SYNTAX

企业IT安全

终极指南

SYNTAX .COM

面对新一代IT安全威胁，您是否未雨绸缪？

生命中只有三件事是必然会发生的：死亡、纳税以及数据泄露。

企业所面临的安全风险和威胁会比以往更多。

由于各大公司纷纷在云端和传统系统上扩展IT环境，因此显著扩大了受攻击面。

同时，移动和物联网(IoT)设备的扩增也让网络罪犯有了新的入侵点。因为一切都是联网的，只要有一台设备受到攻击，就会迅速波及整个公司。

> 数据泄露造成的损失平均起来，高达820万美元，而且需要279天才能检测到并遏制这类泄露现象。
>
> **波耐蒙研究所[1]**

到时就不再是“是否”会遭遇数据泄露的问题，而是数据泄露“有多频繁”和“有多严重”的问题了。

本指南概述了为了防止公司遭受不断发展的风险和威胁而必须采取的措施。

本指南将向您介绍：

- **应时刻盯紧的头号IT安全威胁**
- **为什么数据保护必须习惯逆耳忠言**
- **如何获得对IT安全的认可**
- **综合IT安全战略的各个层面网络安全**
- **人才短缺让企业面临风险**
- **在雇佣安全管理服务提供商之前应该询问的关键问题**

有了正确的IT安全战略和合作伙伴，公司便无需对数据中心、设备和新增内部员工进行投资。

请继续阅读一些最佳实践，了解怎样最大限度地降低安全风险，让内部团队不再埋头于IT管理和技术支持工作，而是全力专注于创新。

应时刻盯紧的头号IT安全威胁

IT安全形势如今正在迅速演变。预计今后几年会出现下列情况。

黑客们会对关键任务资产发起复杂的攻击，其行动远超网络钓鱼。

而从关键任务企业资源计划(ERP)应用程序（如Oracle和SAP）到工业控制系统，又无一不是开放性系统。

与此同时，欧盟和加利福尼亚州等政府正在推行严格的数据保密法规。

这项新法规使公司在保护IT系统，确保客户、员工和供应商的数据保密性时面临更大的压力。

有51%的组织认为自己尚未做好面对安全漏洞的准备，或者无法有效应对安全漏洞。[3]

如违反该法规，则可能面临处罚，对企业造成重大影响。例如，GDPR罚款达到2000万欧元，或高达上一财年全球年营业额的4%，以金额较大者为准。[2]

对于上述变化，大部分企业都感到措手不及。

如何区别风险与威胁

风险是您要避免发生的情况。而威胁则会利用该风险发起攻击。

当您在为来年的网络安全措施做规划时，应考虑下列内容：

1 针对操作技术系统的威胁

针对操作技术（OT，为工业控制系统提供动力的设备）的攻击正呈上升趋势。根据操作技术的状态和网络安全报告[4]，有74%的OT组织在过去12个月内经历过一次恶意软件入侵。

调查的受访者们列举了这些违规行为造成的诸多影响，其中包括“安全性、生产率和收入下降，关键业务数据泄露，品牌声誉受损。”可见性不足是造成这些攻击能得逞的主要原因，因为报告显示有78%的受访者都对其OT环境的网络安全情况一知半解。

IT团队是很难掌握OT环境的全局全貌的，因为诸如阀门、发动机和生产系统这样的OT设备，可能超出了其传统的领域。因此，这些攻击非常令人担忧，针对该问题，一个名为操作技术网络安全联盟(Operational Technology Cyber Safety Alliance)[5]的新组织应运而生，其使命是“为广大OT运营商和供应商提供资源、指导，以降低其在快速发展的世界中面临的网络风险。”

2 物联网漏洞

企业型自动化物联网设备的范围很广，从制造车间的机器人到办公室厨房的联网微波炉均算在内，不一而足。其中还包括个人设备，比如健身追踪器和智能手表。

事实上，还有30%的企业甚至报道也会将游戏机（比如Xbox或PlayStation）接入公司网络。[6]由于物联网设备扩展到整个公司组织，IT团队往往不清楚有多少人在访问公司网络，也不知道访问者的身份和目的。

所有受访者都发现过欺诈性的物联网设备，90%的受访者发现过先前未检测到的独立于自家企业架构的物联网无线网络。[7]第三方物联网也会招致风险，因为IT团队几乎不能控制这些设备。

波耐蒙研究所的一项研究表明，大多数企业组织并未察觉到公司网络上每一个不安全的第三方物联网设备或应用程序。研究还显示，49%的企业不会定期扫描工作场所的物联网设备，只有8%的企业表示会执行实时扫描。[8]

