radware

最高管理层视角

网络攻击趋势、安全威胁及业务影响

2018

应用及网络安全
高管调查报告

目录

为了在当今的数字世界中取得竞争优势，企业会依赖网络与客户联系并进行业务处理。

由于越来越多的交易转移到了云端，保护企业和客户数据安全就成了事关重大的工作。为了更好地理解最高层高管们如何看待网络安全及企业对攻击的防御准备程度，Radware 于 2018 年 4 月征询了来自美国(AMER)、欧洲和中东(EMEA)及亚太地区(APAC)的高级领导人的意见。以下是对全球网络安全趋势的总结，这也是高管们最关心的问题。

执行概要

Radware 每年都会发布对全球高管的调查结果和分析，以便更好地了解最高管理层对当前的网络安全挑战和机遇的看法。

这项研究旨在帮助安全行业更好地了解网络攻击现状，新兴威胁、准备程度以及由此对业务产生的影响。此项研究揭示了重要的全球趋势，即安全威胁对企业如何改造网络和保护客户体验的影响，以及高管的主要安全问题的有趣见解。

重要发现

网络变得越来越复杂，人们也越来越关注网络安全

最高层高管们明白，要想进行业务转型，他们必须接受新技术的整合。受访者将提高信息安全和业务效率作为主要目标。90%以上的高管都声称采用了多个公有和私有云环境，其中绝大多数的受访者都很担心这种分散的体系结构带来的安全漏洞。

全球高管都表示，他们准备将自动化流程纳入其安全协议。过去两年间，Radware 研究揭示了网络安全预算向机器学习和自动化技术的转变，但人工过程仍是策略执行的重要部分。

确保网络安全对于保护品牌声誉至关重要

高管们非常担心安全威胁对业务性能的影响，并指出了客户、品牌声誉和运营生产力的潜在损失。许多人都声称调整了预算优先级，以便更好地保护网络安全，防御攻击。

最能影响高管如何看待企业安全漏洞的事件包括备受瞩目的数据泄露、国家攻击、对企业的网络攻击和政府监管。

风险管理计算会影响安全投资

在决定投资在哪来推动企业发展时，最高层高管们面临着艰难的抉择。至少有四成的受访者认为，越来越复杂的基础架构、数字转型规划、人工智能集成以及向云端的迁移等事件都会给安全规划和预算分配带来压力。

最高层专业人员会积极监控网络中发生了什么。据报道，在过去两年，勒索攻击事件急剧增加。69%的受访者表示，他们遭受了勒索攻击，其中多数人都支付了赎金。三分之二的受访者表示黑客可以入侵他们的网络，一半以上的受访者在过去一年都遭受了网络攻击。由于安全专家供不应求，高管们越来越期望由运营商或 ISP/CSP 来管理安全。

网络安全问题因行业而异

攻击对企业网络的影响因企业所处的行业而不同。长期以来，制造商一直将自动化作为提高效率和生产力的一种手段，并表示计划将自动化集成功能到安全措施中，并相应地调整 IT 预算。

金融/保险行业继续其前瞻性思维，将技术作为业务促进因素，并表示计划将业务转移到云端，同时还会继续关注数字转型。零售/批发行业专注于管理日益复杂的 IT 网络、数字转型规划，并将物联网(IoT)用作更好地服务客户的手段。

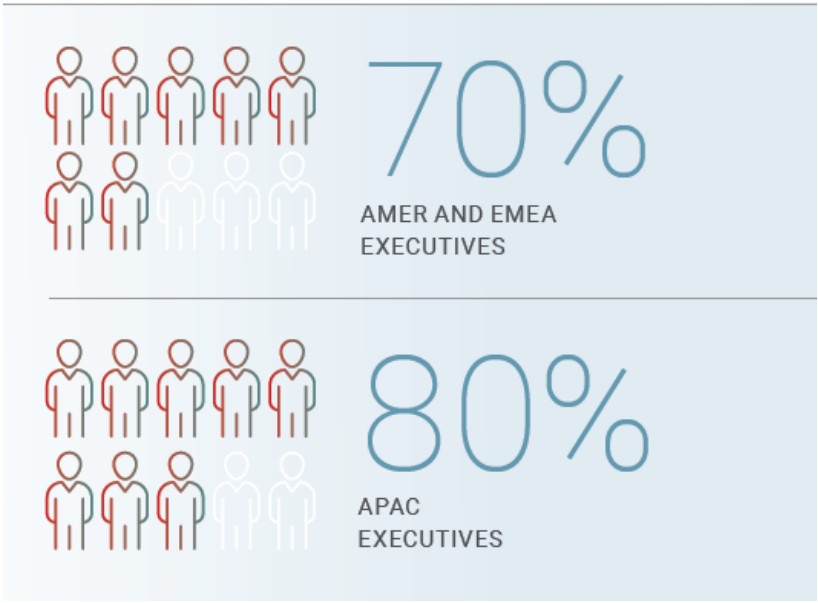
确保
数字转型安全

企业在不断寻找提高生产力和效率的方法。利用他们网络中的技术进步是一个行之有效的方法，更灵活，同时可以降低成本。

客户、员工、供应商和合作伙伴每天都会使用移动应用、聊天机器人、在线门户、电子邮件和其它工具与品牌进行互动。每个接触点都会给网络增加一层复杂性，从而引入危险的新攻击漏洞。

