ivanti

在局面失控前采取行动

当今极端威胁下的网络安全

序言

序言

仅仅是在美国，2016年一年就发生了超过500起公开披露的数据泄露事件，与前一年相比几乎翻了一倍。[1] 2017年2月，研究公司Opinium在一项面向美国和欧洲的IT决策者的调查中发现，有78%的受访者在前一年至少遭遇过一次针对其企业的勒索软件攻击。黑客组织“影子经纪人”（The Shadow Brokers）公布的漏洞曾造成如今恶名远扬的WannaCry攻击，而该组织宣称还会公布更多漏洞。我们也看到了第一笔公开披露的百万美元勒索赎金支付。[2]

NotPetya则让我们初尝了未来式的武器化恶意软件的滋味。然后，又发生了Equifax被黑事件……

如何才能阻止这列数据安全的列车出轨？如果缺乏集中性的安全策略，设备数量的增长将意味着高昂的支出和失去控制。IT团队耗费了大量时间来管理这些设备，加上网络安全人才严重不足，企业已不得不优化安全人员设置。显而易见，一款全面、简化管理、专注于安全基础、能以最强的防护抵御现实攻击的解决方案，与其他方案相比的优势是巨大的。

93%的数据泄露能在几分钟或更短的时间内对企业造成损失[3]——当涉及企业安全时，您没有试错的机会。

您面临的安全风险是空前的

所有类型的高级网络安全威胁都在愈演愈烈[4]，不过这毫不令人意外，不是吗？可是到底为什么会这样呢？

我们并不会在本文中过多探讨这个问题。

我们只需要知道，安全威胁越来越多在很大程度上是因为网络攻击越来越容易了。例如，现在的漏洞工具包让网络攻击变得简单，连新手黑客也能驾轻就熟。这些恶意工具包内含预写的漏洞代码，无需理解原理也能使用。它们通常只是一个简单的网络界面，授权用户可以登录并查看活跃受害者和统计数据，甚至还可能提供支持周期和更新，几乎可比肩合法的商业软件。

还有一个原因是，原本用于网络间谍和网络战争的复杂工具如今已唾手可得。例如，勒索软件最初只是一个简单的吓人攻击，但基于被盗的美国国家安全局（NSA）工具构建的勒索软件已成为企业级的恶意软件，可以挟持计算机并锁定整个系统。此外，2016年发送的所有垃圾邮件中，近40%含有勒索软件[5]。不难想象，只要有一位毫无防备的用户点击了不该点击的东西，企业便有可能失守。

IBM X-Force发现，每两位企业高管中就有一位曾在工作中遭遇勒索软件攻击——也许就是您的企业高管中的一半。[6]

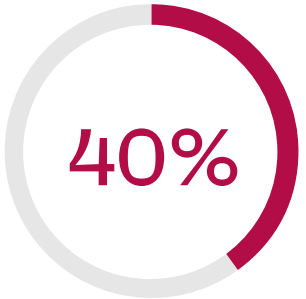
用户：永远是您最薄弱的一环

《Verizon数据泄露调查报告》（DBIR）是安全行业最权威的年度报告之一。每一年，作为全球最大的IT调查机构之一的Verizon研究、调查、解决方案和知识（RISK）团队都会就当年的网络安全状况和主要趋势分享深度洞见。

2017年，RISK团队发现超过90%的安全事件和泄露以网络钓鱼为手段。[7]

同样增速惊人的是受害者数量，勒索软件和其他恶意软件针对用户，而拥有众多设备的用户则深受其害。Verizon的数据显示，2016年有30%的网络钓鱼信息被打开（前一年只有

为黑客购买易于使用的“即服务”攻击选项



的垃圾邮件包含勒索软件

遭遇勒索软件攻击

23%)，而其中又有12%的用户点击打开了恶意附件或链接。[8]

Verizon的2016年度DBIR特别强调了新兴的三步式网络钓鱼攻击：

- 用户收到一封网络钓鱼邮件，内含恶意附件或指向恶意网站的链接。
- 用户下载恶意软件，然后攻击者可以用它来寻找机密和内部信息、通过键盘记录窃取多个应用程序的凭证，或对文件进行加密并索取赎金。
- 有了盗窃的凭证，攻击者还可以展开进一步的攻击，例如登录银行或零售网站等第三方网站。

