2018,谁将威胁你的网络

解读思科最新年度安全报告

Cisco 徐洪涛
hongtxu@cisco.com

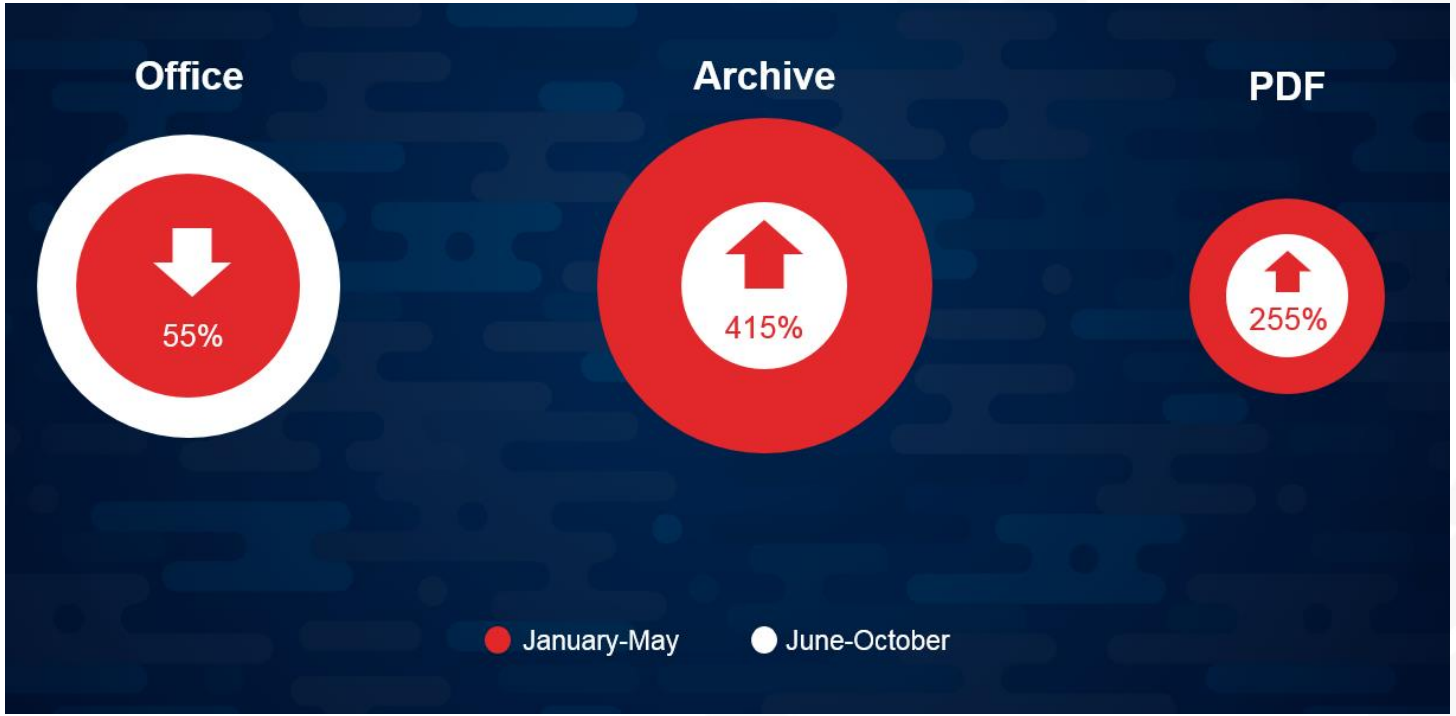
DANCE TOGETHER 舞动未来

2018思科大中华区生态系统与合作联盟高峰会
Cisco Greater China Ecosystem and Alliance Forum 2018

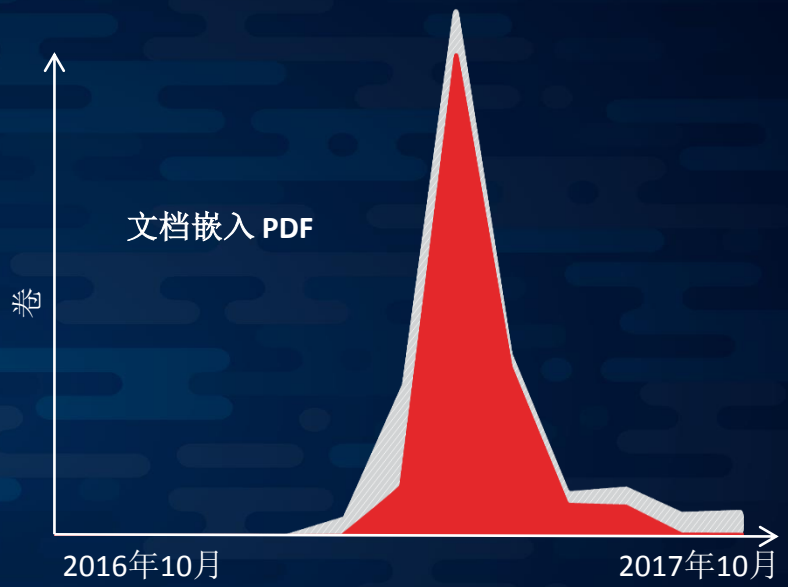
议程

- 2017-2018最新网络威胁趋势
- 我们用户的防御现状与需求
- 我们的机会在哪里?

