如何应对邮件的新型威胁与挑战

思科邮件安全高级防护技术介绍

吴清伟

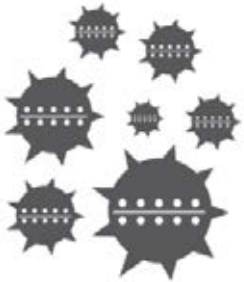
思科大中华区安全顾问

邮件依然是使用最多的攻击手段

思科Talos报告-邮件是最常用的攻击手段

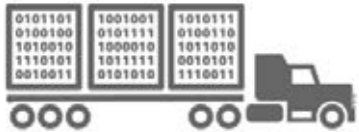
目标侦察

分析，筛选和确定目标



武器化构建

构建特定目标的攻击邮件



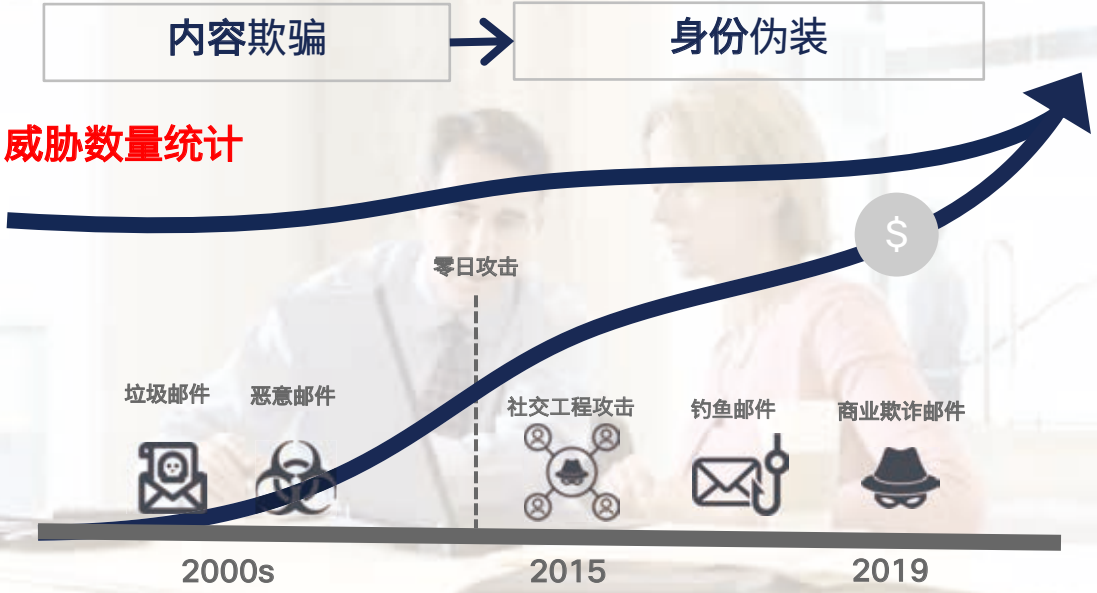
发起传播

发送**钓鱼邮件**，**欺骗邮件**或**勒索邮件**

安装和感染

用户下载恶意代码，驻留或传播

邮件威胁的演变-鱼叉式攻击行为在增加



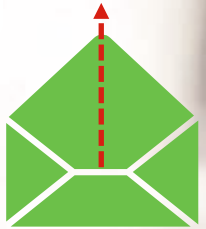
30% 打开了恶意邮件
13% 点击了恶意附件
3:45 发现被攻击所花费的时间

Sources: CSOonline.com, Cybersecurity ventures, Nucleus Research, FBI I3C (Jan '15 – Dec '16)

钓鱼邮件:使企业面临新的风险

- 钓鱼邮件
- 商业欺骗邮件
- 勒索邮件

94%
的钓鱼邮件带有恶意代码附件



30%
的钓鱼邮件被用户点击打开

$91亿美元
2017年
钓鱼邮件2017年造成的经济损失

[1]2016 Cisco Annual Security Report
[2]RSA 2017 Global Fraud & Cybercrime Forecast