最高层高管们明白，要想进行业务转型，他们就必须在保护数据隐私的同时整合新技术。受访者将提高信息安全和业务效率作为主要目标。紧随其后的是创造竞争优势和提高客户体验。一半的高管(47%)还意识到，数字转型活动给企业的安全规划和投资战略带来了压力。

非常关心数据隐私的最高层受访者的百分比



地区差异：**美国**

创造新的收入来源

与其他地区相比，创造新收入来源对美国受访者而言更重要。

将新收入来源列为排名前三的目标

地区差异：**亚太区**

云端的业务应用

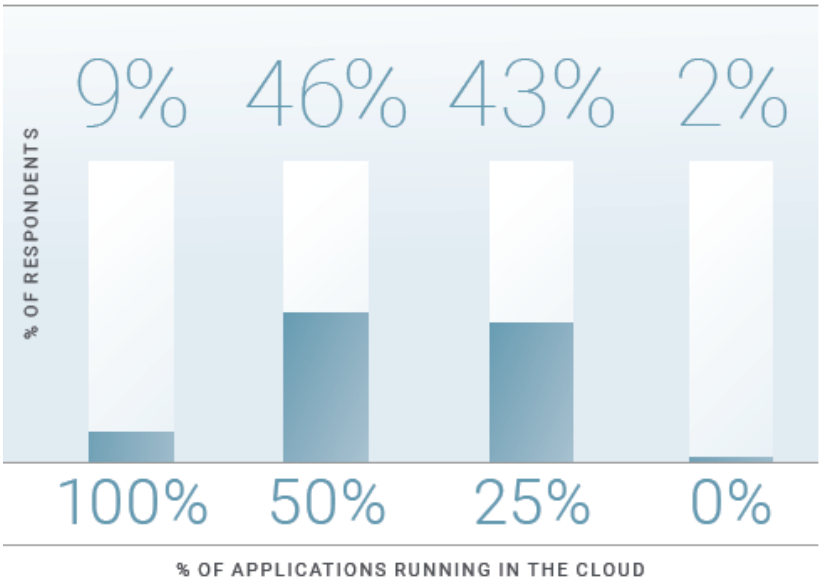
迁移至多个云带来了新的安全问题

90%以上的高管表示采用了多个公有和私有云环境，作为企业 IT 基础架构的一部分。结果显示，多数企业会将 25%-50%的业务应用托管在云中。

重要发现：

显然，最高层高管明白，将网络分散在多个公有和私有云中会带来安全风险。绝大多数受访者(96%)都“非常”或“有点”担心网络漏洞。

在云环境中运行业务应用的百分比



已准备好利用自动化

随着攻击漏洞在复杂网络中的成倍增长，在过去两年，多数(71%)高管称，他们将更多的网络安全预算转移到了采用机器学习和自动化的技术上。约有 25%的高管表示，在此期间，他们的预算重点将保持不变。

重要发现：

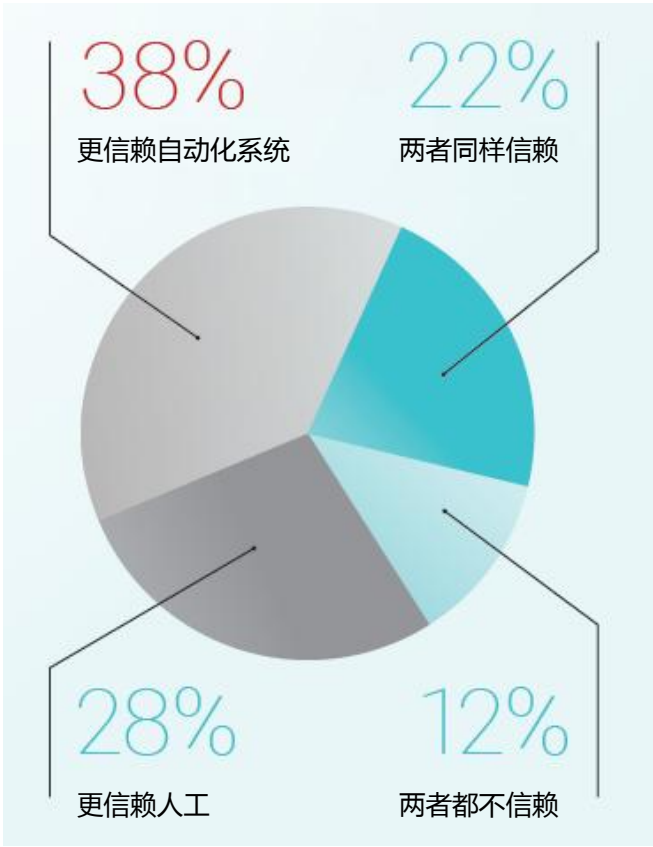
高管们表示，尽管他们已经准备好利用自动化安全防护措施的优势，但人工流程在策略执行中仍占了很大一部分(46%)，这就会让他们面临代价高昂的人为错误。