电子邮件中的恶意软件



攻击者不断的调整对沙盒的逃避

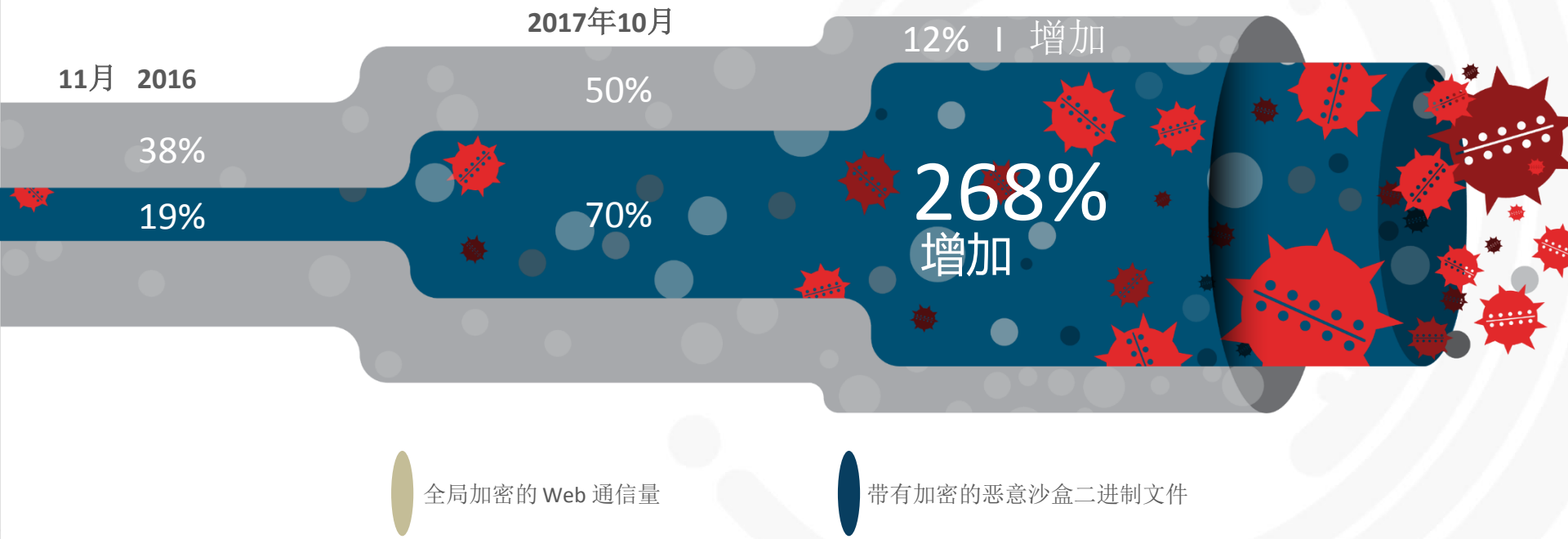


恶意示例

样本总数

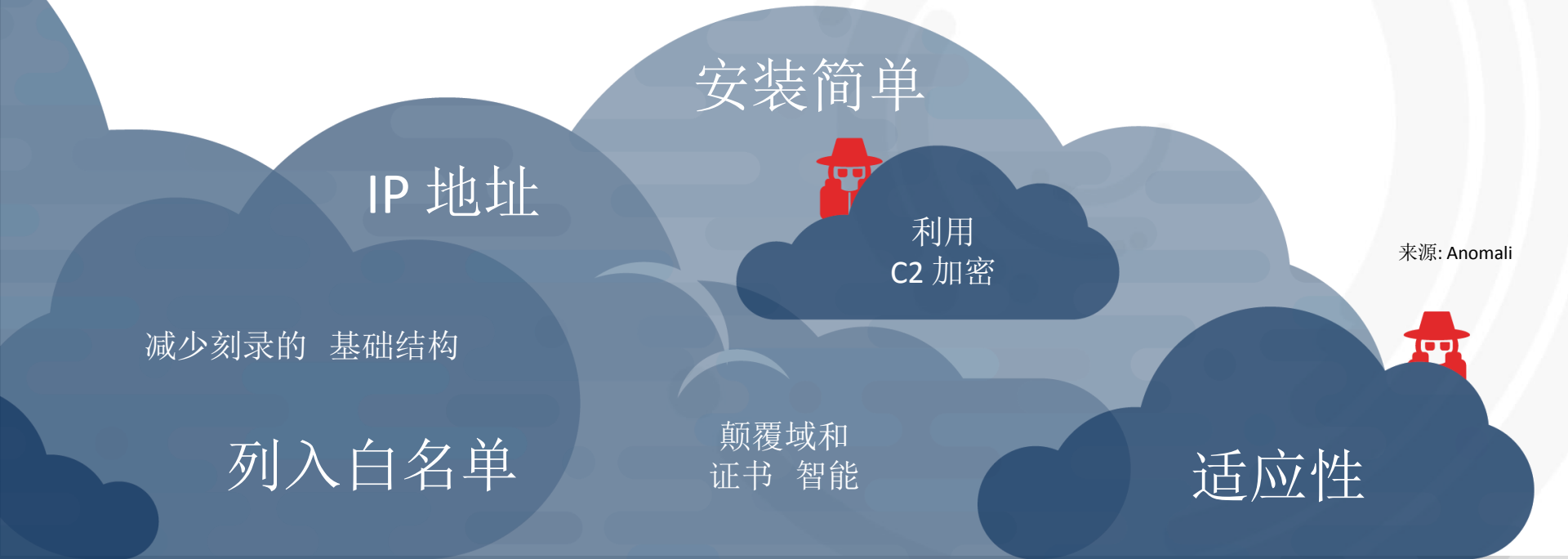
恶意软件传递利用加密隐藏