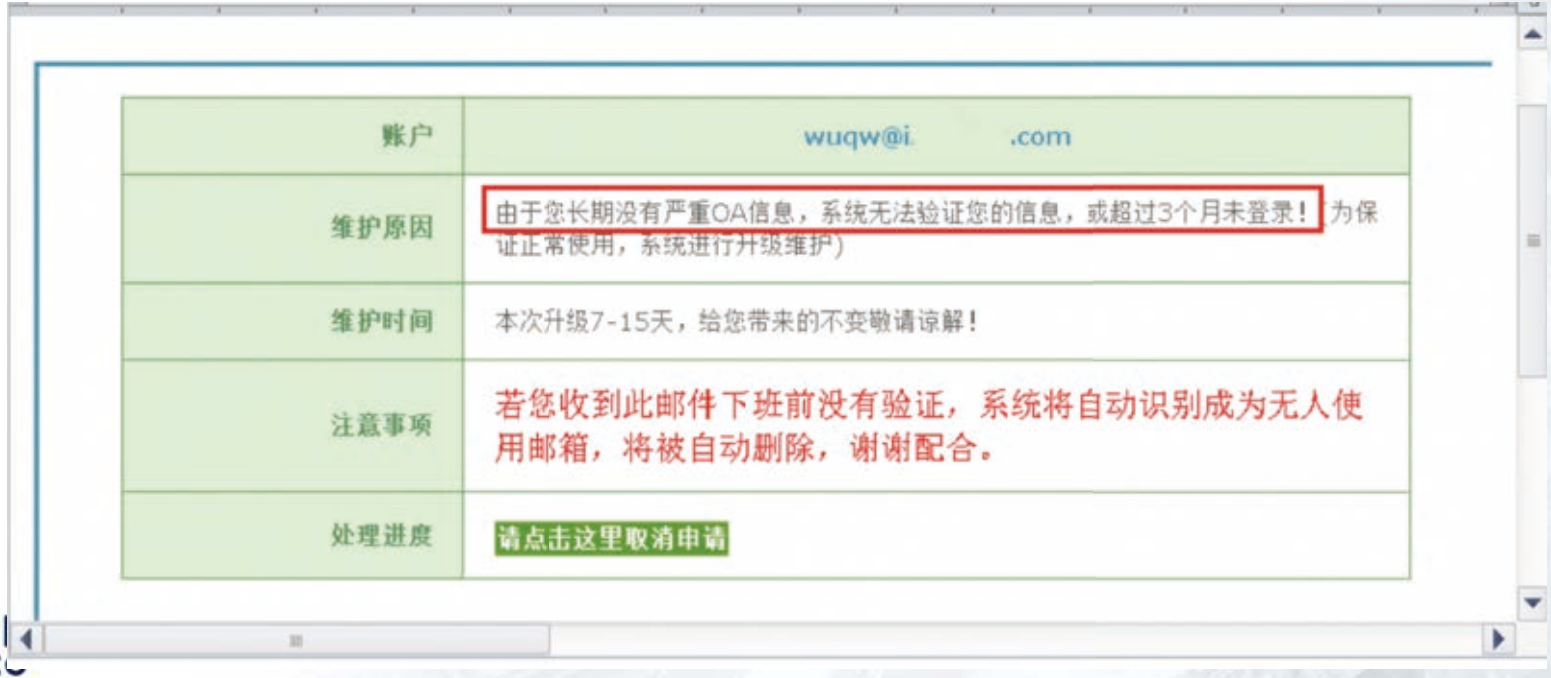
邮件包含
恶意附件或钓鱼URL链接

利用社交信息
构造定向攻击的邮件

轻信诱饵邮件
泄漏个人身份信息

钓鱼邮件示例：骗取个人身份和密码

- 黑客冒充企业IT部分，构建一封要求企业员工更新帐号信息的邮件，目的是骗取用户登录帐号和密码。



账户	wuqw@i .com
维护原因	由于您长期没有严重OA信息，系统无法验证您的信息，或超过3个月未登录！为保证正常使用，系统进行升级维护）
维护时间	本次升级7-15天，给您带来的不变敬请谅解！
注意事项	若您收到此邮件下班前没有验证，系统将自动识别成为无人使用邮箱，将被自动删除，谢谢配合。
处理进度	请点击这里取消申请