分配给自动化安全系统的安全预算的百分比

地区差异：**亚太区**

信赖因素

在防御网络攻击时，与人工相比，全球近四成的高管更信赖自动化系统。

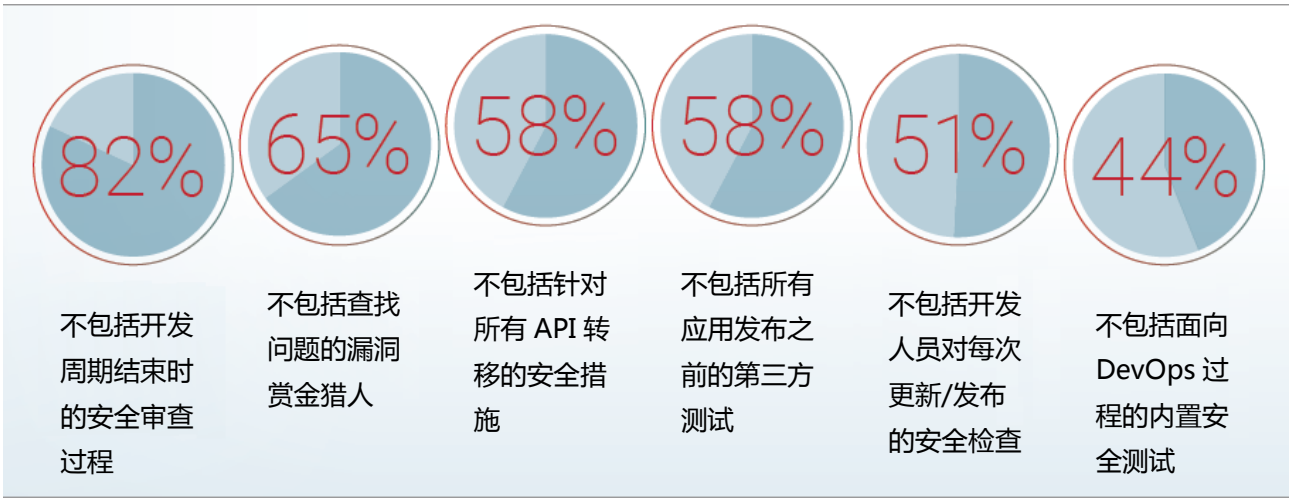


在亚太区，一半以上的受访者表示，他们更信赖自动化系统，而不是人工。

独立的 DevOps

在将新客户体验引入市场的过程中，企业可能会跳过关键的安全检查，从而使其面临本来可以缓解的漏洞。虽然一些企业实施了基本的安全措施，但仍有可以完善的空间。

高管们表示，他们尚未将安全实践集成到应用开发周期中。



将安全性作为 DevOps 过程的一部分的企业表示，**自动化和人工策略执行之间几乎均衡的划分。**。

加密流量的不确定性

随着越来越多的交易涌入互联网，加密流量的容量也在增加。根据谷歌透明度报告 [1]，2015 年以来，跨所有平台(Windows、Android、Chrome、Linux 和 Mac)的 HTTPS 加密流量增长了约 50%。

自 20 世纪 90 年代初以来，安全套接字层(SSL)协议一直是实际上的加密技术。频繁曝光的漏洞导致了其它协议的开发，如传输层安全(TLS)。

[1] Google Transparency Report: https://bit.ly/2sMEYcr

根据 Radware 2017-2018 年全球应用及网络安全报告[2]，30%的企业都声称遭受了 SSL 攻击，另外有四分之一的企业不确定是否遭受了此类攻击。SSL 攻击有多种形式，包括加密 SYN 洪水、SSL 重新协商、HTTPS 洪水和加密 Web 应用攻击。

高管们将加密攻击列入了他们认为危害最大的网络攻击列表中。来自美国的受访者(45%)最有可能将加密攻击视为最大问题，其次是欧洲(41%)。

许多企业都是在没有加密攻击防护措施的情况下运营的。他们面临的部分挑战是，由于 HIPAA 和新的 GDPR 要求等政府法规，他们不确定解密流量进行检查的合法性。许多企业利用 WAF 和/或 ADC 来监控入站流量，尤其是在美国(47%)。

复杂的合规性

地区差异：**亚太区**

SSL Web 策略

[2] Radware 2017-2018 年全球应用及网络安全报告：http://global.radware.com/APAC_2018_ERT_Report_EN