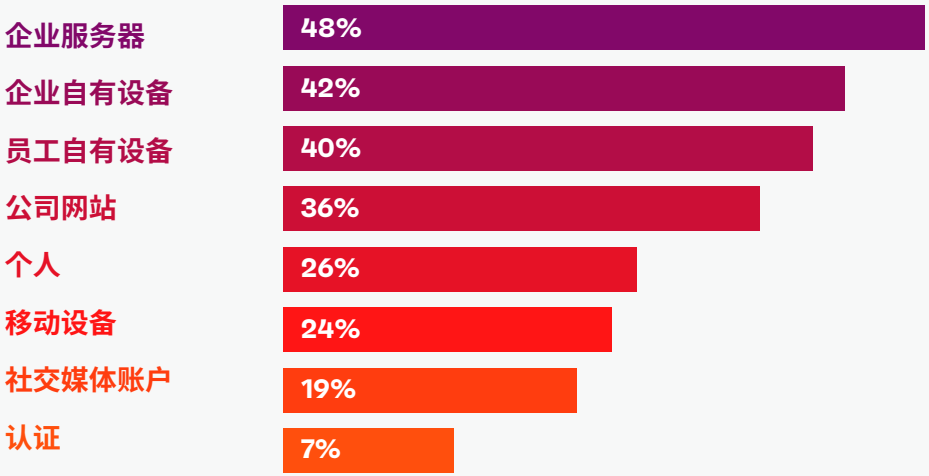
那么，现代网络攻击究竟造成了多少损失？

联邦调查局估计，犯罪分子在2016年第一季度便攫取了2.09亿美元，预计到该年年底，这一数字将超过10亿美元。[9] 而自那以后，情况更变本加厉了。事实是，我们刚刚见识到了第一笔百万美元赎金。[10]

然而，今天的恶意软件，包括勒索软件，所造成的问题并不仅仅是钱。

例如，WannaCry其实并没有谋到太大的收益（截至2017年6月28日的总额约为13.5万美元），但它在传播方面获得了巨大的成功——在一天之内便感染了超过23万台计算机，横行150多个国家。

外部攻击目标：
Forrester 的全球商业技术安全调查



它给企业造成的损失远远超出了赎金本身，支付赎金并不会让企业俯首称臣。问题是，即使支付赎金也不保证一定能恢复丢失的数据；而且，无论结果如何，实际上的损失还包括停机、受损数据、损失的生产力、攻击后的正常业务中断、取证调查、数据和系统的恢复……更不用说您的企业会在客户、合作伙伴和供应链中声誉受损，还可能会面临罚款——如果您最后被发现存在合规问题的话。

联邦快递、默克药厂和航运巨头马士基是这方面的绝佳案例。它们都在今年受到了NotPetya的攻击，且都承认在攻击发生数周甚至数月后还未恢复正常。联邦快递预计系统将在9月底（即攻击后三个月）完全恢复，耗资3亿美元[11]，与马士基的损失金额相近[12]，而默克药厂的估算为2至3亿美元。[13]

专注于您的客户端和服务器

那么，为什么这些拥有强大安全工具的巨无霸企业也会成为这此类攻击的受害者？

首先，企业选择的许多工具并不在保护最脆弱的资产。

Forrester在2016年全球商业技术统计®安全调查（Global Business Technographics® Security Survey）中访问了192位网络安全决策者，他们的公司都在过去12个月内发生过外部安全泄露（员工人数在1000人以上）。调查询问受访者，他们的基础架构的哪些方面是那次外部攻击的目标。结果明确显示，网络中的客户端和服务器才应该是您的关注重点，而不是IT环境的周界。

缺乏重点的安全战略？只会导致无止境的开支

不幸的是，即使您已经掌握了正确的工具来抵御这些威胁，它们也只是您每天配置和管理工作的一小部分。

网络防火墙、网络应用程序防火墙、入侵防御系统、漏洞扫描器……哎呀呀！设备膨胀的成本高昂，且IT团队需要花费大量时间来管理这些设备，这些时间本可用来与安全部门合作，抵御针对环境的真正威胁并作出响应。

打补丁？完全不能真正解决问题

再说，有了正确的工具又如何？它们并不能保证成功。

例如，打补丁并不能真正解决问题。WannaCry和NotPetya的传播都非常迅速，因为它们利用了从NSA窃取的攻击代码和Windows软件的常见漏洞，而这些漏洞都已经有补丁可用。