商业欺骗邮件：数量在逐年上升

- 钓鱼邮件
- **商业欺骗邮件**
- 勒索邮件

$53亿
在2013 – 2017期间造成的经济损失

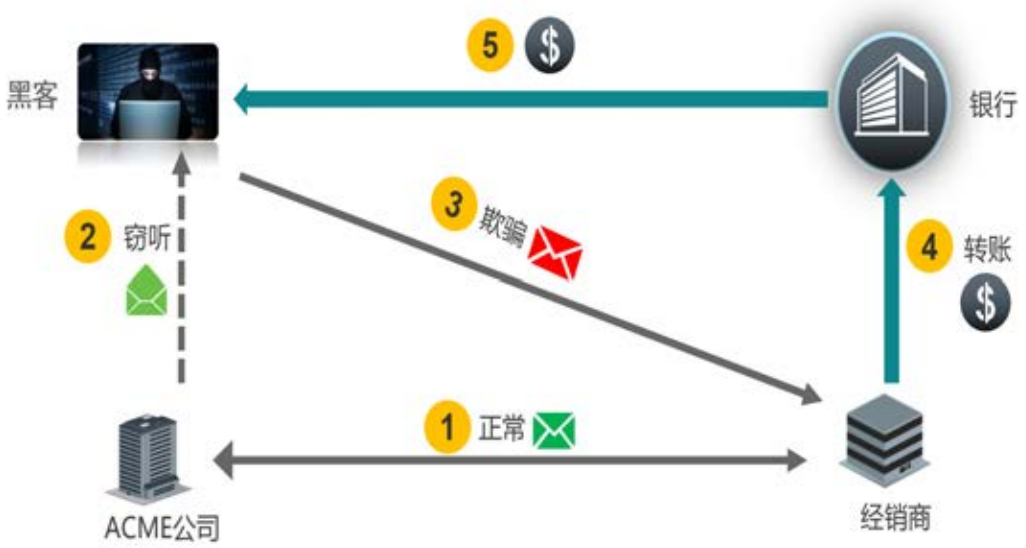
伪造发件人地址
欺骗收件人

攻击者对收件人目标
进行深入的研究

最终目的是
获取金钱或敏感信息

商业欺骗邮件示例：骗取经销商的货款

- 黑客采用虚假域名，伪造了一封要求支付货款的邮件，发给了经销商，导致经销商将数百万货款转入黑客的银行账号。

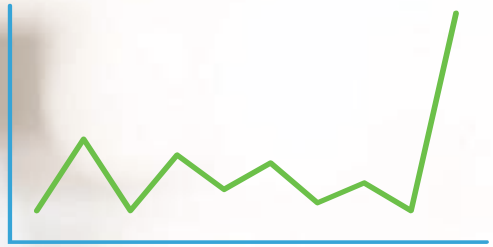


勒索软件邮件：劫持企业勒索金钱

钓鱼邮件

商业欺骗邮件

勒索邮件



勒索软件已经在邮件类型的网络犯罪方式中占有最大的比重

90% 邮件中检测到勒索软件的比例增加了90%

$6千万

单次勒索软件爆发给用户和企业带来的经济损失

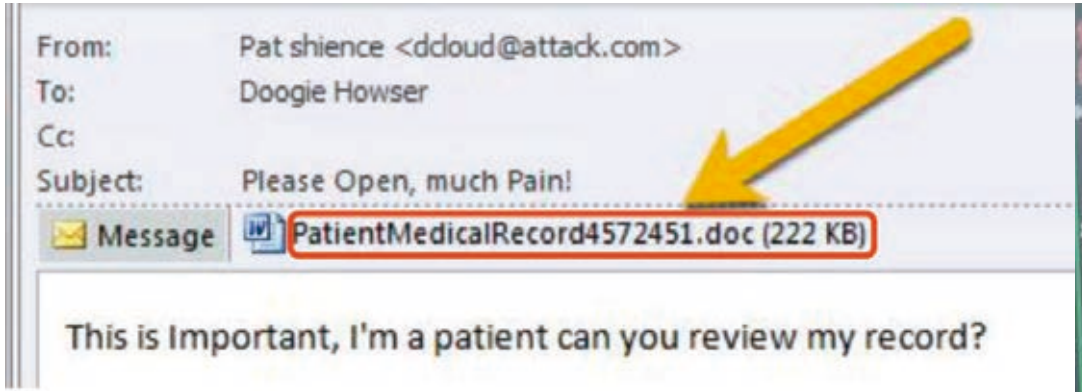
勒索软件加密企业关键文件

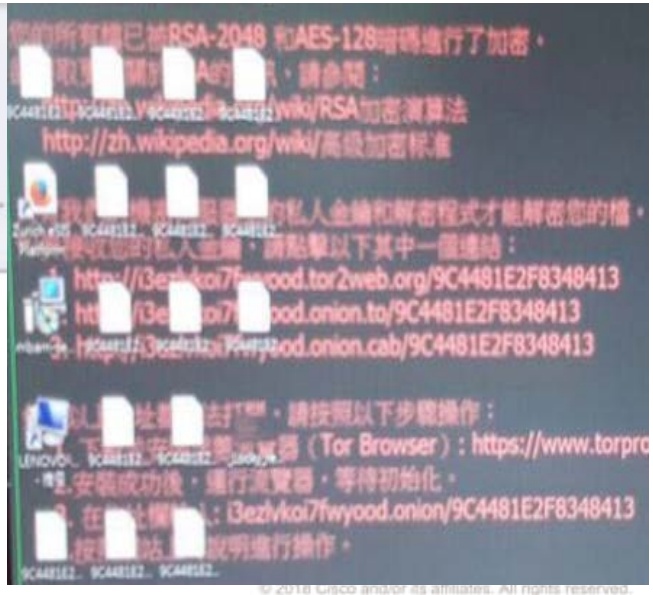
用户系统被锁定无法访问

向企业发出支付金钱的勒索要求

勒索邮件示例：医院电脑的文件被加密

- 黑客在邮件中包含了带有TeslaCrypt勒索代码的附件，冒充病人以定向攻击的方式发送给医生，附件被打开后导致电脑的关键文件被加密。





邮件安全防护需要紧跟威胁演变趋势

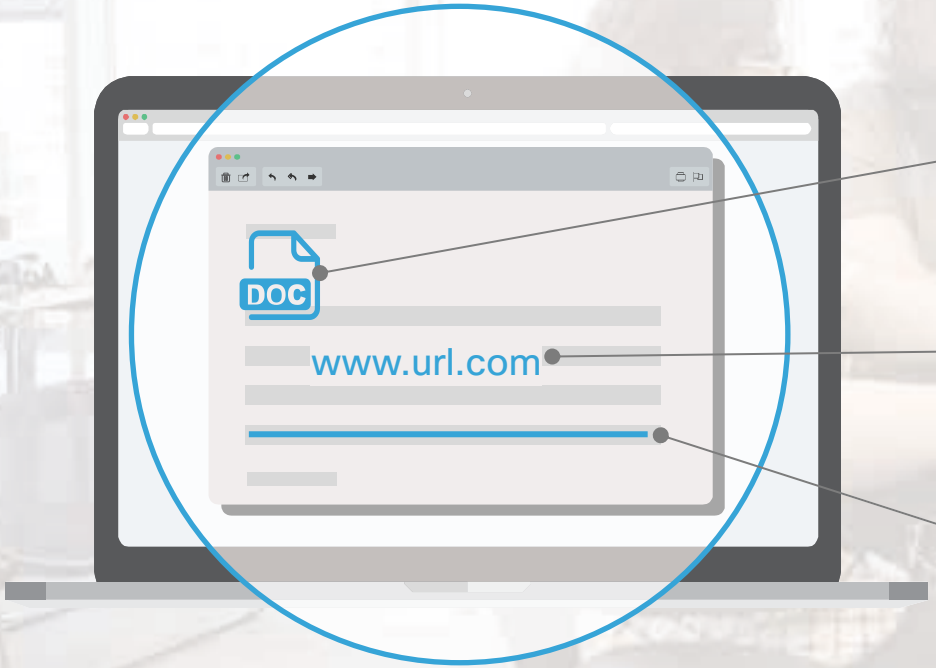
- 单纯依靠签名检测的方式只对静态的威胁有效
- 单纯依赖信誉过滤技术无法应对分散的攻击方式
- 不断变化的Web攻击掩盖了难以发现的潜在的风险
- 恶意文件的攻击不断产生新的变种
- 邮件的可视性在攻击链中无法得到呈现