攻击者接受加密以隐藏其命令和控制活动



使用合法资源实现恶意控制

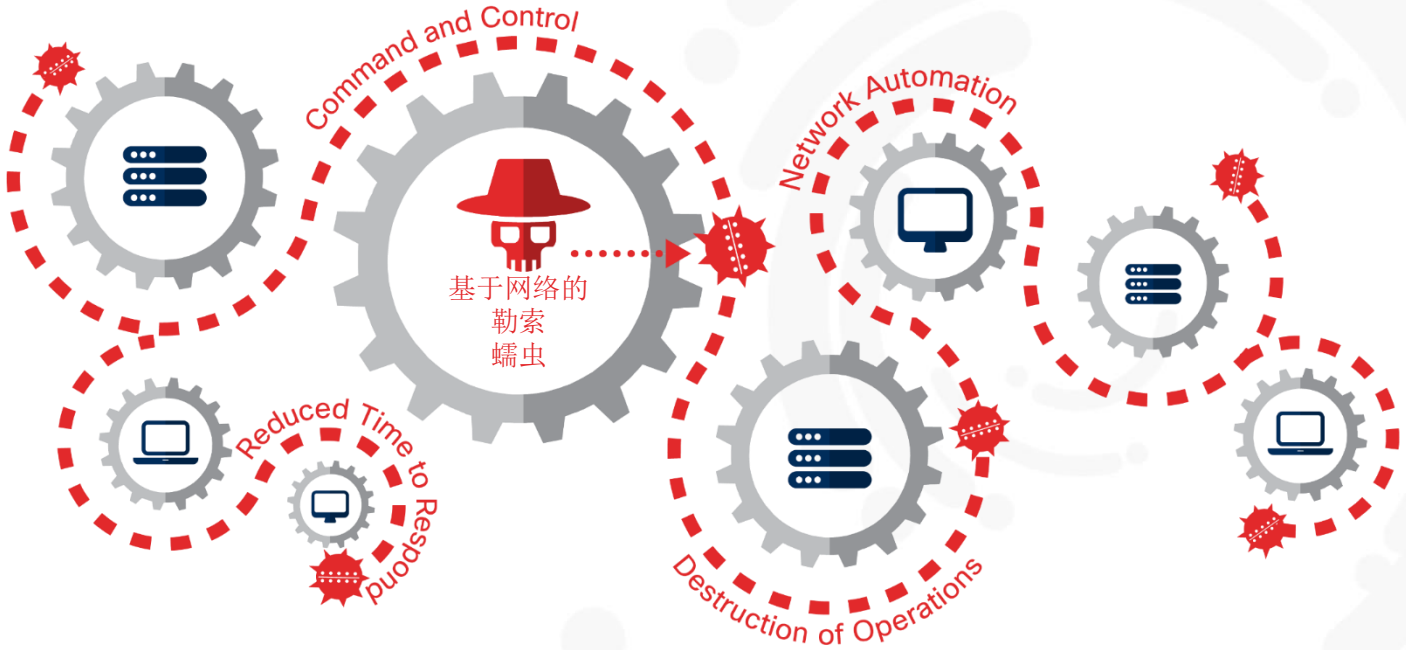
犯罪分子正在采用依赖合法 Internet 服务的命令和控制通道，使得 恶意软件通信几乎无法关闭