软件在本质上便是可攻陷的。数十万行的代码，都是人写出来的。应该不会出什么问题，是这样吗？没有人能写出万无一失、对潜在攻击完全免疫的软件。

- **您的软件越旧，暴露出来的漏洞就越多。**Ivanti喜欢用馊牛奶来描述这个问题。牛奶放得越久，就变得越陈。最后呢？牛奶馊了。同样地，软件发布的时间越久远，它的内在漏洞就越有可能被发现、曝光和利用。
- **遗留软件没有补丁可以打。**这不是一定的。例如，在WannaCry攻击出现后，由于威胁传播太广，微软决定为已不再支持的操作系统发布补丁。但一般来说，您无法依赖对千疮百孔的遗留软件进行更新。
- **新软件还没有适当的补丁。**在WannaCry之前，微软支持的Windows操作系统都有补丁，而如前所述，在攻击之后，不支持的系统也有了补丁。然而，即使有了这么多补丁，就在WannaCry攻击的一个月后，企业 又成了NotPetya的受害者。也许，这些企业还没有获得合适的工具来全面修补整个环境。也许，它们的资源有限，虽然已经竭尽全力，但依然没能来得及。无论原因为何，有补丁绝不意味着补丁能够正确打好。
- **还有最后一个问题……不是所有的东西都能打补丁。**打补丁阻止不了零日攻击。又或者，您因故不能打补丁，比如您正在运行遗留系统，或担心打补丁会损坏您的环境中的某些组件？

软件打补丁

- **软件本质上是脆弱的。**
- **遗留软件没有打补丁。**
- **较新的软件未正确打补丁。**
- **你的软件越老，更多的漏洞暴露出来。**
- **并非所有东西都可以修补。**

您需要运用相应工具来屏蔽没有打补丁的应用程序，例如应用程序白名单和权限管理。无论用户以何种方式、在何处访问他们的桌面，都必须确保他们只获得工作所需的授权应用程序，且不能引入未授权的应用程序，以避免降低桌面稳定性、影响安全、违反许可合规要求、导致用户停机和增加桌面管理成本 。

我们从客户那里听到的其他问题

当然，网络安全的难题不止这些。但是，如果用一句话概括，就是IT和安全部门已经投入了大量精力，但失败却不可避免。

他们拼拼补补构建的网络安全点解决方案呢？并不能作为一个整体良好运作，也不能针对环境风险提供全面、集成的视野。思科的《2017年度网络安全报告》显示，55%的安全专业人员使用至少六个安全供应商。

众所周知的网络安全资源短缺让这种情况雪上加霜。由于缺乏人手或工具来判断哪些警报代表危机、为什么会发生警报，安全专业人员经常不不得不忽略对所有警报的调查。该报告揭露的一个事实是，近一半的警报没有得到调查。

想象一下，这些未调查的威胁能对您的工作效率、客户满意度和企业信心造成什么影响。

现在再考虑这一点：把多家供应商的解决方案和平台拿来拼凑使用，在实际上会造成缺漏、提高风险和成本，也会为已经疲于应付的团队和IT管理带来更大的压力。

未来会是什么样子？武器化的恶意软件

毫无疑问，今天的黑客有能力对全球范围内的重要基础设施造成重大影响——医院、银行系统、电网……，且尤其喜欢攻击陈旧、脆弱的技术设施——比如遗留软件。他们也似乎越来越乐意让这种情况发生。

真是噩梦般的场景。无论如何，网络攻击正变得越来越复杂，背后的意图也在变化，这在很大程度上是因为原本用于网络间谍和网络战争的复杂工具现在对任何网络罪犯来说都是唾手可得。

WannaCry勒索软件让世界各地的医院、银行和企业的计算机都陷入了瘫痪。英国的医院在抢修被劫持的电脑时，不得不拒绝收治病人。NotPetya也对医院造成了影响，导致手术取消，还有其他大型企业如航空公司、银行、切尔诺贝利核电站和一家全球航运公司，后者被迫关闭了包括洛杉矶和孟买在内的港口的集装箱码头。