影子物联网的存在，再加上可见性受限，也难怪有67%的企业都经历过管理物联网设备的安全事件。事实上，有84%的IT领导都表示，物联网设备比公司的管理电脑更易受到攻击。

比起其他类型的数据泄露，针对物联网设备的攻击的危险性要大得多，因为黑客们会将发电站、水处理厂、炼油厂和铁路的物联网设备列为攻击目标。为此，IT世界论坛这样引述物联网攻击最严重的后果之一：“火灾、爆炸或制造设施停运后，为了恢复正常运营而需要产生财务成本”。

3 复杂的勒索软件

根据Malwarebytes实验室的一份报告，勒索软件攻击已急剧增加。[10] 2018年至2019年间，企业检测到勒索软件的比率上升了500%以上。2020年，将有更多的威胁源起方针对企业网络发起两阶段的勒索软件攻击，妄图泄露敏感数据。[11]

如果您的公司遭到了勒索软件攻击，就会面临诸多严重后果。这些风险包括：

- 如果关键系统在攻击下崩溃，就会导致生产率和收入损失。
- 将客户数据遭到入侵的情况告知客户后，品牌和商誉就会受损。
- 损失惨重。勒索软件造成的平均损失为 84,116美元——远高于上一个季度的41,198美元。[12]

很多公司都没有合适的工具和资源来拦截威胁。

专家认为，传统的反病毒解决方案已经不能保护公司免受攻击了。
如今勒索软件进化得愈发难以检测，而公司的用户数量正在激增，因此这些老式的工具无法适应要求。

SANS研究所的一份报告[13]指出，反病毒解决方案只能截获47%遭到入侵的端点。
为了保护您的数据，要寻求一种端点保护解决方案，它能覆盖所有网络区域，可以实时识别威胁。

> “物联网设备面临的风险极大，因为它们通常都处于数字世界与实体世界的交界点上。因此，非法入侵物联网设备会导致现实世界中发生十分危险的后果。”
>
> IT World

4 ERP安全威胁

您是否知道有64%的SAP和Oracle电子商务套件(EBS)部署曾在过去24个月中遭遇过数据泄露?

在这些数据泄露中遭到入侵的信息包括销售数据、人力资源数据、客户个人身份信息、知识产权，以及财务数据。一旦公司最敏感的数据遭窃，后果会极其严重——从违反法规，到财务损失，到最终破产。

然而，很多公司却没有做好应对ERP数据泄露的准备。比如，这些公司运行ERP系统的传统技术可能已经过时，并不安全。事实上，在最近的一项调查[16]中，有82%的高管表示，传统技术为关键业务环节提供支持，而且与公司核心系统集成。

优质威士忌或葡萄酒越久越醇，技术则反之，陈久意味着落后。

您依赖传统系统的时间越久，面临的风险就越大。大部分传统技术太过时，连制造商都不再为其提供支持，因此也无法定期更新或打补丁。

正是这种疏忽造成了安全漏洞，让公司的敏感ERP数据暴露在网络罪犯面前。

> “如果因某场灾难失去数据中心10天或10天以上，有93%的公司会在灾难发生一年内申请破产。而同期50%的企业在发现丧失数据管理后，也会立即申请破产。
>
> 美国国家档案局[15]

5 云的不安全性

每年都有越来越多的公司将其关键任务工作负荷转移到云端，并努力克服由此产生的新安全问题。

根据SANS研究所的数据[17]，有19%的企业在过去一年中曾遭遇过云数据泄露，较2017年增长了7%。

一份云安全报告[18]透露，企业的前五大云安全威胁包括：

- **未授权访问**
- **不安全的接口与应用程序接口(API)**
- **云平台配置错误**
- **帐户或服务器被劫持**
- **数据的外部共享**

云数据泄露导致的后果不一，具体取决于黑客窃取的数据类型和数量，但其中肯定包括在暗网上公布员工、客户和专有数据。一旦数据失控，您必须迅速做出响应，才能遏制品牌和财务损失。

通常，云服务比传统系统更安全。但您不能坐等提供商去打理安全开箱即用系统的方方面面，也不能信赖传统安全工具在云端运行。

云安全报告指出：

> **“有许多传统安全工具的设计并不适合动态、分布式的虚拟云环境。”**

三分之二的受访者表示，他们的传统安全解决方案在云环境下要么根本无法运行，要么功能受限。

6 了解云安全的共享责任模型

有很多企业组织将现场数据存储设施迁移到云上之后，就会迅速应了“眼不见，心不烦”这句古老格言。

尽管云提供商在承担基础架构安全责任方面无疑是首当其冲的，但他们并不负责保护云端的数据。起用云提供商的公司可能会认为这不符合逻辑，但云共享责任模型很明确地阐述了云提供商与公司双方的安全义务。