来源: Anomali

基于网络的勒索的爆发

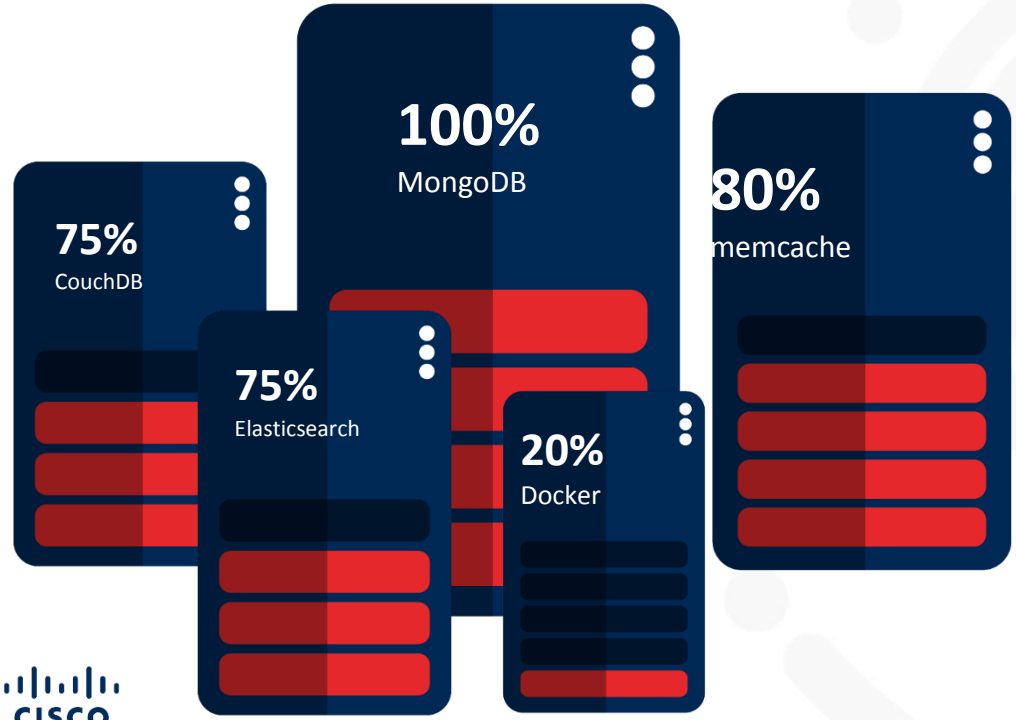
WannaCry 和 Nyetya: 快速移动、自传播的基于网络的勒索攻击



仍然存在未修补机器，当蠕虫将再次攻击，您的网络还安全吗？

暴露的开发系统

大量DevOps 服务器的开放，造成巨大的勒索风险



为了减少暴露于 DevOps 勒索攻击的风险:

- 制定安全部署标准
- 保持对公司公开基础设施的积极检查
- 保持 DevOps 技术的最新和修补
- 进行漏洞扫描

来源: Rapid7

针对IT/OT的攻击

69% 的组织认为 OT 是 2018 年可行的攻击媒介之一

- 20% 的组织认为 OT 将成为最终的攻击媒介
- 10% 的组织认为 IT 仍是唯一攻击媒介

内部威胁日益严重

机器学习算法可以极大地帮助检测内部恶意行为者

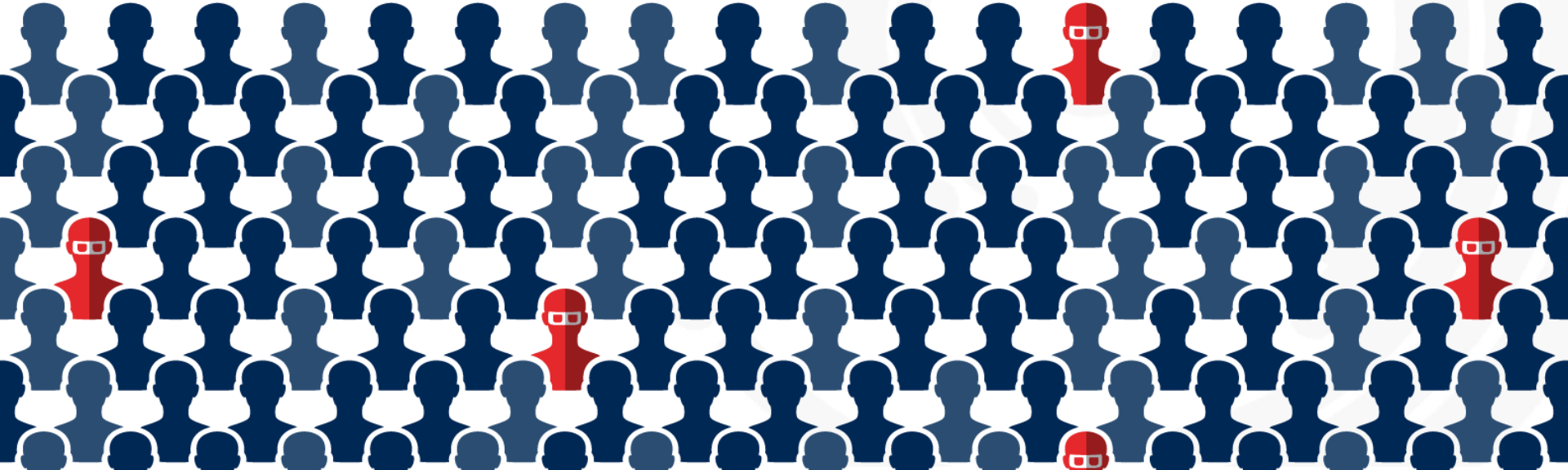
5200
每个用户的文档

数据"
是文档标题中最受欢迎的关键词

pdf
是最常见的文件类型

