



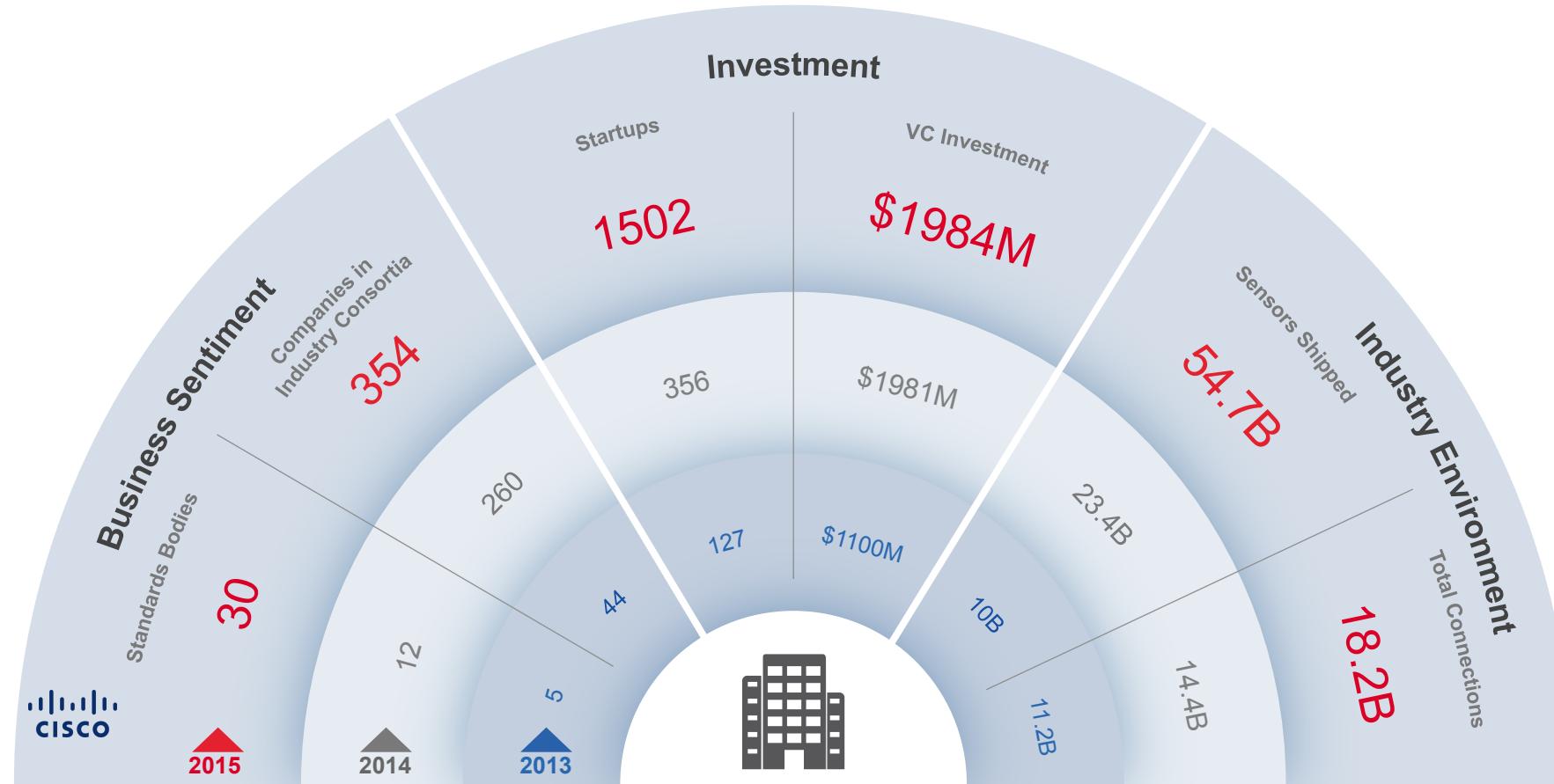
Cisco 2016 年度安全报告

Hongtao Xu

Hongtxu@cisco.com



我们正进入数字化时代



安全报告基于思科全球范围内的遥感勘测数据

每天**160亿**的Web请求

每天**5000亿**的Email通讯

每天阻拦**200亿**的威胁

每天110万的恶意软件样本

 每天**185 亿**的恶意软件查询

2015年的安全能力基准研究



从2015年夏天
开始进行



对12个国家的企
业用户进行研究

US	Italy
Mexico	Russia
Brazil	India
UK	Australia
France	China
Germany	Japan



超过2400 个用户
的调查回应

首席安全官	45%
安全运营官	55%
• 大型企业	13%
企业	38%
中型企业	49%

议程

- 网络威胁分析
- 企业防御状况分析
- 业界见解与展望

网络威胁分析

网络攻击产业化，经济利益是第一目标。更加的灵活、动态

直接的攻击产生大量的利润