这种模型如果维护得当，应当能够提高公司的安全性。

为什么似乎刚发生的数据泄露事件隔天就会上头版头条？

如果公司对于安全责任以及如何管理安全责任存在根本性的误解，就容易受到网络威胁的攻击。

在共享责任模型下，云提供商负责保护云基础设施（包括硬件、软件、网络连接和设施）的安全。另一方面，云客户负责保护自己存放在云端的数据的安全，包括端点、帐户和访问管理。

试想，云共享责任模型，就好比送孩子上学。学校系统代表云提供商，它负责保护孩子安全，以及维护孩子读书的教学楼。但是您身为父母，也就是云的客户，
照料自己的孩子仍是您的最终责任。如果您的孩子，也就是数据，表现失当或感染了病毒，您有责任照顾他们。只有我们双方都各尽其职，系统才能顺利运行，各方才会受益。

您要如何应对这些威胁？

大多数企业组织面对规模和复杂程度日益加剧的网络攻击是毫无准备的。

当您在推行IT安全战略时，应多加考虑它是否能保护您的公司免受上述威胁。如果不能，您就需要配备额外的资源来保护公司。

7 推卸数据责任

企业组织认为，云服务提供商应当负责保护自己存放在云端的数据。这种误解产生的影响很严重。

艾可飞(Equifax)的数据泄露事件[19]泄露了大约1.5亿美国人的个人信息，将近全国总人口的一半。在这起案例中，国土安全部曾警告过Equifax其数据库易遭攻击，但Equifax无视该警告。该公司的数据管治措施不力，其中加密凭证续期失败、以明码文本存储密码，已知漏洞无法修补，这些都是导致数据泄露的温床。

掌控自己的数据

一旦您理解了云共享责任模型，明确了自己在模型中的角色，您就能采取必要的措施，更有效地保护公司数据。

- 建立牢固的供应商关系：即使您要为自己的数据负最终责任，也无需独自应对复杂的网络安全工作。造成对云共享责任模型的误解的主要原因可能是沟通不良。而一个优秀的云合作伙伴应该是坦率公开、善于沟通，并且积极响应的。如果您没有意识到自己承担的数据责任，那么您与云提供商的关系可能并不牢固。
- 首先考察合规性：同样，要寻找一个通过行业审查、可信赖的云提供商。只有16%的云服务通过了一家或多家第三方认证[20]，比如IPAA、PCI、SOC2、SOC3、PCI DSS 或SSAE16。这些认证可以表明云提供商在以客户名义对待安全性和合规性时的严谨程度。
- 招贤纳士：很多管理层的信息安全领导都明白自己的职责是保护数据，但30%的公司都没有足够的人手来保护SaaS应用程序的安全[21]。至于其他的企业组织，则完全没意识到自己的安全职责，对管理这些职责所需的人员和资源也完全没有概念。所以，请与网络安全经理合力打造您的IT部门，确保您的数据得到妥善保护。
- 教育员工：有五分之一的网络安全经理[22]认为云提供商应负责保护自己公司的数据安全，这部分员工的岗位职责涉及信息管理。其他部门的员工经常进行影子IT操作，为黑客大开后门，从而为公司带来巨大的安全风险。与其将员工为便于合作和提高工作效率而常用的应用程序禁用掉，不如与IT员工们协力，将这些应用程序安全地集成到正式流程中。
- 卸下更多重担：除了负责云基础设施安全，还有许多云提供商会提供其他安全服务，以提供更多的保护。所以，您应寻找提供数据监控、管理和恢复服务的合作伙伴，请他们分担您的部分企业安全责任。

为什么数据保护必须要习惯逆耳忠言？

最优秀的IT安全团队不会缩在幕后，默默无闻：他们总是在争论。

如果您的安全团队没有报过忧，那不是因为您没有面临威胁，而是很可能因为他们还没找到漏洞。

谈及安全，没有消息可不是好消息。

您的安全小组不能仅仅维持现状，或通过“勾选几个选项”来确保您通过审核。

合规不等于安全。

使网络规划常用安全控制目录保持一致，其动机通常是希望获得并持有行业特定的合规认证。对托付信赖的企业而言，认证是已获得目标认证的企业获取信赖的关键，可以表明公司的信息安全/网络规划已经制定完成，并测试有效。

请第三方审核组织参与可能耗资昂贵，如普华永道、安永会计师事务所，以及德勤，但这样可以证明公司为了获取合规认证所做出的承诺。这些第三方的作用是实施针对公司网络安全计划的详细审查，希望获得各种认证验收。

“务必记住，近年来披露的许多（即使不是大多数）数据泄露事件都发生在合规企业。这表示PCI合规性（举例而言）已经无法防止大批零售商、金融服务机构和网络托管提供商遭到数据泄露。”

Security Week[23]

这些第三方审核机构能否真正地洞察到必要时公司落实网络规划、执行事件响应的能力?