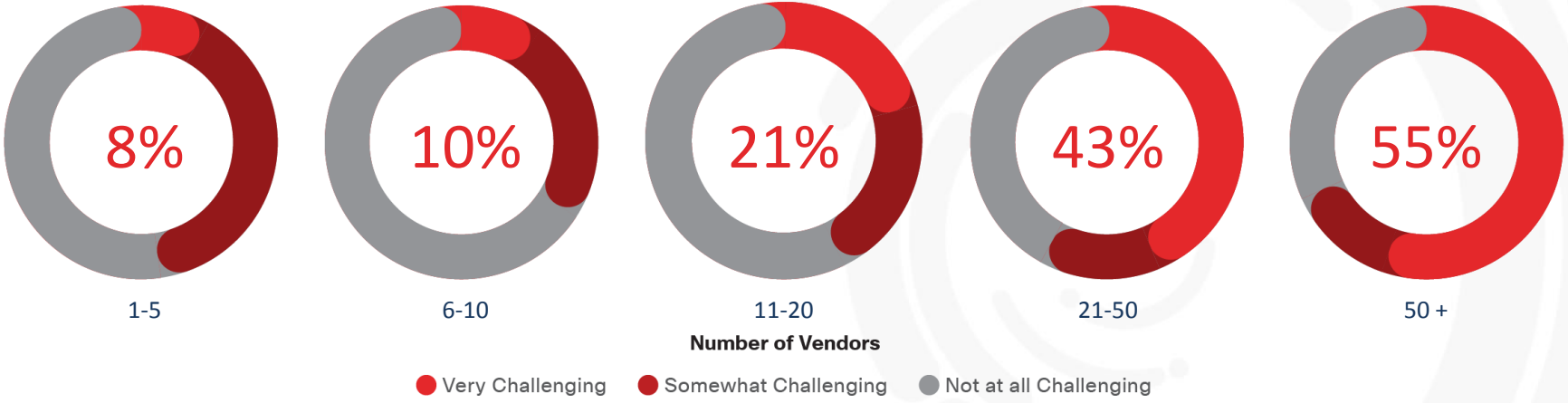
62%
在正常工作时间之外发生

高*
自2017年6月以来恶意活动检测的准确性



我们的安全技术是否有效？

随着供应商数量的增加，业务流程面临的挑战越来越多



	教育	金融服务	政府	医疗	制造	制药	零售	电信	运输	效用/能源
非常有挑战性	17%	24%	16%	42%	14%	25%	19%	14%	12%	27%

防御者的挑战和障碍

关键限制

34%
预算
(5%)

27%
缺乏训练有素的人员
(5%)

27%
认证要求
(4%)

27%
兼容性
问题
(5%)