安全和IT专业人员如何才能保护企业，抵御这些复杂、恶毒、意在造成极端影响的攻击？

专注的安全战略？为您带来IT成功

一个成功的安全策略有很多因素：最有效的策略采用分层设计，可提供多种防护选择，应对任何特定情况。消除缺漏。

- 全局显示您的环境状况，毕竟，如果不知道网络上有什么，就无法作出相应保护（或防御）。
- 减少攻击面——阻止恶意软件和攻击代码执行，为您的安全功能和团队争取时机对入侵的威胁作出补救。
- 检测执行的恶意活动。
- 应对并遏制恶意活动和潜在漏洞。
- 此外还有丰富的数据为您的安全态势和合规性提供指导，提高您的工作效能。

您需要的工具应该更易用、更精简，可自动执行安全程序。有了自动化，您就可以让原本紧张的资源摆脱检测和调查的工作负担。

最后，你还需要能够保护甚至提高用户效率的威胁缓解措施。因为无法完成工作的用户必将更多地联系服务台，甚至会用“影子IT”的方法绕过IT，结果将风险引入环境中。

提供纵深防御

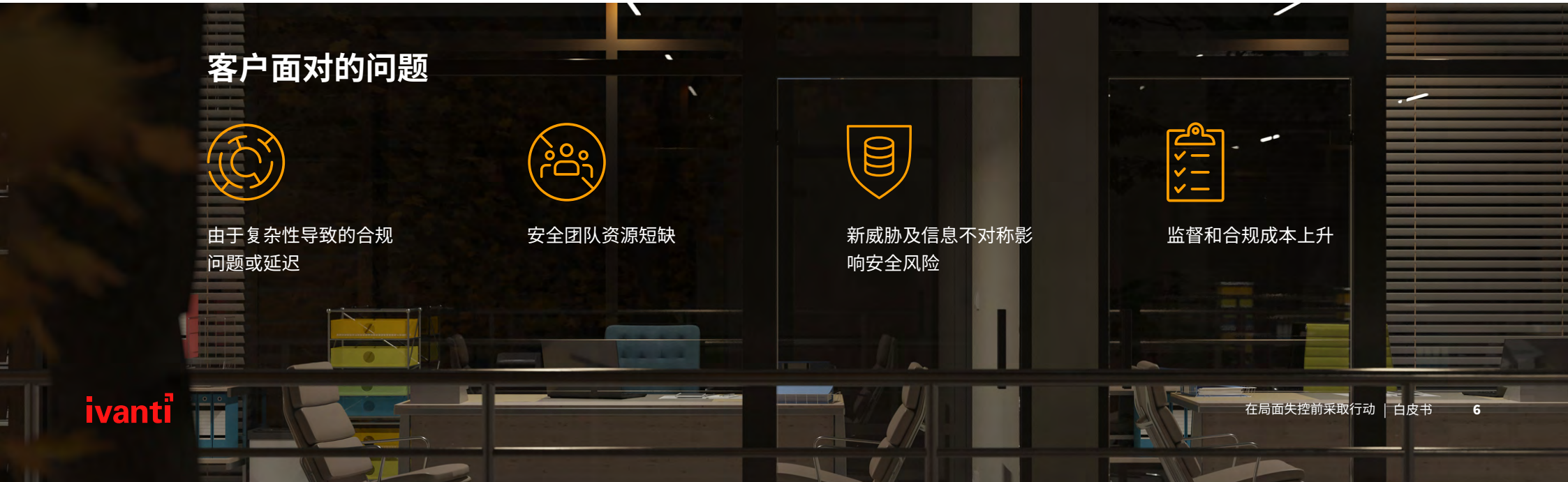
发现全面的风险。

减少攻击面。

检测恶意活动。

采取行动解决问题。

分析数据以洞察问题。



专注的安全战略？为您带来IT成功

通过CIS把这些变为现实

要实现这一愿景，最好的办法是通过一个强大的安全框架。如果安全和IT运营团队能合作实行一套基于共同流程和优先行动策略的专注式安全解决方案，便可降低成本，提高响应速度。

互联网安全中心（CIS）等网络监察机构已达成共识，并正在运用他们的知识和专业技术来识别、验证、推广和维护网络安全最佳实践的采纳。CIS的关键安全控制从NSA的实际经验得出的实践出发，支持和借鉴了许多其他业界领先的网络安全指导。