Angler主要藏身于Limestone和hertzner两个服务托管运营商

! Angler 收入

147

每月重定向
服务器数



90K

每台服务器每天受到的
目标攻击数



10%

遭受漏洞攻击



40%

受到入侵

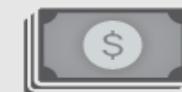


62%

交付勒索软件



X



300 美元

平均赎金金额



3400 万美元

每个攻击活动勒索软件
获得的总年收入

2.9%

支付赎金

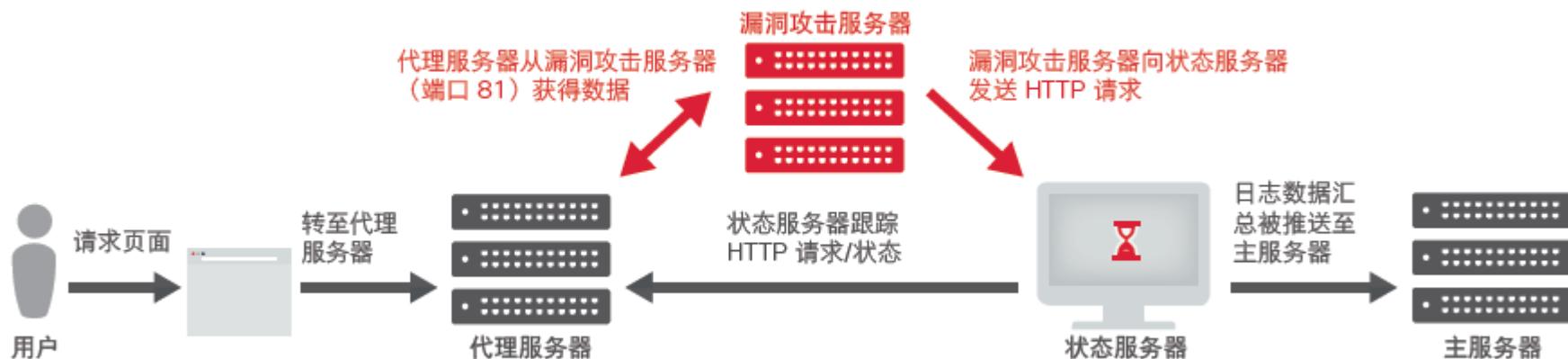


9515 个用户每月支付赎金

攻击者的架构更加灵活

灵活的设计，更容易逃避检测，重建

图 5. Angler 后端基础设施



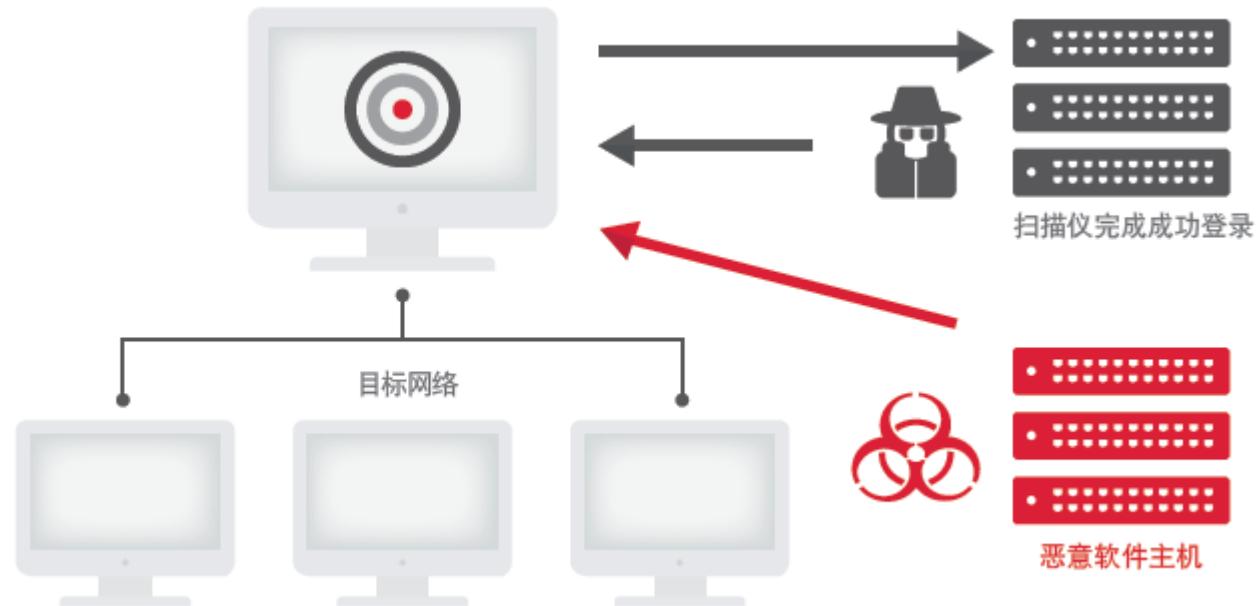
来源：思科安全研究部门

对SSH精神病的拦截

全球协同攻击



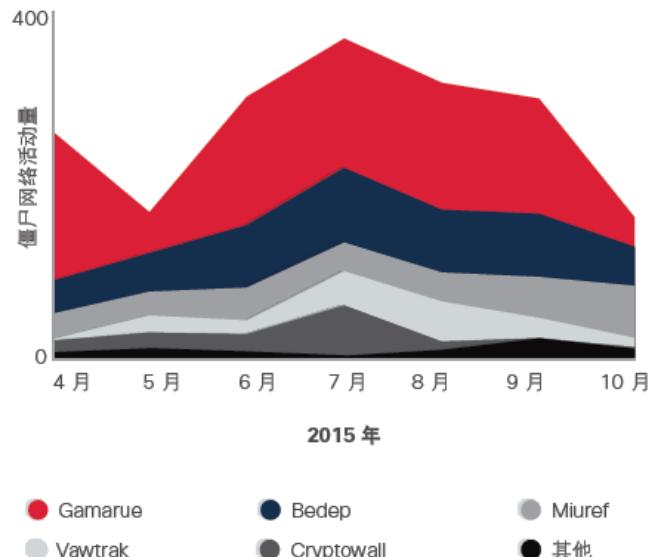
SSH 暴力破解攻击尝试
(30 万个唯一密码)



