我们的重要标准是值得信任、可靠、提供全方位服务。”

——海银金融控股集团首席信息官 楚仕嘉

审时度势，海银作为首屈一指的金融企业，着眼国际化视野和布局，引领着中国金融行业的变革。但以不变应万变，如何获得客户和社会的信任始终尤为重要。

海银金融控股集团首席信息官楚仕嘉认为，数据安全是信息化商业社会的生命线，对于金融集团更是如此。通过建立防范意识，并借助专业数据安全机构的全方位把控，海银才能在全球化布局、以及中国资本市场的变革之中，做到游刃有余。也只有如此谨慎，才能确保对每一位投资者的资产安全，才能获得客户百分之百的安心和信任。

对网络上每一个流动数字的保护 就是对企业信任的维护

金融企业的发展，一定是建立在客户信任之上，任何一个微小的信任危机都可能将雄心建立的商业帝国毁于一旦。保护客户的信任，就要保护好客户的财富和价值，而在数字化时代的今天，保护财富需要从保护网络数据开始。

海银金融控股集团（简称：“海银”）作为一个金融属性的集团，面对信息安全不再仅是“降低风险”，而是对数据资产进行全方位保护，以支持公司业务创新，确保集团国际大金融格局的顺利实现。

思科安全 助力海银开启金融安全新视野

面临正在加快全球化布局的海银，要实现更多金融类业务的快速上线，快速的业务扩张。因此业务体系人员不断庞大，每天都会产生海量的数据。

作为对信息安全高敏感的金融行业，数据安全保护和安全合规性是重中之重。海银面对业务架构调整，所带来的直接问题就是，既要满足金融行业严格的安全管控、统一的安全访问策略要求和安全合规性要求，还需要建立有强大的安全防护架构，保持集团业务的稳定性。

思科与海银展开深入合作，思科凭借全数字化安全解决方案，为海银部署了Firepower下一代防火墙，使用了ISE身份认证引擎服务，并通过思科TALOS团队的全球威胁情报实时防护，海银做到对待安全风险能够自动感知、自动隔离、自动分析，并全面可视。遇到威胁快速识别响应，保障了金融客户数据的安全。

“全面部署思科安全解决方案之后，集团网络可以共享，网络资源得到重新调配，实现了资源利用的最大化、高度化和精准化，并保障了业务稳定性。”

——海银金融控股集团IT安全高级项目经理 冉庆坤

专注威胁防御 实现网络威胁的可视化

作为国际化发展的金融集团，意味着业务类型更加丰富。目前海银在国内外拥有130多家分支机构，要保证集团不断产生的海量数据在网络上的正常传输，就需要能够做到安全的快速部署，与虚拟隔离，并且具备应用层防护功能，保证集团数据的安全及合规性。



事前匹配

通过APIC-EM完成VLAN策略的预配置，再用ISE验证所有接入终端，使它们匹配到不同的角色，最后分配于不同的VLAN中，完整的准入策略就生效了。

事中监测

当监测到正在使用中的终端有非安全行为时，将其置于临时隔离区中，保证网络安全。确认其无安全风险时，再分配于合适的网络中。

事后分析

Firepower与ISE强大的报表功能提供了详细的终端接入分析情况，据此不断优化预配置策略，以确保安全策略可以完成闭环。使得海银的管理便捷高效，最大可能释放了员工生产力。

海银在网络边界和数据中心均部署了思科Firepower下一代防火墙，集成业界领先的NGIPS和AMP（高级恶意软件防护）功能的思科Firepower，可完全实现“全栈可视性”、“专注于威胁”等重要功能特点。基于思科Talos安全情报的AMP（高级恶意软件防护）可以持续分析和追溯警报，为海银提供不只是单个时间点对高级恶意软件的检测、分析、遏制，配合IPS、状态防火墙等涵盖了网络的攻击前、攻击中和攻击后的完整的攻击周期，实现了快速有效的架构式安全防护。



“海银金融控股集团作为金融公司，在网络边界和数据中心部署ISE身份认证服务引擎，解决了不同设备再接入网络时的身份识别与策略分配。”

——海银金融控股集团IT安全高级项目经理 冉庆坤

共享全球威胁情报 实时提供全面威胁防护

海银正在加快全球化战略布局，海外业务逐渐增长，企业终端分散在海外各个地区，受到网络攻击面扩大。思科TALOS团队还为海银提供基于全球视野的安全防护，通过思科TALOS团队的支持，可以在第一时间响应最新的威胁，实现快速精准的防御。

思科TALOS团队构建了世界顶尖的威胁检测网络，采用自动化安全大数据方法分析来自全球的邮件、网站和超过1亿5千万网络终端设备的威胁情报，每天可以分析全球1/3的邮件总量，分析超过150万独立恶意软件样本，收集大约160亿网站的请求。Google每天的搜索量大约为35亿次，思科TALOS收集分析的量是这个数字的4.5倍。

目前根据最新的思科2017年中网络安全报告，思科已实现将行业平均威胁检测时间从100-200天，降至3.5小时，快速洞悉威胁，并形成阻隔，从而实现有效的安全防护。

持续进化的网络安全防御 助力海银不断突破陈规

随着越来越多企业实现全数字化，大量服务和应用都将采取加密技术作为确保信息安全的首要方法。对于使用互联网通信并在线处理业务交易的金融企业而言，加密技术可以为其提供更强的隐私性和安全性。Gartner认为，2019年将有一半的恶意软件活动采用某种加密技术来掩盖恶意软件传送、命令和控制活动或数据泄露。

海银的数字化改变赋有前瞻意识并能够与国际领先的科技接轨，运用国际化眼光的战略思维引领行业变革发展，未来更将会部署思科Stealthwatch全面可视，更可在无需解密时使用网络分析方法识别恶意软件。思科以威胁防护防护为中心全方位的安全解决方案正在为海银国际化布局保驾护航。

思科安全助力海银 把握数字化转型机遇

思科通过超过十年的网络安全研究和洞察，借助其领先的技术，构建全面安全防护架构，实现简化运维，帮助海银根据业务需求快速部署，让新业务从测评到上线时间缩短了70-80%，获得更多安全收益。也让金融行业的IT部门人员工作产生了质变，核心价值从执行升级到安全策略的制定和部署，以支持集团业务的不断创新，让企业国际化发展中大胆布局，充分把握全数字化转型机遇。



具备 FirePOWER 服务的 ASA 5500-X



Cisco Firepower 4100 系列



Firepower 2100 系列



Cisco Firepower 9000 系列

[点击了解思科Firepower下一代防火墙](#)

☎ 致电: 4006 680 680

北京
北京市朝阳区建国门外大街2号 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: 2001103
电话: (8621)22014000
传真: (8621)22014999

广州
广州市天河区林和西路161号中泰国际广场A塔34层
邮编: 510620
电话: (8620)85193000
传真: (8620)85193008

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。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作关系。(1110R)

出版日期: 2017 / 10

©2017思科及其子公司版权所有

Page 03