思科将各种防护技术有机整合带来全面防护

思科TALOS：业界领先的威胁情报分析

思科邮件安全实现全面的威胁防御

如何减少企业暴露的邮件攻击面



邮件附件

URL链接

邮件内容

邮件附件

威胁类型

勒索软件

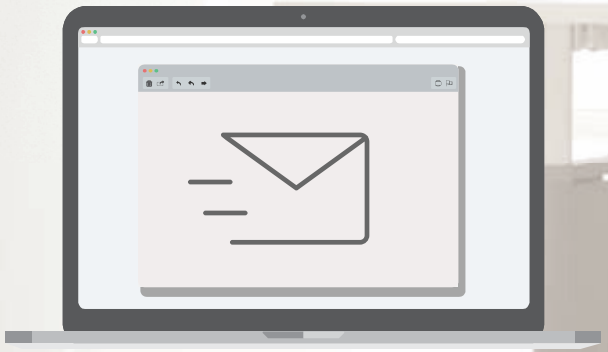
钓鱼邮件

典型场景：拦截貌似正常的恶意附件

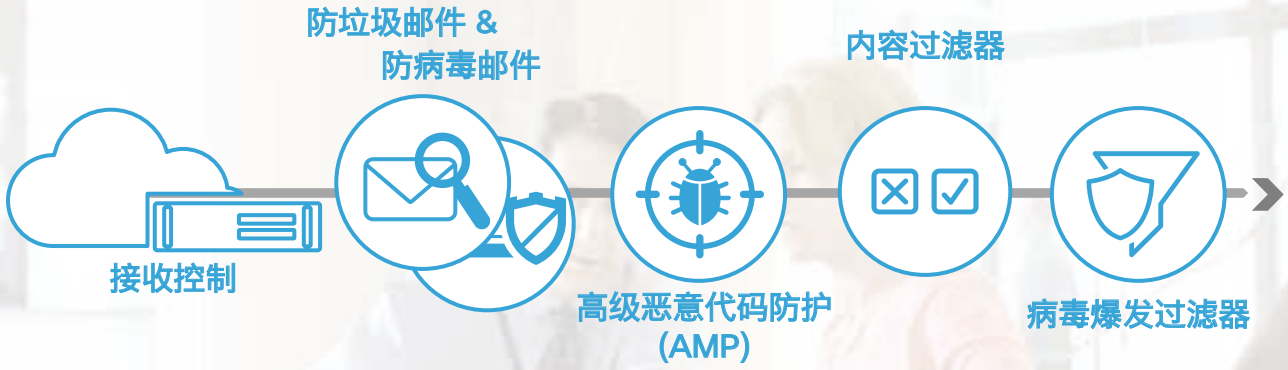
HR部门的Dave收到一封带有简历附件的邮件

Dave打开了看起来貌似正常的邮件附件

附件中内嵌了自动下载链接，在Dave不知情的情况下，将恶意代码下载到Dave的电脑上



多种技术拦截隐藏在附件中的恶意代码



信誉过滤和自适应分析拦截垃圾邮件

接收控制+防垃圾邮件（上下文自适应扫描引擎）

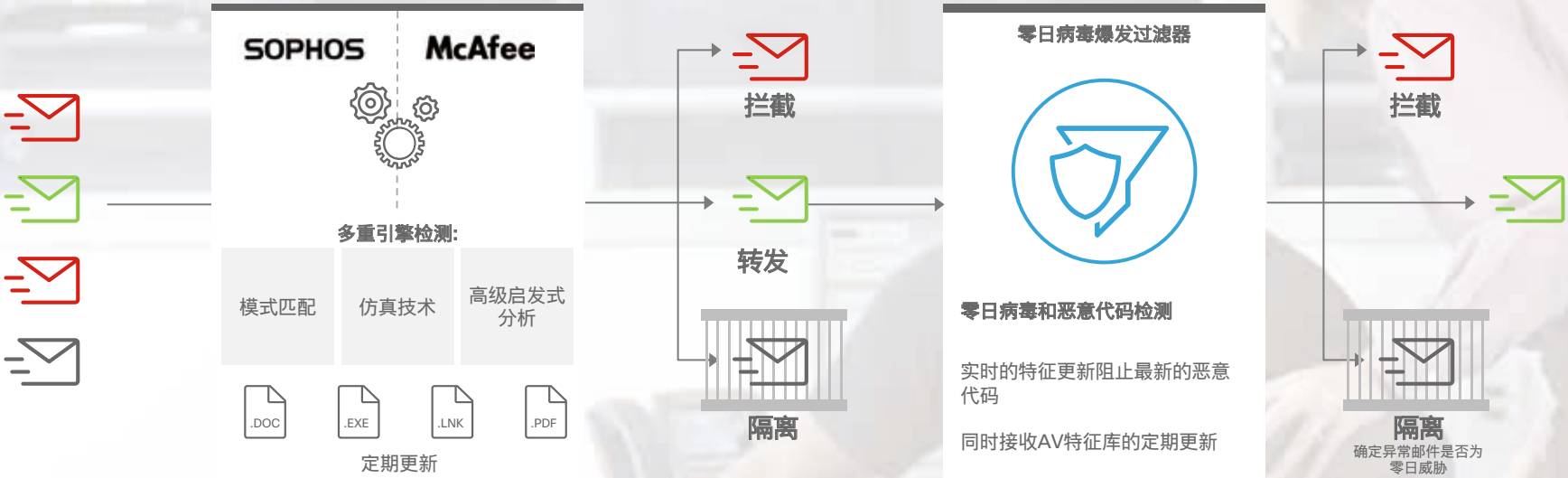
评估发件人信誉度，对发件方进行邮件的接收控制

垃圾邮件拦截精确度99%， 误判率低于百万分之一。

隔离可疑邮件用于后续分析

已知病毒和零日病毒邮件的拦截

防病毒邮件处理



扫描附件
拦截已知病毒

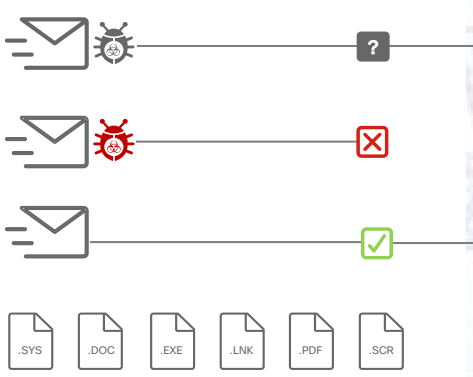
对非病毒邮件转发
进行进一步检测

防御零日类型的恶意代码

检测和拦截高级恶意威胁

双向的高级恶意代码防护 (AMP)