不同于政府实施的程序，第三方组织用来执行审计的方法会产生截然不同的结果。如果审核员只会从各种控制系列内部对待审材料进行部分抽样，就可能检测不到安全控制中的漏洞，这些漏洞会被大量冗长的政策和程序演示所掩盖。

这种审核的风险在于，审核员只是验证了公司政策和程序中存在被规定为标准的内容。

这当然不是对公司自保有效性的真正测试。

即使审核员勾选了合规性矩阵中的所有必选项，也不能确保公司的安全。

如今，合规性达标已成为让公司高管们高枕无忧的实践操作。

必须在合规性与安全性之间求取平衡。

追求合规性本身值得推崇。但是，如果您的安全团队只注重合规性，那么您的企业将面临更大的风险。侧重于合规性的法规要求是静止不变的，而如今的安全模型则通常是动态变化的。技术和网络犯罪的变化速度难以捉摸，使如今的法规很难推行最佳安全实践。

因此，公司必须放弃省事省力、逐项稽核、满足合规要求的方法，而应改换为目标驱动的思维方式，侧重于保护客户数据，而非循规蹈矩地填写合规表格。因此，公司必须采取综合的IT安全措施，保护全部信息和资产，包括移动设备和用户。

需要注意的一个关键方面是每个系统或设备的风险承受能力，因为它们需要不同水平的保护。比如，前台的笔记本电脑没打补丁的严重性，比不上您的ERP系统没打补丁的严重性。您的团队应当审核每个系统的重要性，然后决定落实哪些安全措施。

此外，您的团队还必须提出积极措施来保护数据，即使这些建议会引发争论。最成功的IT安全团队会展开具有挑战性的对话，从而引发利益相关者之间的分歧。

为了准确掌握自己面临的安全风险，您必须习惯这些逆耳忠言。

例如，许多经理都认为补丁措施具有破坏性，不愿意花时间去执行。您的安全团队必须向经理们解释为什么打补丁非常重要，并阐明如果不更新公司设备则会面临哪些风险。

- **如果黑客侵入了您的智能手机或平板电脑，会产生哪些后果？**
- **他们可能会窃取并公布哪些信息？**
- **这会让您公司的财务状况或商誉蒙受怎样的风险？**

您的安全团队在更新系统补丁的时候，会在短期内让您公司的领导们倍感不适，因为比起眼前的短暂分歧，商业效益更加重要。

一旦发现威胁，您的安全团队必须控制由此产生的任何分歧，并针对保护数据安全的措施提出建议。解决分歧的讨论不可能总是一帆风顺，但这个过程对安全策略的成功是至关重要的。

如何让IT安全获得认可

许多企业领导都没有充分意识到IT安全对公司的运营和盈亏底线有多大的影响。为了让您的安全措施获得认可，必须说明这些措施对财务的影响。

领导团队通常会有一种虚假的安全感。他们认为：“我们不会遭到攻击”，或者“只有最资深的黑客才能攻破我们的防御”。

然而，将近80%的IT决策者表示，他们在过去12个月中至少遭遇过一次安全事件，而且严重到了事后必须召开全体公司大会或董事会会议的程度。[24]

众多此类攻击都源于基本的安全漏洞，利用这些漏洞，网络罪犯可以轻而易举地发起攻击。例如，欠缺技术的黑客可能会找到某人的登录信息，或购买被窃取的凭证。一旦掌握了这些信息，黑客就可以从您的网络中窃取数据。

仅仅在Gartner象限右上角拥有一个安全产品，并不表示您是安全无虞的。这只是一种虚假的安全感。

您应确保工具随时处于有效状态，并且掌握最新的最佳实践。您肯定不愿意事后遗憾地说：“我不知道这个安全工具一直在后台运行。”

请不要一设置完安全工具就抛之脑后，否则后果不堪设想。

企业组织无不在面临着风险，所以要趁攻击还没发生就召开董事会会议，针对IT安全展开对话，而不是坐等黑客来攻击，这一点至关重要。董事会必须充分了解您面临的风险，以及可以采取哪些措施来避免数据泄露。

如何培养IT安全文化

下面三种方法可以帮助您营造IT安全文化，首先是在会议室中：

1 以确凿的数据说明后果

很多领导团队认为，网络安全是首席信息官(CIO)或首席信息安全官(CISO)负责处理的工作。

只有36%的IT领导表示，其他高管将网络安全视为战略重点，因而影响了他们在技术和人员方面的投资。[26]