为客户创建安全的环境

公司网络是与客户互动的关键，这些客户期待响应及时的应用、快速的性能，最重要的是，能够保护数据安全的防护措施。

客户体验的基础就是信任和可用性。如果任何一个因素出现问题，企业品牌都会受到冲击。

最高层高管非常清楚安全威胁对企业的影响。受访者认为以下三个安全威胁对企业的影响最大：

1. 客户流失(41%)
2. 品牌声誉受损(34%)
3. 生产力/运营损失

客户回击

41%

的高管表示，发生数据泄露事件后，客户会起诉企业。

问题近在咫尺

当企业目睹其所在市场的企业遭受攻击后，他们更有可能改变内部安全策略。

影响企业安全改变的特定事件

针对同行公司的备受瞩目的数据泄露事件

自己企业遭受的数据泄露事件或网络攻击

GDPR、PCI、HIPAA 等政府法规

国家攻击

最高层领导变动

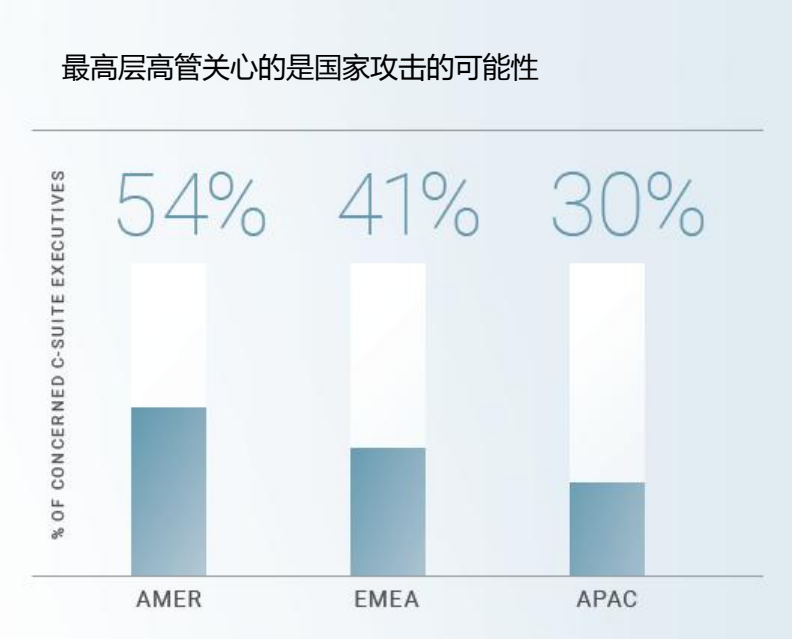
在评估企业安全协议时，高管(61%)表示，针对同行公司的备受瞩目的数据泄露事件是主要影响因素，其次才是对自己公司的网络攻击(59%)。高管们还看到，在 Equifax 和 Target 等公司发生数据泄露事件后，最高层高管会被解雇。

重要发现：

客户并不是网络攻击的唯一受害者。四成以上的高管表示，由于数据泄露事件，他们的个人信息也被曝光了。

发生国家攻击时

过去，企业间谍活动通常是指相互竞争的公司试图窃取商业机密。现在，带有政治和军事目的的不良分子把目标对准了企业网络，获取数据、索要赎金或肆意进行破坏。



平衡
投资和风险

在决定投资在哪来推动企业发展时，最高层高管们面临着艰难的抉择。

由于网络攻击的威胁变成了何时发生而不是是否会发生的问题，因此企业必须仔细评估与安全漏洞相关的风险以及实施有效的安全解决方案的成本。

40% 的受访者认为，以下因素会对企业的安全规划和投资带来压力：	1 越来越复杂的基础架构
	2 数字转型规划
	3 人工智能与业务流程的集成
	4 向云端的迁移

为不可避免的趋势做好准备

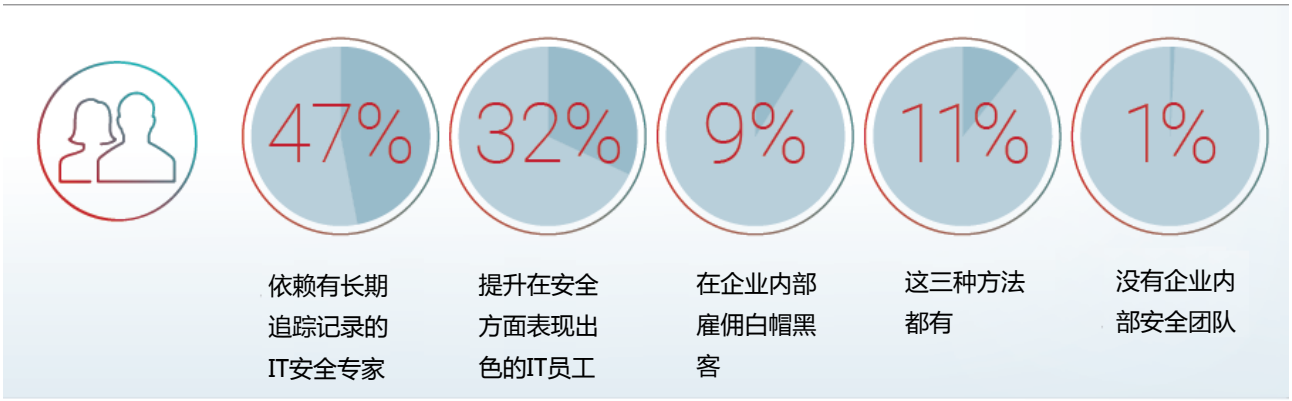
尽管网络攻击的威胁一直笼罩着企业，但仍有约 25%的受访者承认他们无法解决重要安全问题或正处在规划阶段，如对新技术进行安全评估(23%)，或与教育机构协作，积极招募安全专家(31%)。

排名最高且已出现两年以上的安全措施包括，要求供应商完成安全检查和进行网络安全保险投资。高管们描述了近两年与相似企业共享网络攻击情报的进展，与远程工作相关的更严格的策略，以及越来越多地依赖自动化解决方案。