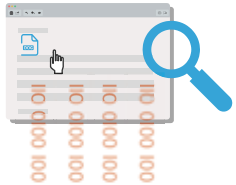
文件信誉度



已知威胁的签名 | 模糊指纹分析 | IOC威胁指数

文件沙箱

- 高级分析技术
- 动态分析技术
- 846以上的分析指数



未知 | 正常 | 恶意

文件回溯

拦截已知恶意代码

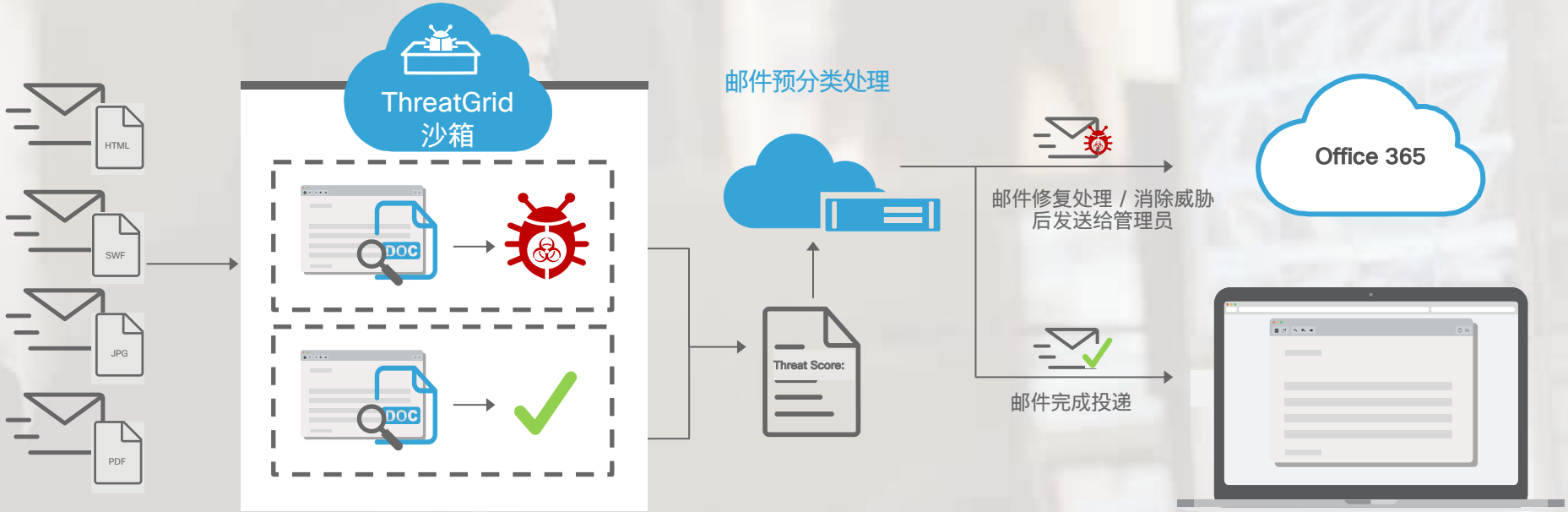
确保安全地分析可疑文件

O365邮箱自动修复威胁

进出网络的邮件的完整可视性

利用沙箱对未知附件的深度检测

ThreatGrid沙箱分析技术



ThreatGrid提供连续的可疑文件分析

采用上下文驱动的文件分析方式

接收威胁报告和评分并且做出判定决定

O365用户支持自动修复恶意代码

URL链接

威胁类型

勒索软件

钓鱼邮件

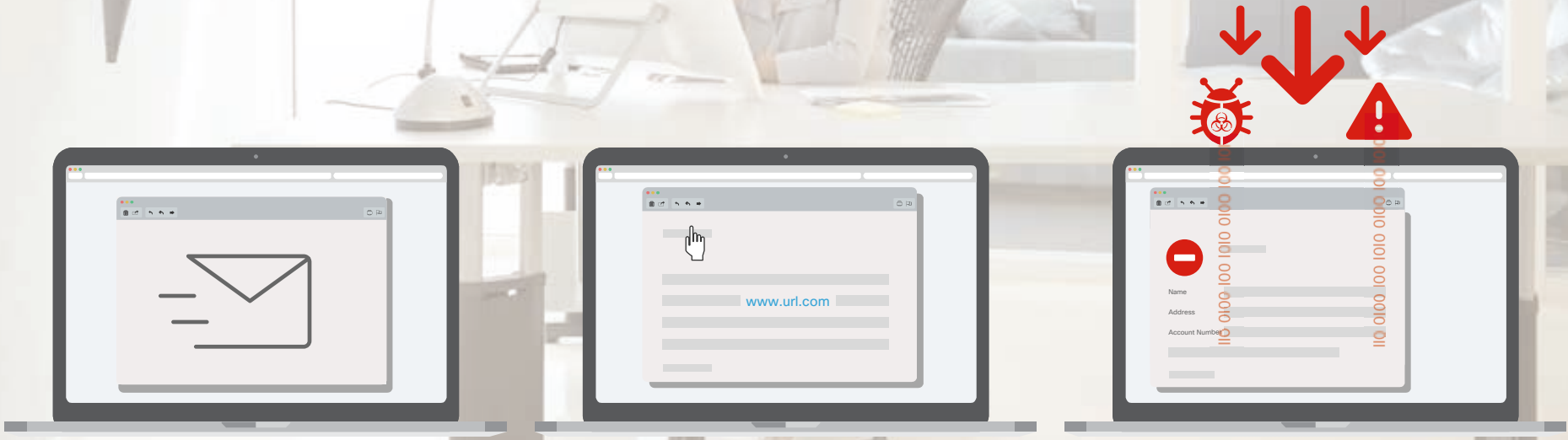
欺骗邮件

典型场景：防止钓鱼邮件中的URL的风险

员工Sarah收到一封银行的邮件，说她有诈骗行为

由于紧张，Sarah点击了URL链接并进行登陆