然而，承担风险的是整个公司，一旦发生数据泄露，整个公司都将承担后果。例如，一旦客户数据遭到入侵，公司就会失去客户的信任，进而影响整个公司，不只是影响IT。

因此，网络安全属于业务经营范畴，而不仅仅是一个技术问题。

如果想让您的安全措施获得认可，必须明确解释它对业务的影响。向董事会说明在忽视安全的情况下将对盈亏底线产生怎样的影响。如果您先前曾追踪过任何攻击，就可以探讨这些攻击源自何处，影响了哪些业务领域，以及带来了何种损失。

除了列明诉讼费和技术减灾等确凿的费用之外，切记要讨论品牌受损和其他无形资产的损失成本。

董事会可能还不清楚数据泄露的发生频率、范围，以及造成的财务影响。
向董事会说明真实的数字，就可以促使他们对您的安全措施加大投入。

68%的IT领导表示，他们的董事会并不清楚自家企业为了防止网络攻击，或减轻网络攻击的后果而采取了哪些措施。

波耐蒙研究所[25]

2 建立风险概况

过去，公司董事会依靠管理层去降低风险。2008年金融危机爆发之后，董事会增强了坚守公司盈亏底线的责任心。

IT安全风险概况可以让领导团队信息更灵通，更有责任心。在制定风险概况时，应务必阐明以下方面：

- **IT基础设施，包括硬件、软件、移动设备和物联网设备**
- **ERP系统风险，比如意外停机期间导致生产力和财务损失**
- **与可能暴露敏感数据的合作伙伴、供应商和客户的联系**
- **可能导致巨额罚金的隐私风险和潜在违规行为**
- **人员在与系统互动时的行为和意识**
- **非常繁多的风险定义**

查看上述每一项，根据行业最佳实践和数据给出一个安全评分。

然后，进行优先级排序，这样，您就能了解哪些项需要先行处理了。

通过可视化的方式，比如控制面板，向董事会展示这些信息。这样，他人可以直观看到您面临的风险，并迅速评估最易受攻击的环节。

然后，当您采取了措施改善安全态势时，就可以用控制面板至少面对面地向董事会呈现季度环比变化，而且在全面推出您的安全计划之初，应每月与董事会进行一次沟通。

3 根据董事会意见推出计划

大多数企业领导对最新的安全技术和最佳实践并不感兴趣。如果您的展示侧重于IT安全的技术方面，领导层可能不会予以关注。

相反，他们想了解：

- **目前存在哪些安全问题**
- **这些问题会对公司的财务状况产生怎样的影响**
- **需要采取哪类措施来尽可能降低这些问题招致的风险**
- **解决问题所耗费的相关成本**

阐明上述问题，您的领导团队就能掌握所需信息，做出明智决策。信息分享之后，董事会就可以决定是接受当前的安全风险，还是采取措施减轻风险。

> “网络安全没有‘一步到位’的解决方案，也没有所谓药到病除的‘良方’。网络的安全计划需要持续的关注和投入，它需要的是持续改善，这一点非常重要，必须向董事会阐明。”
>
> Zaki Abbas
> VP and CISO at Brookfield Asset Management[27]

将安全对话持续下去

您的安全计划获得了认可，但IT安全对话并未止步于此。应当定期让领导层了解关于新风险、问题和法规的最新情况。要让董事会知悉您的努力对公司和盈亏底线产生了怎样的作用。