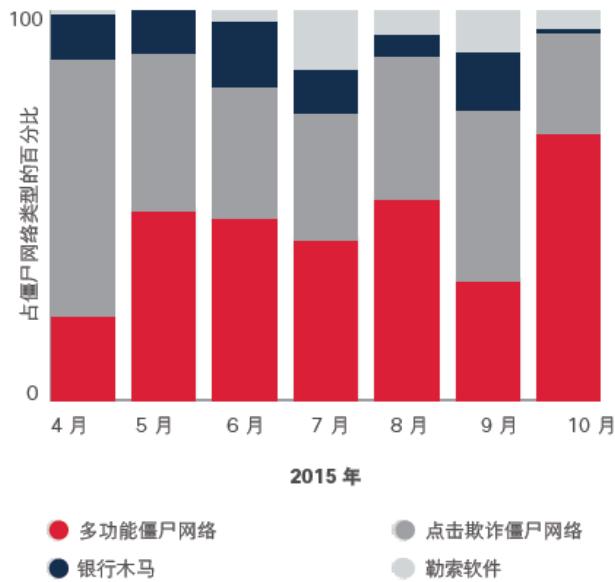
2015全球僵尸网络概括

2015主流恶意软件

图 10. 各项威胁的增长（感染用户的比例）



2015僵尸网络类型

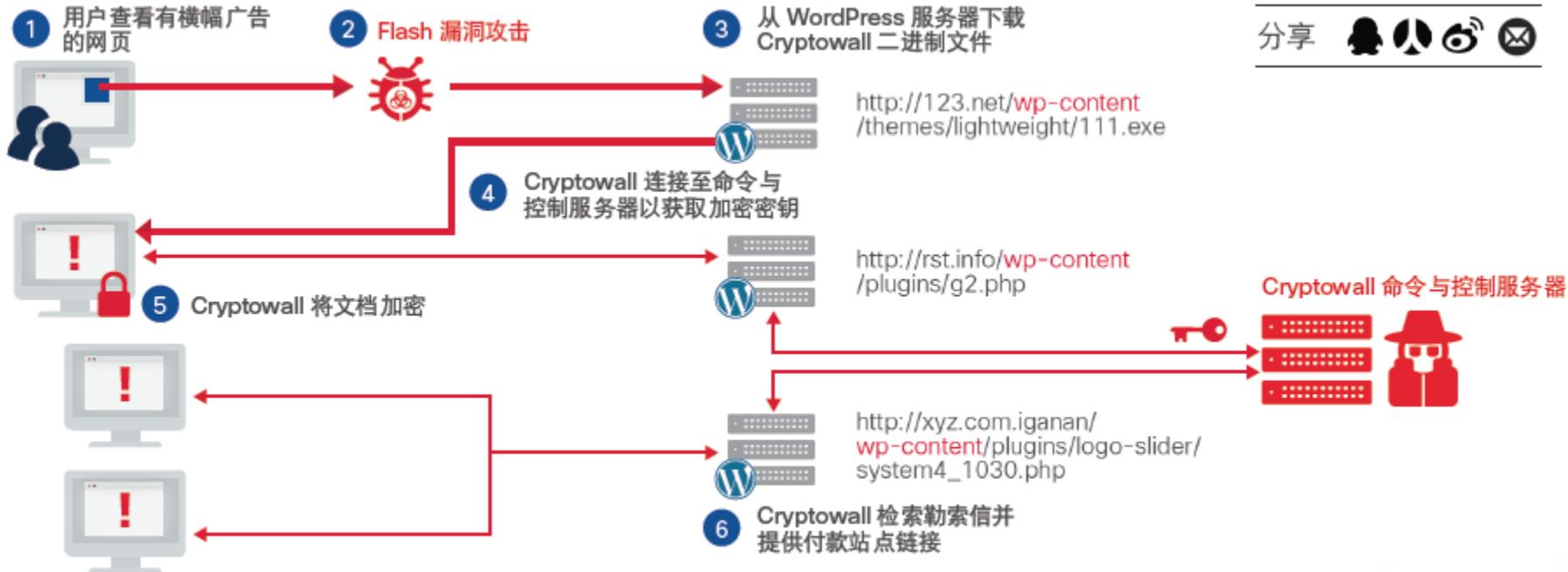


来源：思科安全研究部门



存在漏洞的基础架构，被快速广泛的利用

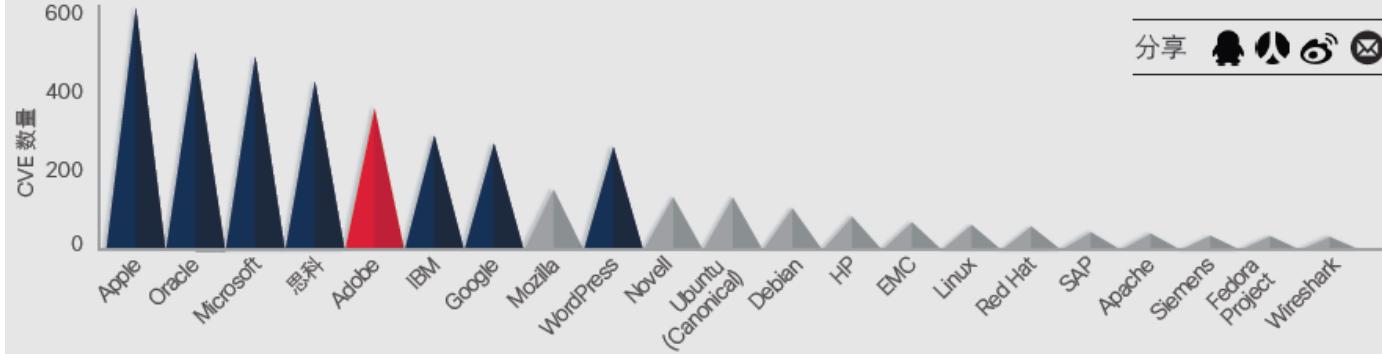
存在于WordPress的攻击，增加了221%



2015主要漏洞分布

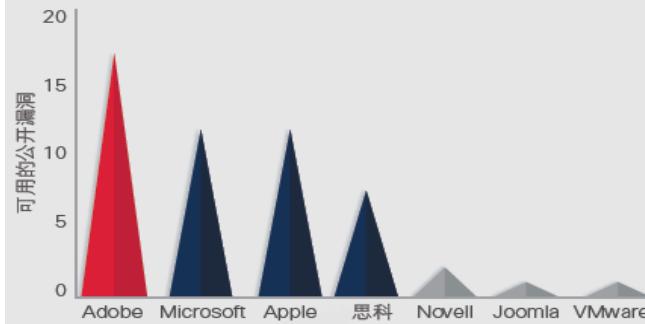


图 18. 按供应商划分的 VE 总数



分享

来源：思科安全研究部门美国国家漏洞数据库

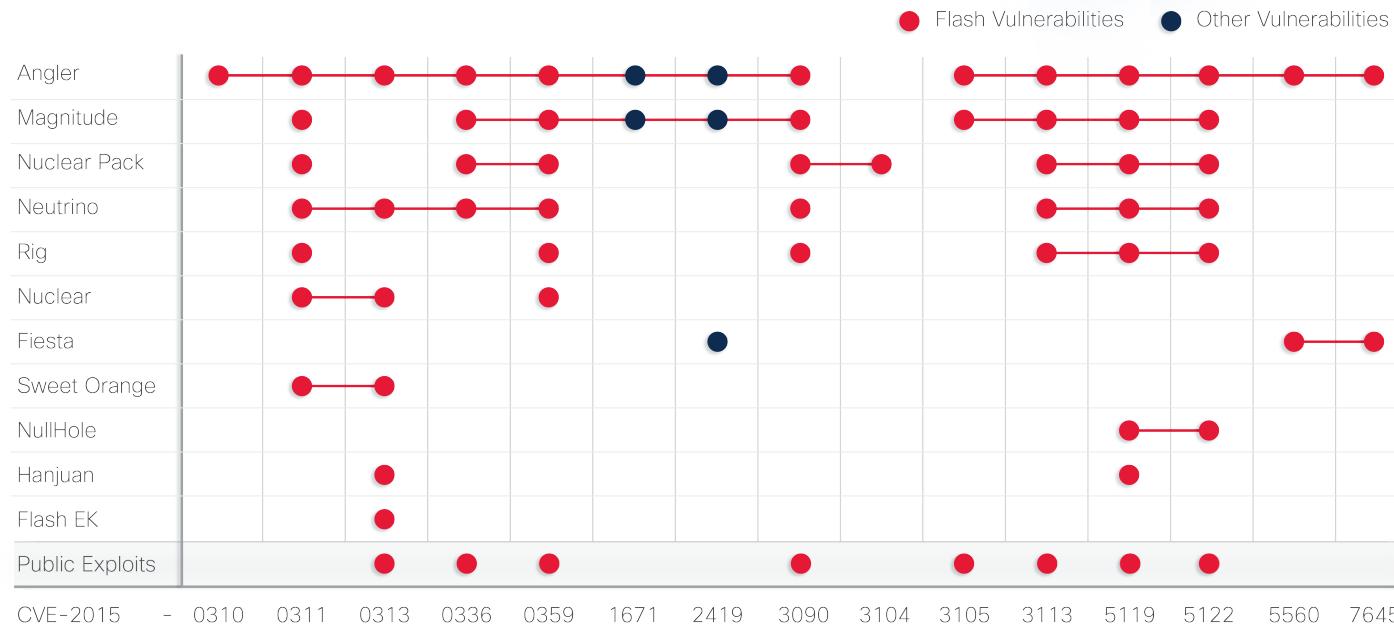


上图显示2015年按照供应商划分的漏洞总数