重要发现：

对最高层高管而言，及时了解安全问题是一项永无止境的任务。五分之二的高管称会依赖安全厂商来了解最新攻击矢量，并不断更新安全措施。约有三分之一的受访者表示，企业的内部团队负责日常安全。约有五分之一的受访者向第三方研究公司订阅了安全问题更新。

高管们将内部安全团队定义为以下的人才类型：



重要发现：

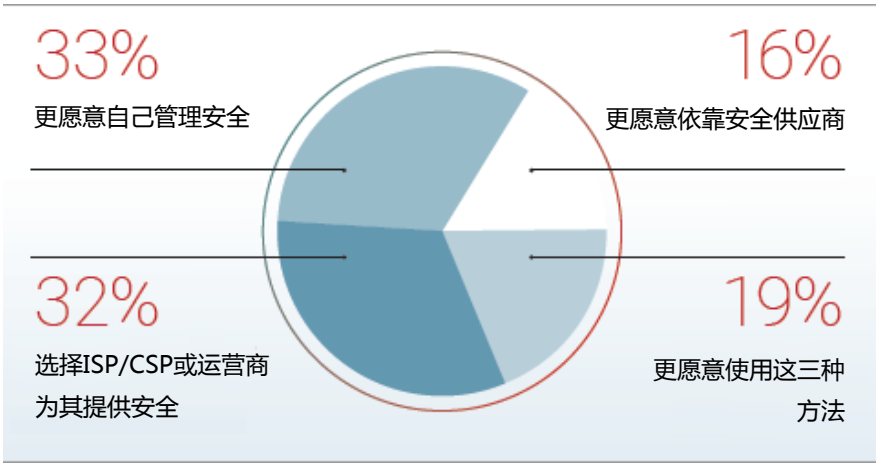
所有地区的多数受访者(65%–81%)认为，他们的内部安全资源足以满足他们的安全需求。然而，66%的受访者认为，黑客可以入侵企业网络。

由于安全专业人士的供不应求，内部技能缺口并不容易解决。因此，更多的高管表示，有必要向外部安全供应商寻求帮助。

66%

的受访者认为黑客可以入侵企业网络。

人才短缺迫使高管们转向企业外部寻求安全支持。



人才短缺遥遥领先

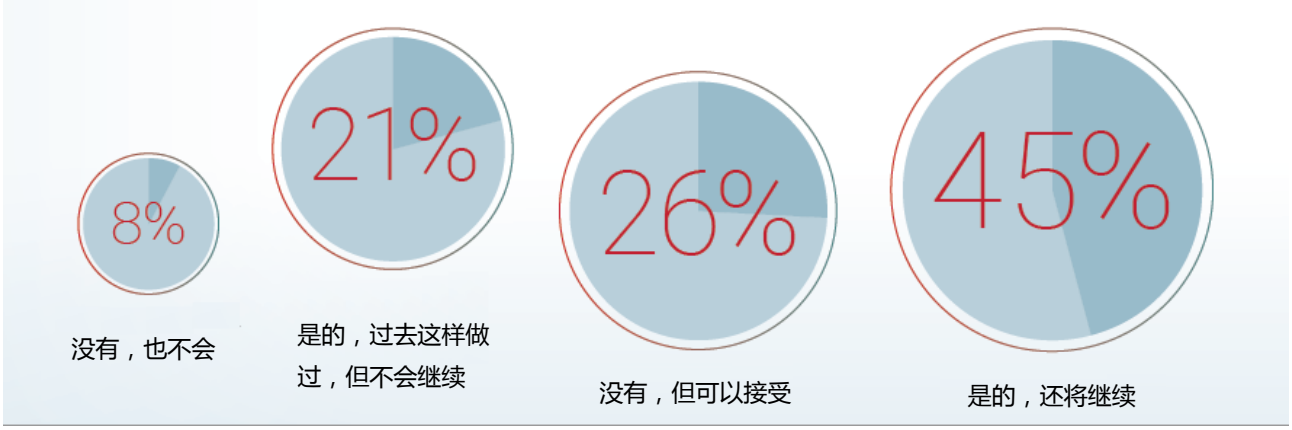
根据最近的网络安全风险投资报告[3]，由于安全人才的缺失以及网络攻击事件的日益增多，到 2021 年，将会出现 350 万个 网络安全职位空缺。随着需求的增长和供应的减少，对知识型人才的争夺可能会增加。

[3] 网络安全风险投资新闻：https://bit.ly/2Jeq6i9

雇佣黑客

约有三分之二的受访者“极其”或“非常有可能”为内部安全团队雇佣一名前黑客，而近一半的受访者表示，他们已经邀请了黑客来测试系统，查找漏洞，并将继续这样做下去。

为 IT 安全团队雇佣前黑客的可能性



高管们对前黑客或现任黑客测试漏洞的开放程度是有限的，这可能是因为与回报相比，风险过高：

- 15%的高管不允许黑客测试企业的物联网(IoT)应用和设备
- 18%的高管不允许黑客测试企业数据库
- 17%的高管不允许黑客测试企业策略和程序

地区差异：**亚太区**

欧洲高管是最先让黑客参与保护网络安全的。

根据Radware 2017-2018年全球应用及网络安全报告[4]，这可能是因为这些地区的网络遭到攻击的可能性要高两到三倍。

在去年的高管调查报告中，欧洲高管最有可能为安全团队雇佣前黑客。今年，美国和亚太地区赶上了欧洲；一半以上的受访者表示，他们“非常”或“极有可能”雇佣前黑客。

[4] Radware *2017-2018 年全球应用姐网络安全报告：*
http://global.radware.com/APAC_2018_ERT_Report_EN