由于URL链接是假冒的，Sarah的个人帐号和密码给假冒网站给窃取了。



ESA如何识别伪装的URL链接？

对邮件内容进行检测

方式: 内容过滤器

定制内容过滤器
提供额外安全防护

记录完整的用户交互记录

易于部署企业合规性策略

检测定向混合类型的邮件攻击

方法: 爆发过滤器

借助Talos拦截已知类型攻击

隔离带有可以URL链接的邮件

修改邮件内容
阻止对用户的危害

重定向流量阻止恶意链接

邮件内容

威胁类型

欺骗邮件

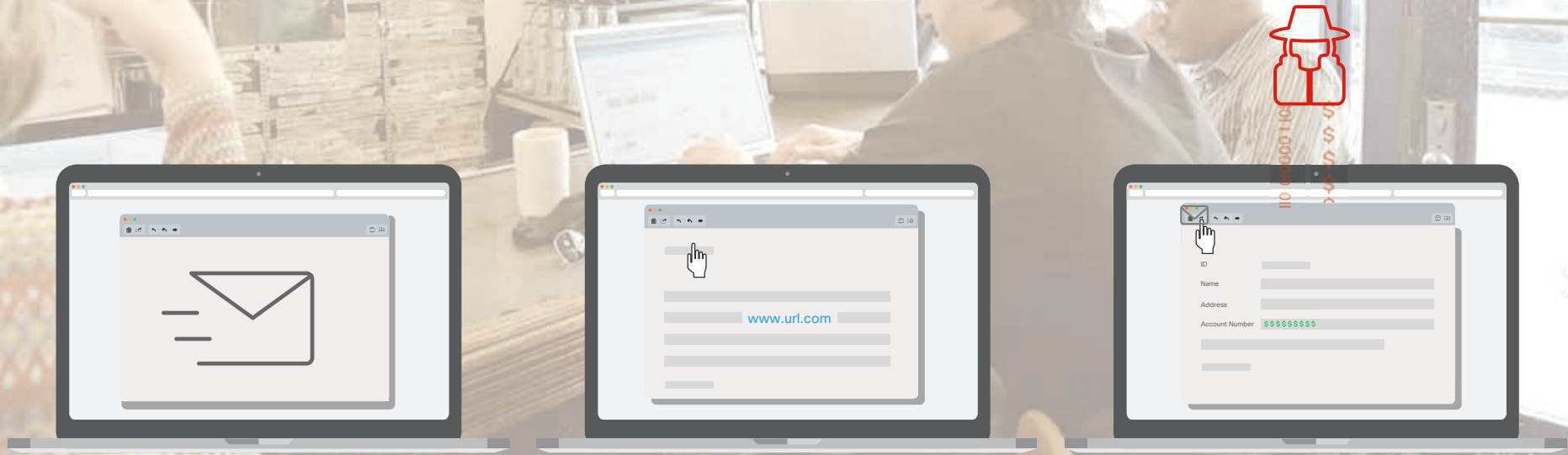
钓鱼邮件

典型场景：防止鱼叉类型的邮件攻击

财务部员工Kevin，收到老板的邮件要求他立刻转账一笔资金

为了避免业务受到影响，Kevin立即进行资金的转账

事后发现，Kevin把钱转给了邮件欺骗者的银行帐号上

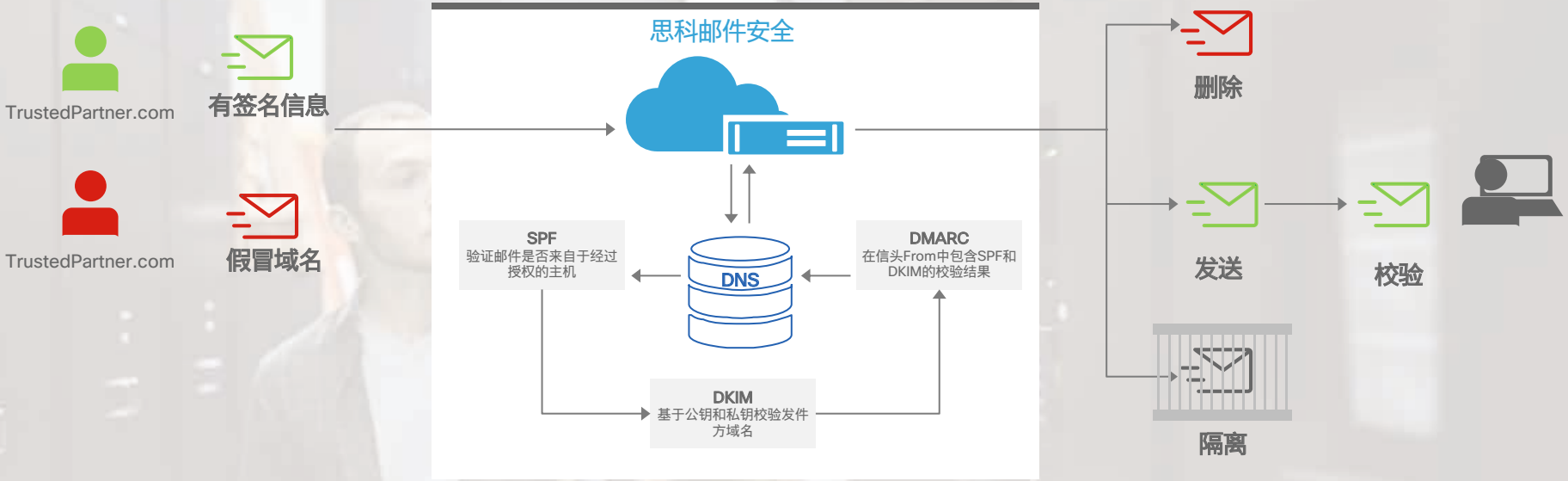


ESA如何避免鱼叉邮件攻击的风险

邮件中没有恶意链接或者恶意附件.
靠什么去判断这封邮件?