它的最终目标是什么？是为了帮助您迅速确定防御策略的起点，把稀缺的资源用于可获得即时和高价值回报的行动，以及专注于您企业特有的额外风险。

- 优先行动列表
- 即时和高价值的回报
- 符合监管规定
- 基于实际攻击经验

使用经过验证的框架，找到可满足整个企业大部分需求的单一供应商解决方案，然后针对特殊需要以单点解决方案为补充，将为您降低成本，同时给您想要的高效、纵深的防御策略。

CIS的研究和案例分析表明，按照CIS的基准配置IT系统可以消除80%到95%的已知安全漏洞

通过五个关键安全控制，迅速提升安全水平

具体而言，CIS的五个关键安全控制可以为您奠定坚实基础，极大地改善企业的安全态势。所以，它们也被称为“基本网络卫生”。

1. **硬件资产库存和控制** 用CIS自己的话来说[14]，就是“积极管理（盘点、跟踪和纠正）网络上的所有硬件设备，确保只有授权设备能够访问，未授权和不受管理的设备将被发现并 阻止访问。”
2. **软件资产库存和控制** 同上，但针对于软件：“积极管理（盘点、跟踪和纠正）网络上的所有软件，确保只有授权软件能够安装和执行，未授权和不受管理的软件将被发现并阻止安装或执行。”
3. **持续的漏洞管理** “持续获取、评估新信息并采取行动，以识别漏洞、进行补救并最大限度地减少攻击者的机会。”
4. **控制管理员权限的使用** “盗用管理员权限是攻击者在目标企业内部扩散的主要方式”。提供相应的流程和工具“以跟踪、控制、阻止和纠正计算机、网络和应用程序上的管理员权限的使用、分配和配置”。
5. **硬件和软件的安全配置** “使用严格的配置管理和变更控制流程来建立、实施并积极管理（跟踪、报告、纠正）笔记本电脑、服务器和工作站的安全配置，防止攻击者利用服务和设置漏洞。