即使是正确的措施，只是纸上谈兵但不付诸行动也是远远不够的。

企业领导始终会追求投资回报，其中不仅包括工具，也包括最佳实践。

综合IT安全策略的关键层面

综合的安全策略需要分为多个层面，每个层面都能起到消除风险，减缓潜在攻击发展的作用。

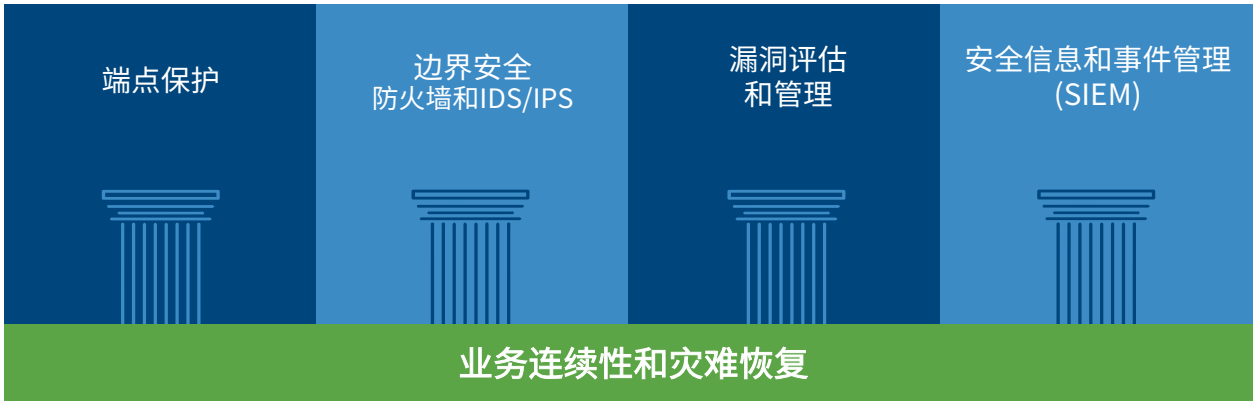
试想，您的安全策略就好比一个漏勺。如果把水倒进漏勺，水会全部漏掉。

然而，如果把几把漏勺叠放在一起，就能堵住漏勺的漏洞。最后，漏勺底部只能漏出几滴水。
尽管无法确保100%的安全，但可以堵住大部分安全漏洞，由此提升防护性。

摸清黑客的思路——从外部攻入。

一旦通过了用户端点，您就进入了网络。然后进入系统，最终进入应用程序。一个综合的安全策略包括以下几个层面：

最低限度的网络安全态势四大支柱



端点保护

公司的恶意软件月平均感染率为1%到3%。但根据IDG的一项调查，有26%的受访者表示该感染率高于3%。[28]

企业通常投资刚性技术，无法保护企业不受最新威胁的攻击。例如，有许多企业认为IDPS会拦截恶意内容，但防火墙和IDPS只能保护网络边界的安全。

要阻止威胁，就必须在端点进行阻断。应寻找一种端点保护解决方案，实时拦截每个网络区域的威胁，包括ERP基础架构、域名系统(DNS)层级和移动设备。

下面再介绍五种保护端点不受攻击的方法：

1 投入基于行为的分析

传统反病毒解决方案是基于签名确定的，并且仅针对已知威胁提供保护。因此，这些方案只能检测到一小部分网络安全风险。

具有智能沙盒功能的安全解决方案可提供更高级别的保护。它们会基于行为指标，对文件进行静态和动态分析。

这些方案会询问，“哪些是用户、设备和系统的典型行为类型？哪些构成了偏差行为？”凭借这些解决方案，各家公司均表示已经筛除了500个虚假威胁指示，最终仅获得了2、3个真实的威胁指示。

2 实时拦截威胁

包含大数据分析和机器学习的安全解决方案可以帮助您在有害软件感染您的系统之前检测到这些软件。这些技术会基于先前的分析来确定某异常行为是否代表威胁，不需要安全专家事先定义复杂周密的规则。

3 对员工开展如何发现威胁的培训并验证员工的警觉性

据思科公司表示，有77%的数据泄露都始于恶意电子邮件。[29]为了防止员工打开这些电子邮件，下载病毒，您必须提高员工对现有威胁的认识。训练有素的员工也能在察觉到危险的时候立即发出警告，这样，您就能迅速响应，控制风险。除了培训之外，也应该对员工开展测试，确保他们的确在关注威胁，而且每天都在这样做。

4 为移动设备打补丁

有很多设备，尤其是安卓设备，在发布时运行的都是已经问世一年的操作系统。同时，这些设备很少打补丁，因此极易成为黑客攻击的目标。

根据赛门铁克的一项研究，美国五大运营商中有71%的安卓用户运行的是至少已经发布了两个月的安全补丁。[30]

而且，据谷歌透露，正在使用的安卓设备中有一半在去年没有收到平台的安全更新。31很少采用开箱即用系统进行保护，您必须找到其他方法来保护您企业的移动设备。

下面介绍可以保护移动设备安全的五个步骤：

- **禁止使用无法打补丁的移动设备。**

  这项举措可能会遭到反对，因为员工往往对移动设备的品牌抱有强烈的个人喜好。但是您不能放任不打补丁和不受控制的设备进入网络。您可以制定公司政策，要求员工在工作中使用安全的设备。