基于发件方域名拦截欺骗邮件

启用DMARC, DKIM和SPF检查



检测发件方域名的信誉

验证发件人的详细信息

拦截来自虚假域名的邮件

伪造邮件发件人的检测

Business Email Compromise: 商业欺骗邮件

邮件预处理

From: Chuck <chuck.robbins@mail.com>

Subject: [紧急] 需要帮忙转账资金

检测SMTP的信封地址:

```
$ telnet mail-smtp-in.l.mail.com 25
Trying 74.125.206.26...
Connected to mail-smtp-in.l.mail.com
Escape character is '^]'.
220 mx.mail.com ESMTP i11si22058766wmh.67 - gsmtp
HELO mail.outside.com
250 mx.mail.com at your service
MAIL FROM:<adam@outside.com>
250 2.1.0 OK i11si22058766wmh.67 - gsmtp
RCPT TO:<alan@mail.com>
250 2.1.5 OK i11si22058766wmh.67 - gsmtp
Data
```

Recipient Domain

Sending Domain

Actual Sender

SMTP Envelope

From: adam@outside.com

Subject: {可能伪造} [紧急] 需要帮忙转账资金

邮件后期处理

SMTP信封发件人的真实性	将发件人地址和公司通讯录进行对比	在主题上添加提醒信息，警告收件人存在风险	记录此类行为和采取的动作

如何拦截伪造域名的邮件

Advanced Phishing Protection：高级钓鱼邮件的防护

APP高级钓鱼保护

本地威胁分析

- 对行为进行分析，对身份进行认证，提供增强型保护。

减少商业欺骗邮件

- 识别定向钓鱼邮件的攻击，仅仅放行合法邮件。

如何拦截伪造域名的邮件

Advanced Phishing Protection: 高级钓鱼邮件的防护

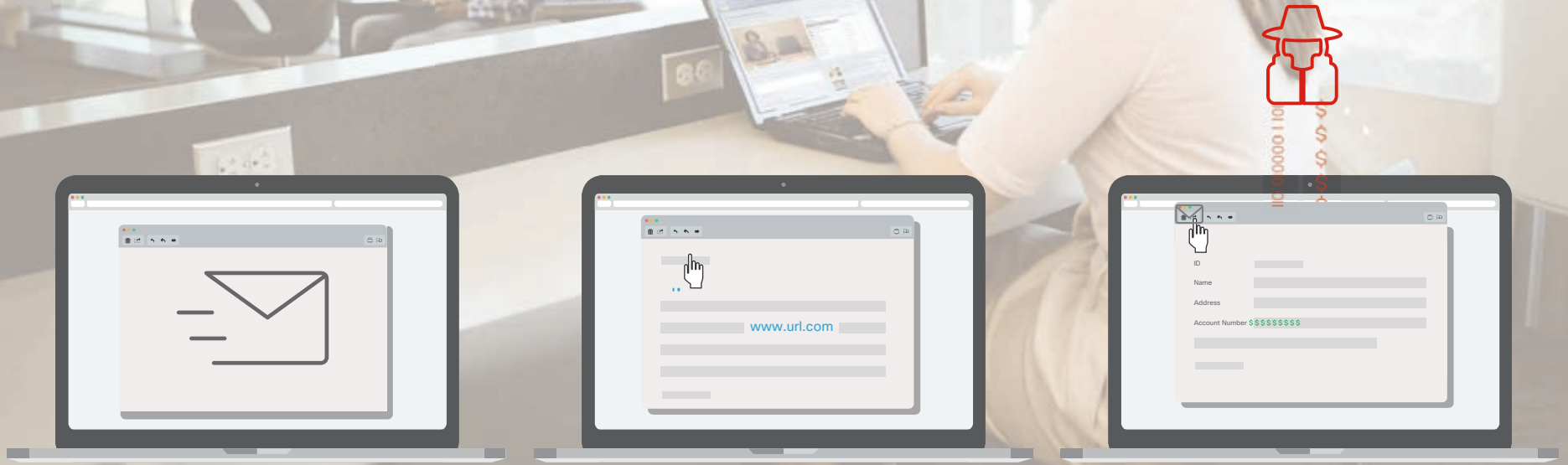
- 分析并管理不可信的，可疑的邮件，为该邮件分配信任评分
- 根据信任评分执行邮件处理的策略
- 移除已经确定的伪造邮件