需要的关键功能

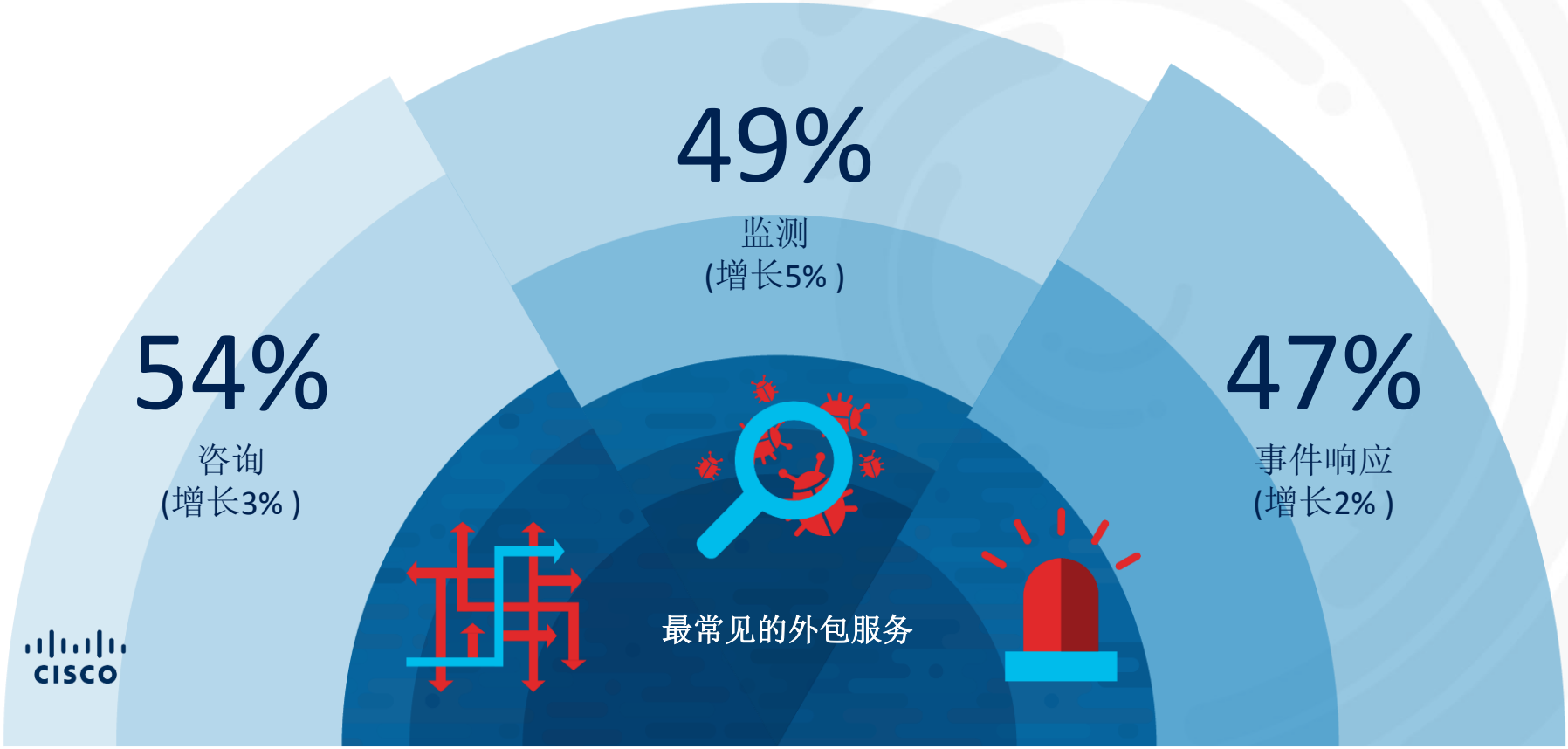
移动设备
57%
寻找非常和极具挑战性的防守

公共　云中的数据
56%
寻找非常和极具挑战性的防守

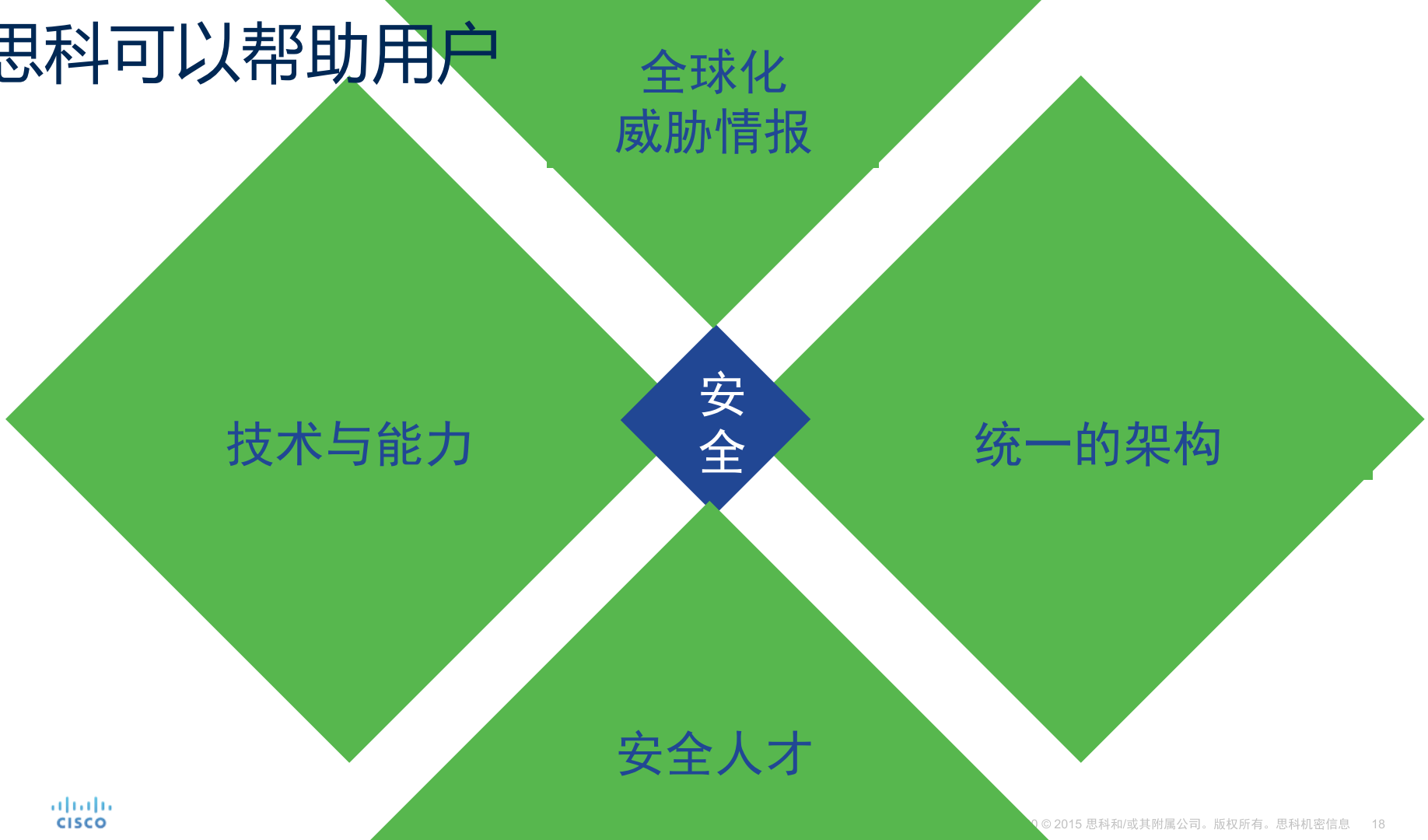
用户行为
(例如, 单击电子邮件或网站中的恶意链接)
56%
寻找非常和极具挑战性的防守

数据中心/服务器
56%
寻找非常和极具挑战性的防守

外包的需要



思科可以帮助用户



同步全球威胁情报，知彼,洞悉万千威胁

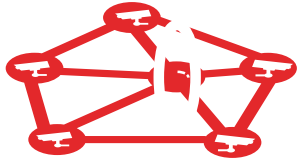
Cisco TALOS
威胁情报

国际刑警组织

中央网络安全和信息化领导小组办公室
国家互联网信息办公室

IBM

全面网络可见+全球威胁情报，
帮助我们准确检测和阻挡最新
威胁



DDoS

邮件攻击

勒索软件

专业安全人才实战培养，着力有效安全运维

“What I **hear**, I **forget**

What I **see**, I **remember**

“百闻不如一见”

What I **do**, I **understand**”

“实践出真知”

内容：

- 模拟全球发生的最新威胁
- 学习如何利用技术有效防御
- 快速发现问题，作出响应
- 红方/蓝方网络对抗


THANKS !
https://www.cisco.com/cn/securityreport
DANCE TOGETHER
舞动未来
2018思科大中华区生态系统与合作联盟高峰会
Cisco Greater China Ecosystem and Alliance Forum 2018