计算数据泄露事件的成本

数据泄露的代价很昂贵。这不仅会增加货币成本，直接影响到企业利润，而且更令人头疼的是对品牌声誉和客户信任等资产的损害。近 40%的受访者估计，每次攻击的刚性成本都在 100 万美元/欧元/英镑/人民币以上，其中有 5%的受访者估计，成本在 2500 万美元/欧元/英镑/人民币以上。虽然软性成本难以量化，但从长远来看，软性成本的影响要比刚性成本要高得多。

刚性成本	软性成本
因业务损失、内部资源使用、外部资源成本、赎金、律师费和其它可计入项目造成的可量化的货币损失	包括品牌破坏、客户流失、生产力损失、高层领导变动、股票估价下降和其它主观因素等在内的定性损失

高管们对影响最大的数据泄露和危害最大的攻击类型的排名

安全威胁对企业的影响

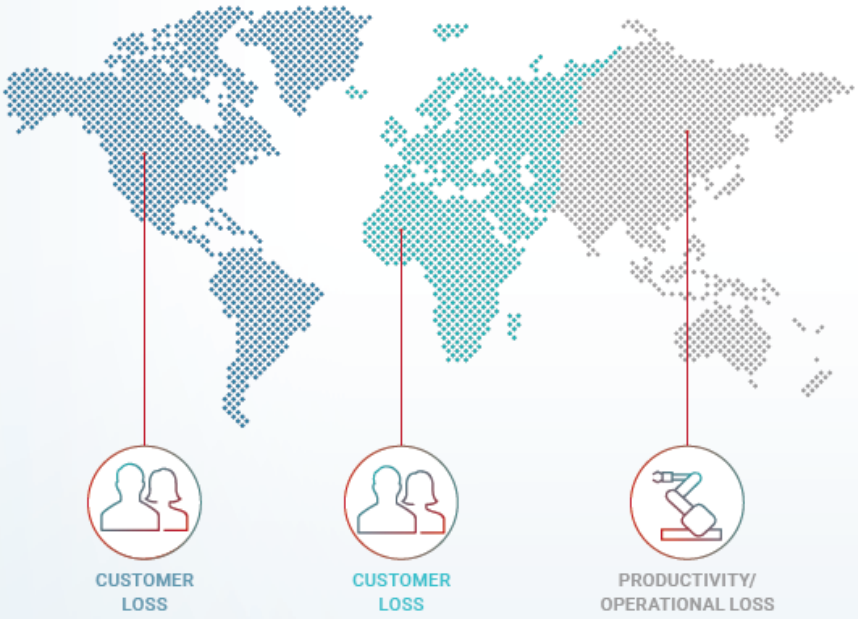
1. 客户流失
2. 品牌声誉受损
3. 生产力/运营损失

危害最大的攻击

1. 社会工程威胁
2. 勒索软件
3. 恶意软件

各地区的业务影响

每个地区的受访者对网络攻击对其业务的影响的权重各不相同



AMER

1. 客户流失
2. 股价下跌
3. 收入损失

EMEA

1. 客户流失
2. 品牌声誉受损
3. 收入损失

APAC

1. 生产力/运营损失