左图显示攻击可以利用的漏洞数目

来源：思科安全研究部门 Metasploit 漏洞攻击数据库

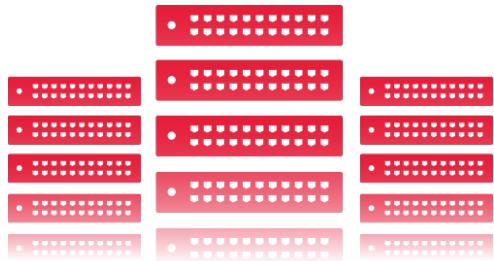
Web攻击: Flash漏洞被最多利用



Flash平台是网络犯罪分子很喜欢的一种威胁载体

DNS: 需要关注更多

网络中的盲点，攻击者利用DNS获得的控制，偷走数据，并重定向流量



91.3%

的恶意软件在攻击中使用了DNS



68%

的企业不监控DNS

浏览器感染：一直存在的问题



超过

85%

的企业每月都存在被恶意的
浏览器插件感染

企业防御现状分析

信心在下降,但是安全意识的提升将促使企业更多的投入

层出不穷的安全事件，导致威胁防御信心下降



59%

的受访者自信拥有最新的技术。

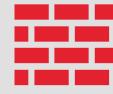
-5%



51%

的受访者高度自信能够事先检测到网络中的安全弱点。

0%



54%

的受访者自信可以阻挡恶意的攻击威胁

-4%



45%

的受访者自信能够定位和缓解威胁

-1%



54%

的受访者自信能够验证攻击

+0%



56%

定期审计自己的安全策略

+0%

基础设施老化:10年累积的问题

92%

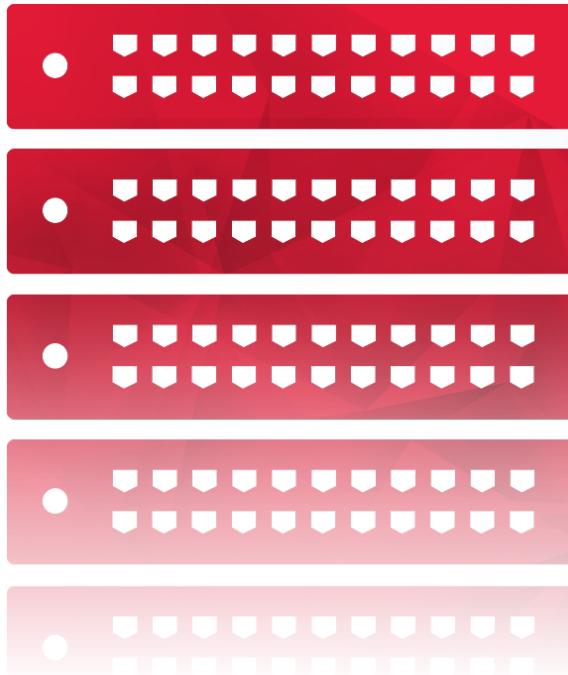
互联网上的设备，存在已知的漏洞，平均每台设备有26个漏洞

31%

互联网上的设备，已经停止了服务

5%

互联网上的设备，已经中止了生命周期，金融/运营商/医疗/零售



提升安全能力的障碍

安全团队在执行他们计划的时候会受到一些限制

图 42. 预算限制是安全升级的主要障碍



对安全问题的担心驱动了用户的投入

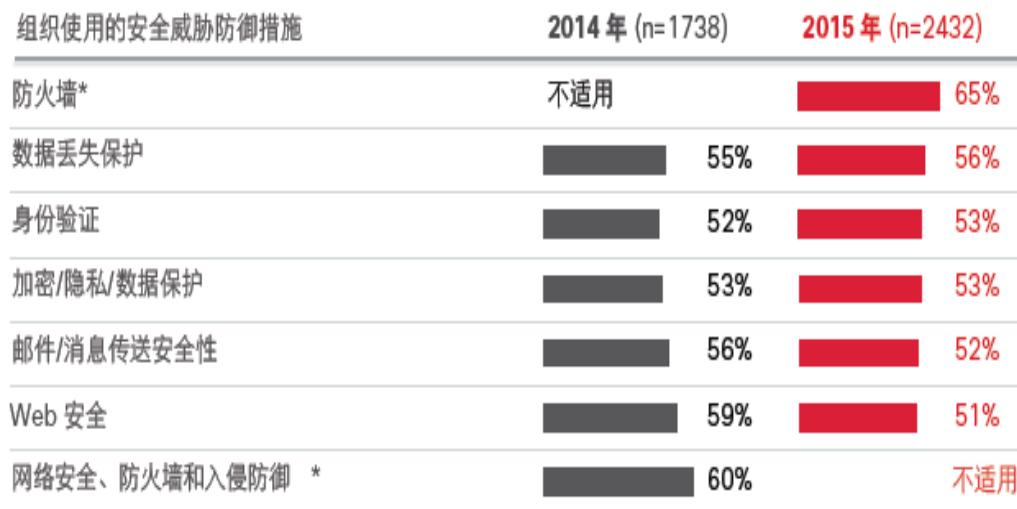
更多的企业正在采取措施抗衡逼近网络的威胁。.