- **强制性打补丁。**

  移动设备管理平台应当允许您针对不打手机补丁的员工制定惩罚措施。例如，如果员工不安装最新的补丁程序，您就可以在他们的不安全设备上锁定他们的电子邮件帐户。

- **使用入侵检测系统来识别已泄露的设备，获取针对潜在威胁的警报。**

  每天扫描网络，查找易受攻击的设备。

- **定期盘点，查看是否有员工在使用违规设备。**

  这样，您就能在黑客利用员工的不安全移动设备侵入您的网络之前主动出击，解决问题。您还可以监控危险行为，比如有员工试图在手机上安装未经授权的应用程序。

- **强制执行命令。**

  确保补丁程序即将执行，使用VPN来验证最低的安全级别（比如Windows防火墙已启用），同时运行通过审核的最新操作系统安全补丁程序。已安装并启用所需的安全端点解决方案。

5 与提供安全管理服务提供商(MSSP)合作

根据IDG的一项研究，将反恶意软件和端点保护工作外包出去的公司都有较低的恶意软件感染率。[32]在启用了MSSP的公司中，有81%报告称感染率为3%或更低，相比之下，启用了协调响应团队的公司中有69%，使用了分布式事件响应团队的公司中有65%，以及启用了网络事件响应团队(CIRT)的公司中有63%具有这一感染率。

此外，仅19%启用MSP的公司的感染率高于3%，相比之下，启用了协调响应团队的公司中有32%，启用了分布式事件响应团队的公司中有35%，以及启用了CIRT的公司中有30%的感染率高于3%。

凭借与MSSP的合作，您还可以更快实施端点保护，最大限度地缩减招募、雇佣和培训合格安全人员的需求。

防范网络钓鱼

许多网络攻击的突破口都是网络钓鱼或社会工程。

CSO杂志[33]表示，已报道的安全事件中有80%以上都是网络钓鱼。

例如，员工会点击电子邮件中的网络钓鱼链接，或打开恶意附件。

教会员工如何发现并避开陷阱，可以避免遭受很多攻击。

信泰宜合会给员工发送自制的钓鱼邮件，看看谁会上钩。如果有人点击了这些电子邮件中的某个链接，就会收到一个自动通知，要求他们参加数据安全课程。我们还要求员工参加一年一度的进修课程，让他们对IT安全随时保持高度警惕。

> 已报道的安全事件中有80%以上都是网络钓鱼。
>
> CSO 杂志[33]

黑客是怎样侵入网络的

网络罪犯的侵入水平已超过了通过电子邮件窃取凭据的水平。他们现在会通过多种渠道将数据列为窃取目标，其中包括利用不安全的应用程序。下面介绍几种黑客用来侵入网络的技术：

鱼叉式网络钓鱼

这是最常见的网络钓鱼类型，在企业网络遭受的所有攻击中占比达95%。34在鱼叉式网络钓鱼攻击中，黑客会收集与目标相关的个人信息，以提高成功几率。比如，他们可能会发出一封看似来自商业合作伙伴的电子邮件。

网络捕鲸

网络罪犯利用这种技术来尾随高管（大鲸鱼）。网络捕鲸邮件通常会显得来源可信，并且包含个性化信息，诱使高管点击恶意链接。

克隆网络钓鱼

在这类攻击中，网络罪犯会克隆合法的电子邮件，并将链接或附件替换为恶意链接或附件。克隆的电子邮件很难甄别，而且传播速度快，黑客会借机接近您公司的多名员工。

商务电子邮件入侵(BEC)

网络罪犯展开BEC攻击时，会先侵入首席执行官或其他高管的电子邮件账户，然后从此人的账户发送欺诈邮件。这些电子邮件可能是要求财会人员支付紧急款项。由于这些消息从表面上看来自高层领导，员工更有可能遵照要求行事。美国联邦调查局报告称，BEC骗局在过去三年间已导致美国多家企业组织损失近16亿美元。[35]

电话钓鱼（语音钓鱼）

网络罪犯会致电受害者，要求他们拨打某个特定的号码，这个号码通常是受害者的银行电话。一旦受害者拨通，网络罪犯就会试图获取受害者的账户信息。

短信钓鱼（SMS钓鱼）

黑客企图利用短信链接窃取公司信息。

许多企业仍在依赖防病毒软件来抵御网络钓鱼的攻击。然而，这些工具只能解决已知的攻击。每个月都会新增近150万个网络钓鱼网站，所以您的防病毒软件可能无法发现新的未知攻击。除了采用防病毒保护外，请务必采用下一代网络钓鱼防御工具。这些工具包括：

- **基于信誉执行的过滤，**拦截可疑的统一资源定位符(URL)
- **端点检测**和响应软件，可验证访问您机器的所有文件和电子邮件
- **入侵检测系统，**用于监控网络中的威胁
- **入侵防护，**防止端点接触到网络钓鱼网站
- **域名系统(DNS)**保护，可防止网络钓鱼电子邮件和释放器病毒破坏服务器内部，进而在开始攻击之前将其拦截
- **发件人代理框架(SPF)**验证收到的电子邮件是否来自已授权主机，让恶意内容无法进入收件箱。