2. 客户流失
3. 知识产权损失

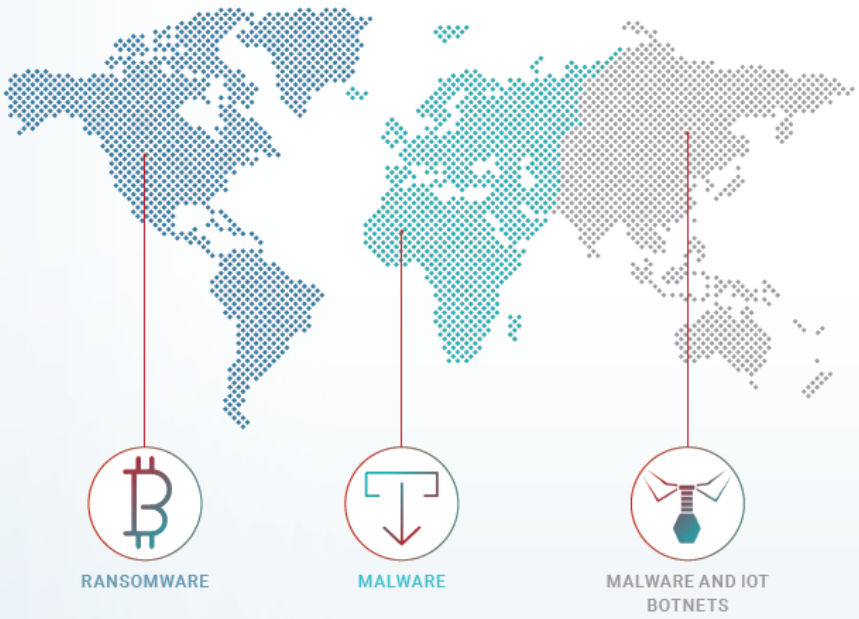
被攻击笼罩的企业

现实是，企业每天都面临着大量的威胁和攻击。许多高管不确信是否能够阻止侵入到企业网络的黑客。他们全力扩展安全基础架构，与部署在网络内部的技术进展保持同步。

最高管理层对当前网络威胁的看法

攻击严重程度的地区差异

高管们认为以下攻击类型的危害最大



AMER
1. 勒索软件
2. 加密攻击
3. 脉冲式攻击

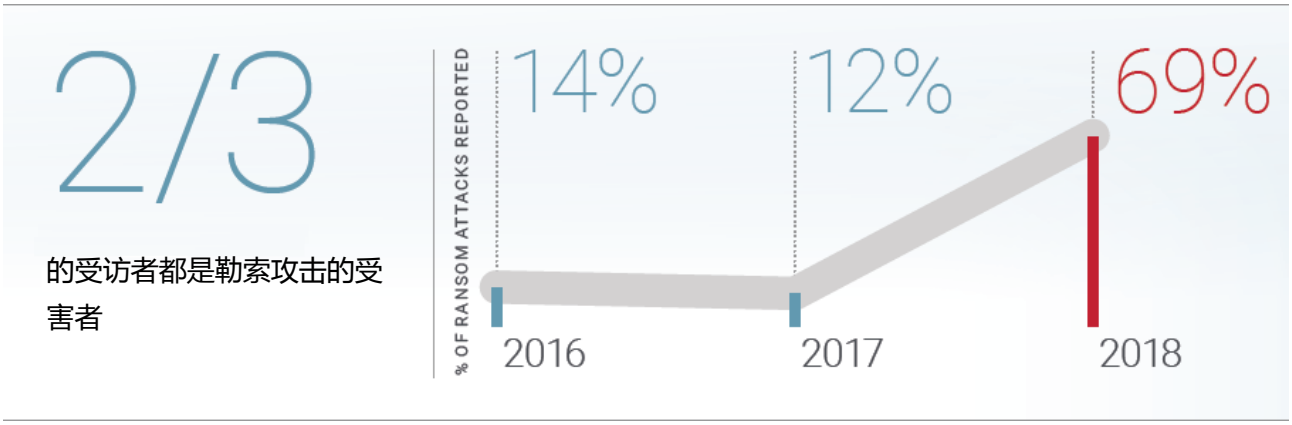
EMEA
1. 恶意软件
2. 高级持续性攻击
3. 社会工程攻击

APAC
1. 恶意软件及IoT僵尸网络
2. 社会工程和Web应用攻击

赎金的计算

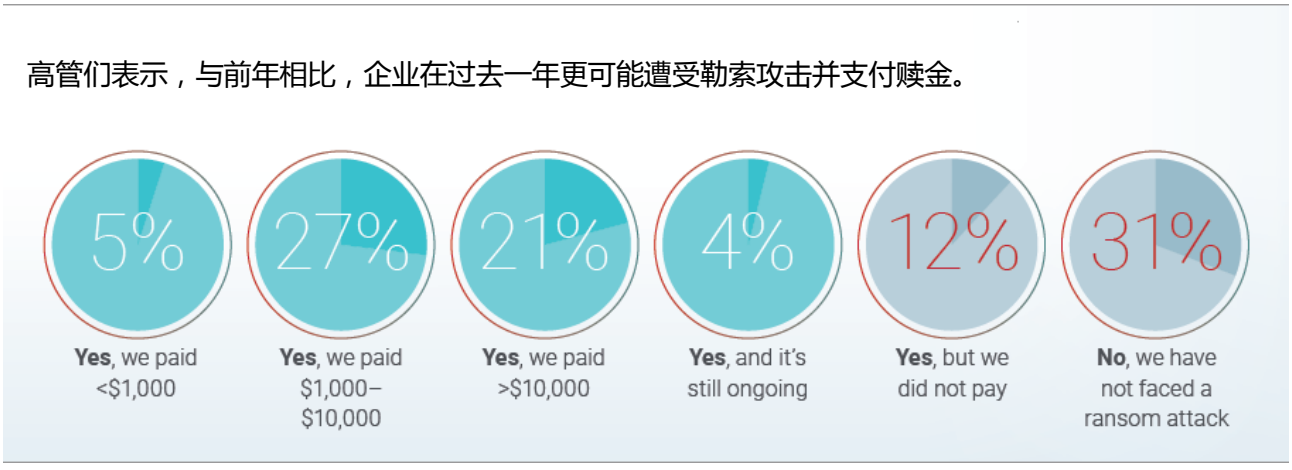
Radware 年度高管报告的受访者指出了过去两年勒索攻击频率的大幅上升，以及企业支付赎金的意愿。

过去两年，勒索攻击急剧增加



尽管最高层高管不太可能对每一个安全威胁都了如指掌，但多数(69%)高管称，企业在过去一年都遭受过勒索攻击，其中多数企业都支付了赎金。在那些尚未遭受过勒索的企业中，一半以上的高管表示他们可能会支付赎金，这取决于风险或赎金金额。