典型场景：防止敏感信息通过邮件泄漏

Tina收到了一封某公司HR部门发来的邮件，请求提供某员工的背景调查信息

一切内容看上去都是合法正常的，于是Tina就把员工信息发给了对方

事实上Tina没有识别对方身份真伪的情况下，将员工个人信息发给了攻击者



出站邮件的数据泄露和域名信誉的保护

防止企业敏感信息泄漏

DLP: 数据泄露预防

制定出站邮件的控制策略

扫描邮件中的敏感信息

阻止数据泄漏行为

邮件加密后发送提升通信机密性

思科CRES：邮件加密服务

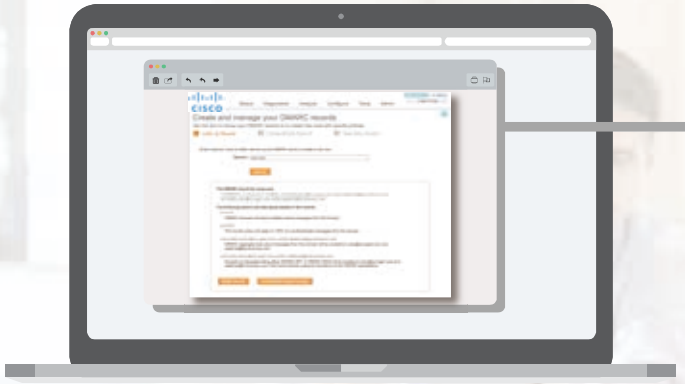
扫描邮件中的关键字，执行加密策略

通过认证才可以访问加密密钥

对已经发送的邮件保留控制

如何保护企业域名的信誉

Cisco Domain Protection：保护企业域名信誉



Cisco Domain Protection

阻止企业域名被用来发送钓鱼邮件

保护企业域名和信誉

- 通过分析和更新状态，监控企业域名被用来发送恶意邮件的状态
- 检验并记录有哪些攻击者在冒充使用企业域名发送邮件

Automate DMARC authentication

- 满足各种法规对邮件安全的要求
- 通过有效的工具或服务推动 DMARC 的部署和应用

如何保护企业域名的信誉评分

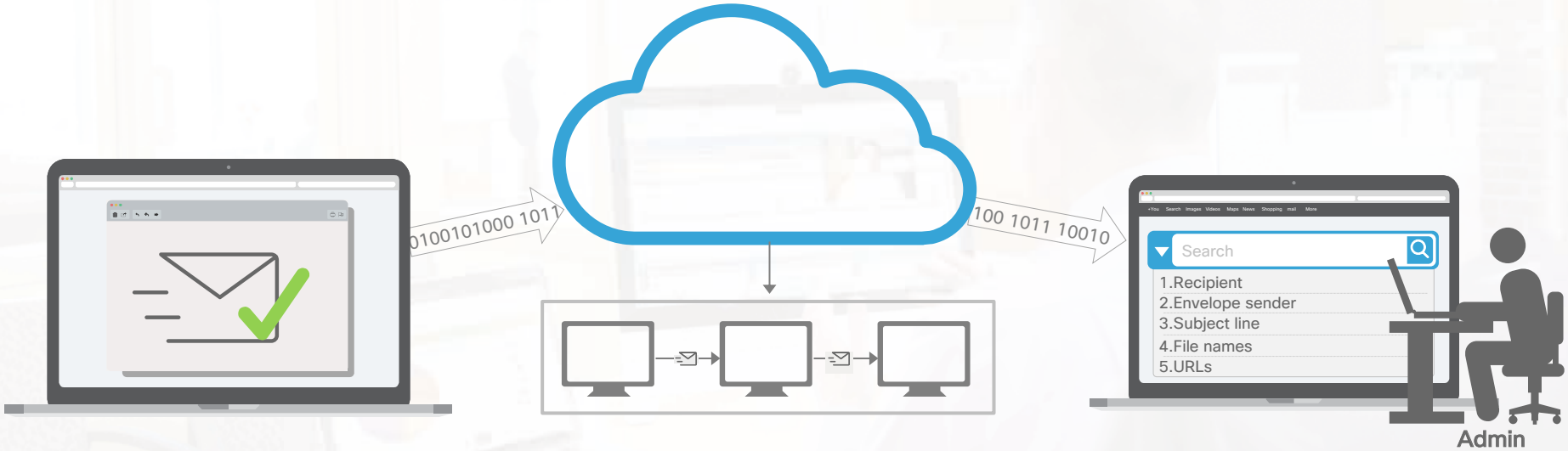
Cisco Domain Protection: 思科域名保护

- 管理, 创建和更新DMARC, SPF, DKIM等记录
- 识别各种冒充域名邮件的源头
- 企业域名被冒用状态的可视化监控

邮件的运维与管理

便捷了解用户邮件的处理状态

邮件处理过程的全程跟踪



实时的邮件状态跟踪

基于特定条件跟踪邮件处理记录

检索同类威胁的受影响用户

全面监控邮件处理的系统状态

统一全面的的系统运行报表

查看详细信息:

- Email Threats
- Malicious Attachments
- Email Volume
- Spam Counters
- Policy Violations
- Virus Reports
- Outgoing Email Data
- Reputation Service
- System Health View

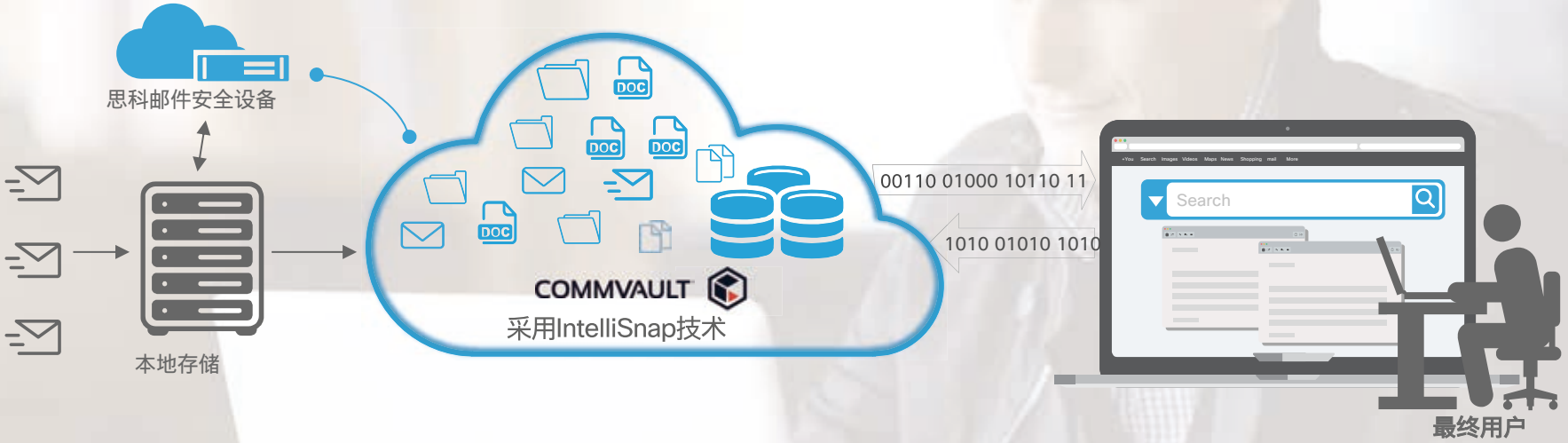
多种方式访问管理平台，并提供统一报表

减少威胁发现与响应时间

定期生成报表，提供系统运行状态

简化归档邮件的备份与恢复

支持与Commvault产品的集成



自动化数据管理优化存储

保存关键邮件和附件

与O365集成方便获取归档邮件

思科高级邮件安全技术应对新型威胁与挑战

减少敏感信息的暴露，
降低攻击面

支持各种应用场景
的可视化与监控

先进的防护技术
和精细化策略

高级邮件安全技术

可视性与可靠性

简化运营与管理


CISCO