安全意识和专业培训	90%	+1%
正式书面的安全策略	66%	+7%
外包的审计和顾问服务	52%	+1%
外包的事件响应服务	42%	+7%
外包的威胁情报服务	39%	N/A



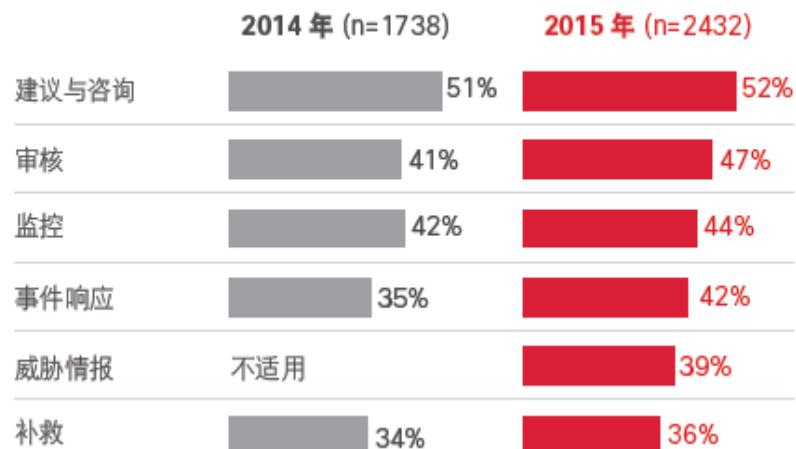
目前最为常用的安全工具

防火墙和数据丢失防护是最常用的工具



安全服务外包在增加

哪些安全服务是外包的？

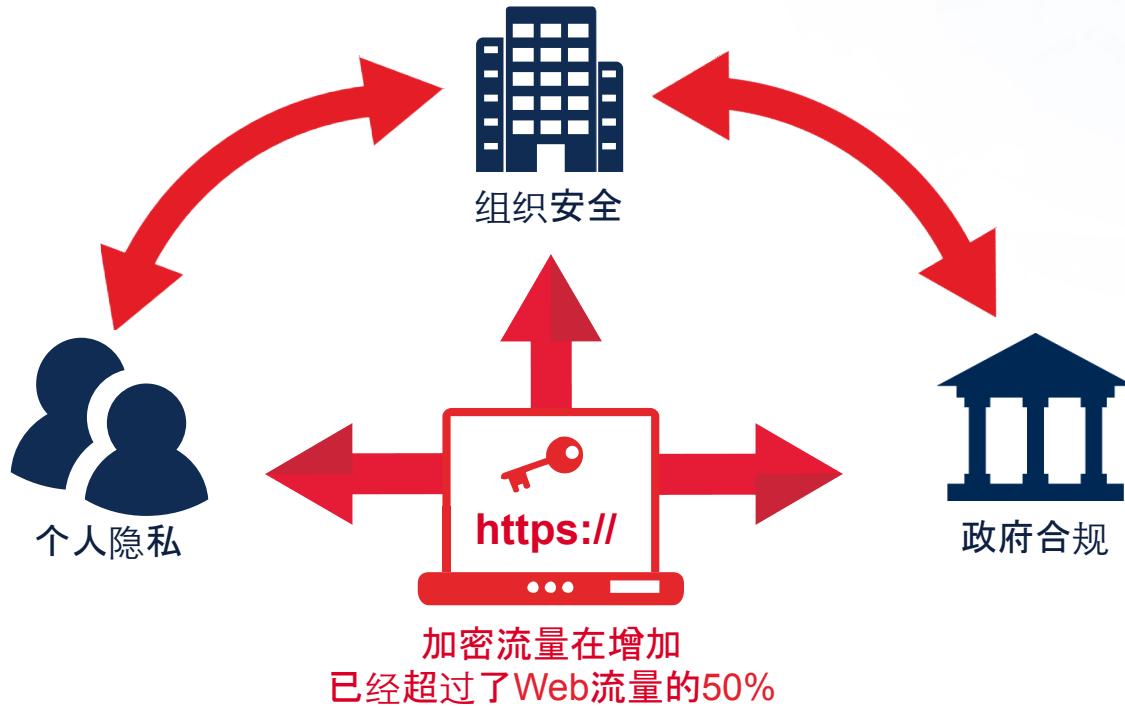


* 防火墙和入侵防御在 2014 年是一个代码：“网络安全、防火墙和入侵防御”。