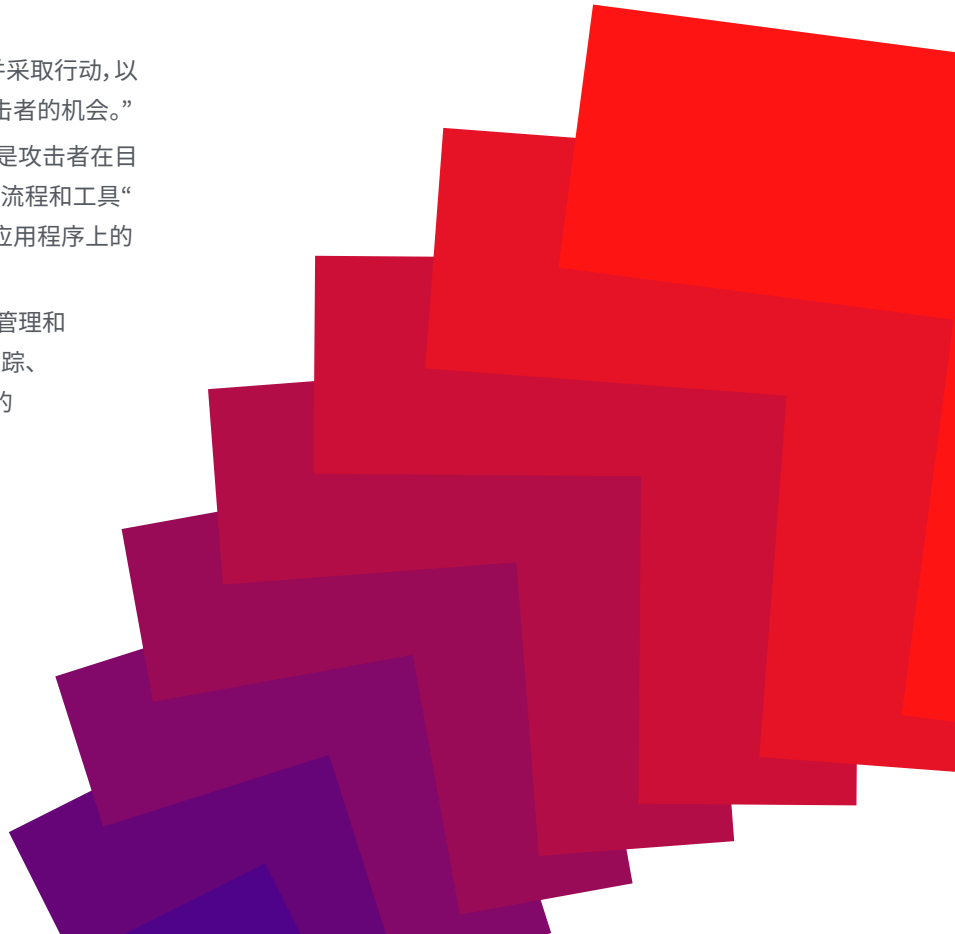
平衡安全性和用户需求

发现用户的需求。

在不受干扰的情况下提供安全性。

提供服务升级/风险规避。

使用正确的工具提高生产力。



自动化功能，例如发现、补丁管理、应用程序和设备控制、管理员权限管理和安全配置等，是基于CIS五个关键安全控制

的Ivanti解决方案的基本要素。此外，Ivanti能帮助客户顺利、经济、轻松地实行这些控制措施，且最大限度地减小对用户效率的影响。用户再也不需要每隔5分钟就联系服务台申请访问权限。未授权、不安全的“影子IT”变通方法被消除了，而工作依然可以快速完成。

我们还可以帮助您了解您的成效

没有对环境的真正洞见，就谈不上真正的防御。Ivanti Xtraction以复选框的形式为您生成报告，按需提供数据，并能够轻松创建新的仪表盘和报告，把准确的数据呈现给高管、总监、业务线（LOB）和应用程序所有者。

预置的连接器可关联您使用的几乎所有工具（服务台、监控和ITAM工具集、电话系统等），无需编码、商业智能专才或电子表格，也无需担心会出现数据孤岛。Xtraction还可以自定义连接更多的工具，让每个人都能查看整个企业的相关数据及其上下文，从海量信息中获得关键、有价值的洞见，轻松地做出更明智、更快速的决策。

总结

不要把钱浪费在错误的地方，也不要让您的安全和IT团队绞尽脑汁为您的企业提供所需的保护，却没有适当的资源和专业协助。实行强大的网络安全策略，从而能够把精力集中在如何达成最重要的目标上。然后，选择能满足这些核心安全需求的解决方案，保护您的网络环境不受当今的复杂、普遍的网络威胁的侵害。

补丁和漏洞管理

尽可能修补和保护操作系统和第三方应用程序。

应用程序控制和权限管理

在实践最小权限原则时阻止所有其他应用程序运行。

端点安全

添加高级反恶意软件和 AV 功能、设备控制 和所有设备的全局策略。

安全程序管理

将安全功能与工作流和资产管理流程相结合 完成一个安全的生命周期。

关于Ivanti

Ivanti 让无处不在的工作空间成为可能。在“无处不在的工作空间”，员工使用数不清的设备访问IT网络、应用程序和数据，以便能够在任何地方保持工作效率。Ivanti 自动化平台连接业界领先的统一端点管理、零信任安全和企业服务管理解决方案，通过单一操作窗口让企业实现自我治疗和自我安全，而用户则能够自助服务。已有超过40,000家客户，包括78家财富百强企业，选择了Ivanti来为他们发现、管理、保护和服务从云端到边缘的IT资产，并为员工提供卓越的终端用户体验，无论他们在哪里、用什么方式工作。更多信息请访问 ivanti.com.cn

ivanti

ivanti.com.cn
+86 (0)10 85412999
ContactChina@ivanti.com

1. Privacy Rights Clearinghouse
2. https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-bylinux-targeting-ransomware/
3. Verizon 2016 Data Breach Investigations Report (DBIR)
4. EY’s Global Information Security Survey
5. 2016-17 5 2016 IBM X-Force research, http://www03.ibm.com/press/us/en/pressrelease/51230.wss
6. Op. cit.
7. Verizon 2017 DBIR
8. Verizon 2016 DBIR
9. http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
10. https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-bylinux-targeting-ransomware/
11. https://www.infosecurity-magazine.com/news/fedex-notpetya-cost-us-300-million/
12. http://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html
13. http://files.shareholder.com/downloads/ABEA-3GG91Y/5005768664x0x954059/3E9E6E5C-7732-4401-8AFE-F37F7104E2F7/Maersk_Interim_Report_Q2_2017.pdf
14. https://www.cisecurity.org/controls