勒索攻击越来越令人担忧



影响
垂直行业

攻击对企业网络的影响因企业所处的行业而不同。从方向上看，对制造行业、零售行业和金融行业受访者的调查结果显示，新兴的安全趋势针对的是各个垂直领域的需求。

零售/批发行业

将近三分之二的零售企业表示，企业至少有一半的业务应用都位于云端，他们担心云网络之间的安全漏洞。过去一年间，这一垂直领域的管理层通报了近 20 起攻击事件。(这是一些规模大到足以引起最高层注意的攻击。)为了支持电子商务，这些企业网络中的客户接触点最多，因此很让人头疼。

高管(77%)表示，自己企业的数据泄露是对企业安全规划影响最大的事件。

规划和投资重点关注的是越来越复杂的企业 IT 基础架构(64%)、数字转型规划(58%)以及 IoT 的应用(50%)。

这一垂直行业可能(47%)希望供应商或 ISP/CSP 来提供安全防护措施。

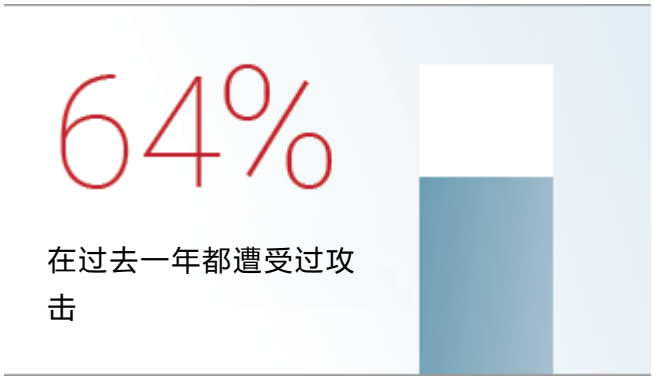
高管们估计攻击的成本为 160 万美元/欧元，三分之二的企业在遭受勒索攻击之后支付了赎金。

制造行业

长期以来，制造商一直将自动化作为提高效率和促进生产的手段。因此，受访者专注于管理日益复杂的 IT 基础架构(50%)并计划集成自动化(43%)来实现自动化安全措施，就不足为奇了。为了实现这一目标，高管们(75%)表示会将更多的 IT 预算转移到安全自动化上。

受访者密切关注市场上发生了什么，有三分之二的受访者表示，针对同行公司的备受瞩目的数据泄露是对他们自身安全规划影响最大的事件。

高管门估计攻击的成本为 360 万美元/欧元/英镑/人民币，三分之一以上的企业在遭受勒索攻击之后支付了赎金。



金融/保险行业

企业网络是金融企业业务的命脉，这也是这一垂直行业可能会更多地投资于安全来保护资产的原因。例如，在 2017 年遭受了网络攻击的 Deloitte5 表示，在未来三年，公司计划在安全方面投资 5.8 亿美元。

金融企业尤其需要了解同行公司的情况。受访者(86%)称，针对同行公司的备受瞩目的数据泄露事件是对他们自身安全规划影响最大的事件。

高管们描述了一幅未来增强网络安全的场景，其中，计划迁移到云(68%)、数字转型规划(65%)和集成安全自动化(62%)在规划和投资重点中排名最高。

通过集中在第三方测试(59%)和内置在流程中的安全测试(56%)，这一垂直行业正在集成并执行 DevOps 安全。

高管们估计攻击的成本为 230 万美元/欧元/英镑/人民币，几乎一半的企业在遭受勒索攻击之后支付了赎金。

59%

的企业在过去一年都遭受过攻击。

展望未来

最高层高管意识到，企业在整合新网络技术、进行业务转型和防御频率和复杂程度都在不断增加的网络攻击方面面临着多重压力。

随着越来越多的企业在 IT 体系架构中增加了多个公有和私有云环境，新漏洞的引入将企业和客户数据置于危险之中。

高管们知道，他们的网络可以被黑客入侵，并且也做好了将自动流程纳入安全协议的准备。越来越复杂的基础架构、数字转型规划以及人工智能的集成都会影响他们对安全规划和预算分配的考虑。

风险很高。安全威胁会严重影响企业的品牌声誉，进而造成客户流失，降低运营效率并引起法律诉讼。这份高管调查报告的结果强化了网络安全在全球高管心目中的重要性。

关于此研究

2018 年 4 月，Merrill 研究所代表 Radware 对全球来自美国、欧洲和亚太等地区的 232 名高管进行了调查。参与 2018 年应用及网络安全高管调查报告的受访者必须来自收入至少为 2.5 亿美元/欧元/英镑/人民币的企业，且拥有高级副总裁或更高的头衔。尽管今年的调查吸引了 更多的最高管理层企业领导人， 但至少有一半的受访者必须是最高管理层高管。参与调查的企业中约有一半企业拥有 1,000 到 9,999 名员工，平均员工数约为 3,700。美国受访者的平均员工数最高，约为 4,300。

Radware 是为物理数据中心、云数据中心和软件定义数据中心提供网络安全和应用交付解决方案的全球领导者。Radware 屡获殊荣的解决方案组合为全球企业提供了基础架构、应用及企业 IT 防护服务，确保企业的数字体验。Radware 解决方案成功帮助了全球 12,500 多家企业和运营商客户快速应对市场挑战，保持业务连续性，在实现最高生产效率的同时有效降低成本。更多信息，请访问：www.radware.com。