行业见解与展望

加密流量：日益发展的趋势

Web流量加密的趋势，会使防御者更难去跟踪威胁，造成了防御的盲点。



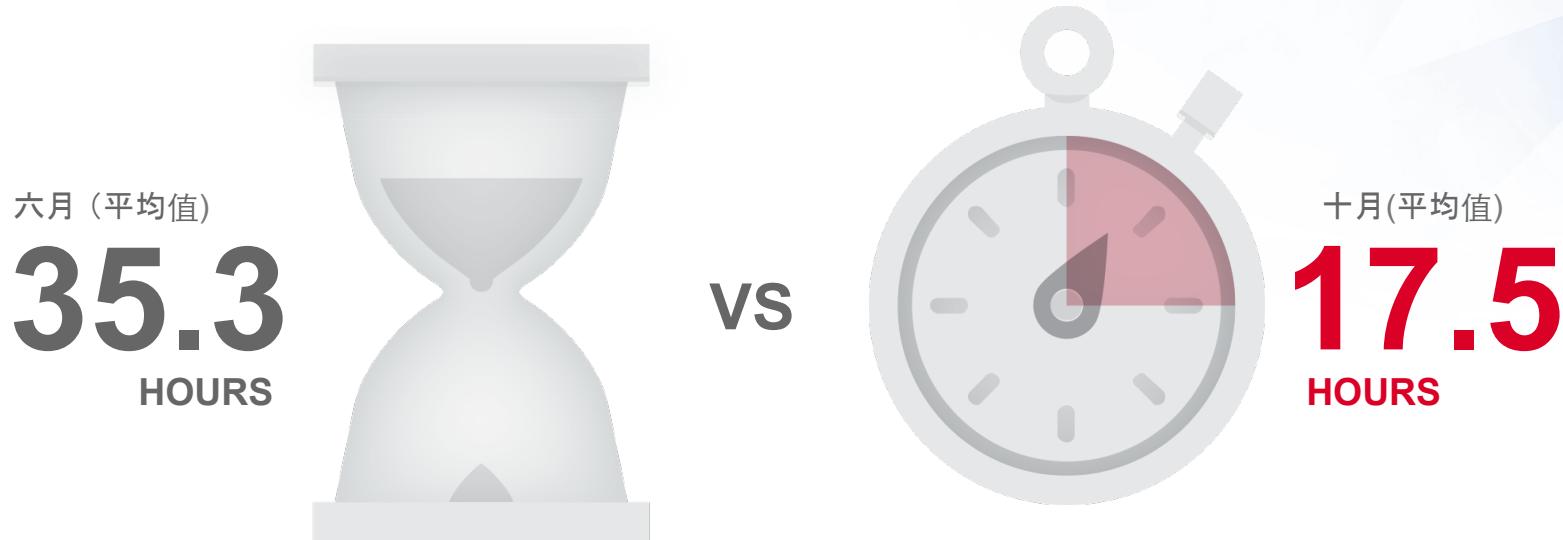
集成式威胁防御的六个原则

1. 需要使用更为丰富功能的网络和安全基础架构
2. 单凭独立的“一流”技术，无法应对当前最新的威胁，反而会提高网络复杂性。
3. 集成式的威胁防御必须能够检测/阻挡加密的恶意活动
4. 开放式的APIs 至关重要
5. 必须减少要安装和管理的设备和软件数量
6. 利用自动化和协作，来减少检测时间，快速的缓解和修复威胁。

团结就是力量：协作至关重要



检测时间TTD: 减少恶意攻击者的操作空间



恶意软件的快速识别(threatgrid)和可追溯的安全设计
使思科的对未知威胁的检测时间大大低于目前业界的平均值100-200天

企业高管对网络安全的关注度



48%

的高管非常担心自身企业的网络安全

41%

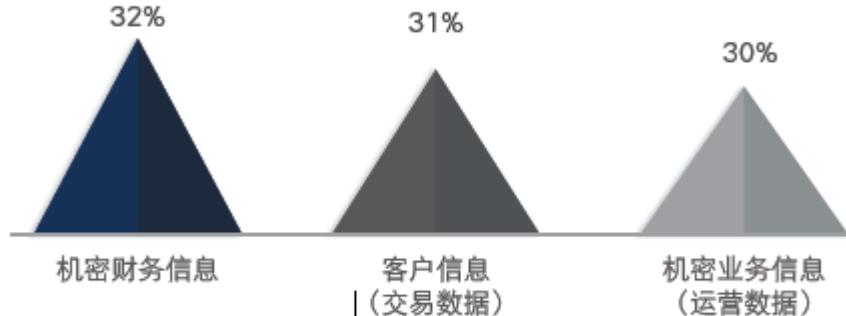
表示与三年前相比，他们对网络安全的担忧增加

92%

同意应该提高更多的网络安全相关的信息

企业对安全风险的看法

图 63. 高管对保护关键数据安全的担忧



来源：思科安全研究部门



图 64. 对安全风险的看法



企业认为组织的基础设施在以下方面存在很高的安全漏洞风险：



来源：思科安全风险和可信度研究

企业所面临的安全挑战

图 65. (全部受访者) 所面临的外部挑战

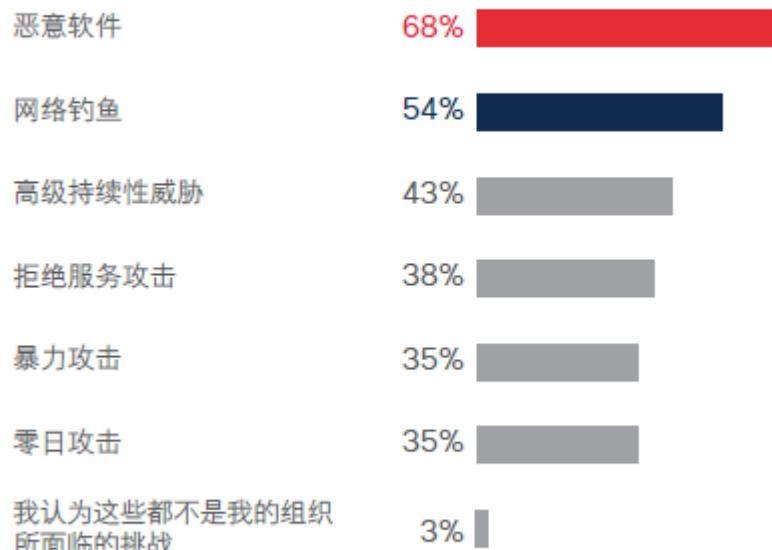
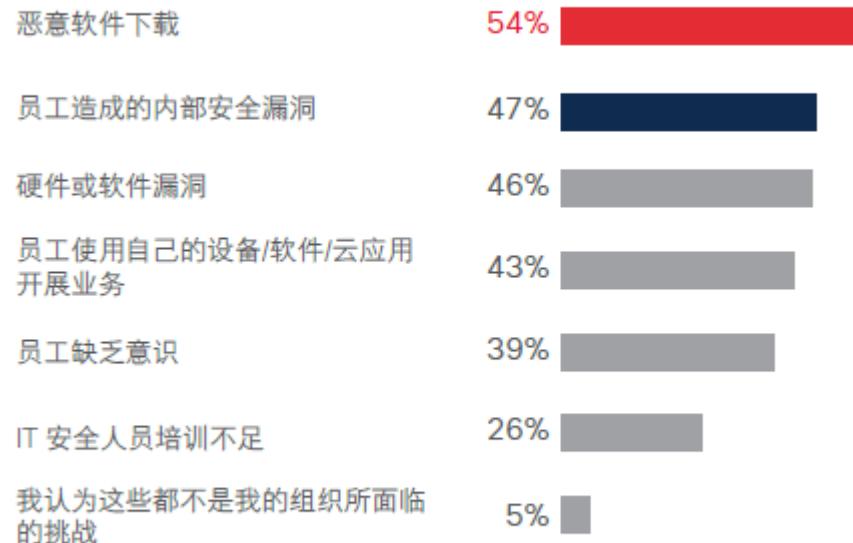


图 66. (全部受访者) 所面临的内部安全挑战



来源：思科安全风险和可信度研究

来源：思科安全风险和可信度研究

值得信任供应商，但是也需要经过验证

技术供应商需要展示他们的可信度：



从一开始就将安全纳入到其解决方案和价值链中

制定并落实降低风险的策略和流程

营造注重安全的文化

快速和透明地应对漏洞

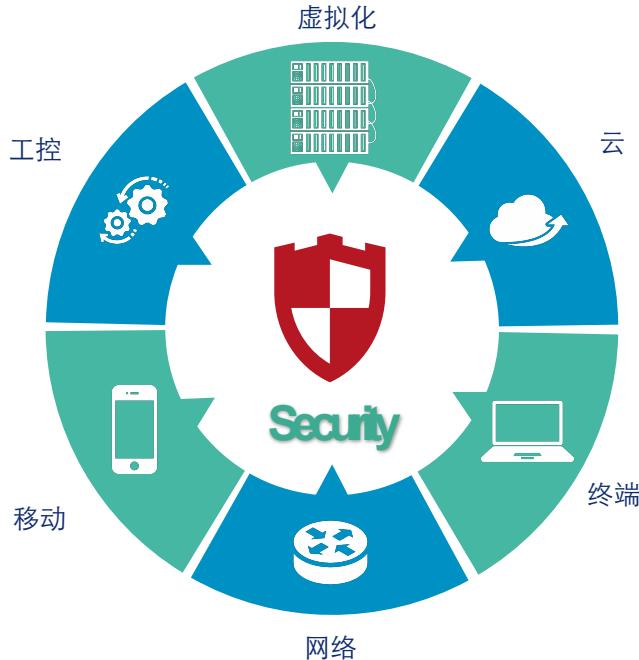
发生安全事件后提供快速补救和保持持续警惕性

思科2016年度安全报告贡献者



Lancope®

思科提高全面领先的网络安全解决方案

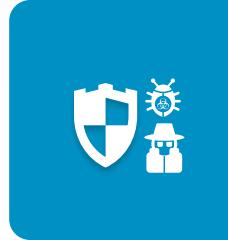


我们提供无处不在的安全防护
CISCO



全面可见

全面自动化
识别终端/应用/服务资
源等信息
了解全面
网络/终端信息



专注威胁防御

云安全智能Talos
在攻击前/中/后阶段进
行防御
自动防护/快速检测/
快速响应



整体防御

灵活开放平台，
可扩展，与网络基础架
构结合
全民皆兵，全面防护

NSSLAB评测最佳防御效率

99.4%

帮助用户将威胁的检测时间从100天减少到

17.5小时

全球市场份额
领先第二名一倍多
34%

2016 思科年度安全报告



攻击者的趋势：
利用合法的资源，
善于部署
难以探测
高盈利



防御者的趋势：
防御信心在下降
安全担忧驱动更多的行动
和战略



我们需要协作，来抵御
当今高级的持续的攻击，
为未来提供更好的架构

2016 Annual Security Report

www.cisco.com/go/asr2016