入侵检测预防系统(IDPS)

入侵检测预防系统(IDPS)包括安装在服务器或防火墙上的硬件设备和软件的组合。这些系统会监控您的网络，搜寻可能有攻击迹象的异常活动模式。

同时，预防系统会自动拦截潜在的威胁。IDPS可以根据恶意互联网协议(IP)地址的内容来拦截流量，并就本次操作向您发出警报。例如，IDPS允许有HTTPS流量，但会查看HTTPS请求中是否嵌入了SQL注入式攻击。IDPS不仅能最大限度地降低数据泄露风险，还便于您更深入地了解您的系统。

但是安装了IDPS技术并不意味着就此安全无虞。公司往往会在IDPS上投资数百万，但几个月甚至几年后却发现它不起作用。

下面的10个问题可以帮助您明确IDPS目前是否功能正常：

1 您多久查看一次IDPS?

IDPS不是安装完就万事大吉的系统，它需要每天检查，不断调整，才能确保对系统执行监控。如果您无法执行这些劳动密集型活动，就等于是在对保护您的企业毫无用处的系统上浪费金钱。

您最后一次查看IDPS是什么时候？为了证实它正在发挥保护企业的作用，您多久进行一次IDPS测试?

2 在过去30天里，发生了多少起入侵事件?

检查您的IDPS，查看它在上一个季度里为您的网络击退了多少此攻击事件。如果您有300名以上的员工，则每个季度至少应当发现一次攻击事件。

如果没发现任何事件，那么可能是配置错误。

3 您的IDPS多久更新一次？它是怎样定义的?

您的IDPS可能会显示为“24小时内最新”。但如果该系统再次采用的是多年前的定义，那么显示的这句内容毫无意义。

请检查您的IDPS，确认它启用的是否为最新定义。

4 您会解密流量进行检查吗?

您可以通过SSL加密来检查流量。防火墙使用SSL加密密钥来解密并查看内容。如果内容被允许，防火墙会打开，将加密的数据包发往目的地。

5 您的许可证正确无误吗?

IDPS许可证非常复杂，并可能误导您认为自己已经向IDPS授予了许可，而事实上则不然。当您购买IDPS时，需要对特定功能授予许可，比如URL过滤、IDPS签名，和DNS签名。

您应检查IDPS，确保许可证正确无误，IDPS系统可以执行检查。

6 您的IDPS的当前系统吞吐量是多少?

监控您的IDPS吞吐量，就可以掌握系统和网络的运行健康状况。追踪这一数字，就能了解到自己最近遭遇的威胁数量是否有所增加。

您的安全团队应该大致了解您IDPS的吞吐量，也应清楚它在上一个季度的趋势走向。

如果吞吐量为零，说明您的IDPS没有发挥作用。

7 您的IDPS策略是否相互抵消?

如果您应用于IDPS设备的策略发生了重叠，则可能会相互抵消。

比如，如果您重新定义了一个预过滤对象，它可能会绕过现有的所有策略。于是，设备将无法运行。

每个策略都应接受测试，确保彼此不重叠，不会妨碍各自的功能性。

8 您的IDPS解决方案是处于Gartner魔力象限的顶端，还是通过了分析师验证?

您应当选择一个通过了分析师验证的顶级IDPS。如果您要在法庭上替您的入侵检测策略辩护，就必须证明您使用的是领先的IDPS解决方案之一，并且已经尽了最大的努力去保护客户数据。

如果您购买了未经验证，或打折出售的技术，就很难为自己辩护了。

9 谁对您的IDPS负责?

很多首席信息官都没有专门设立安全团队，所以他们要求网络管理员或初级工程师自行设置并负责管理IDPS。

但是，如果为您的IDPS进行配置和实施监控的人员是同一个人，您就不会开展对持续的安全与合规至关重要的制衡。依据萨班斯-奥克斯利法案(SOX)审计的一部分规定，公司必须说明网络与安全之间的职责分离。

同时，您的网络管理员可能没收到来自IDPS的警报。因为系统悄无声息，他们可能会认为IDPS的运行一切顺利。

但没有消息可不是好消息。如果没人收到警报，说明您的IDPS没有发挥作用。

10 您是否安排了团队专门负责IDPS?

像IDPS这样复杂的安全技术，需要一个经验丰富和热忱的团队进行管理。如果您的内部员工欠缺IDPS经验，则可能要花费几个月来完成系统配置和策略测试。

但如果和IDPS的专家合作，就可以在大约10小时内配置好系统，并在几周内完成测试，不用等待几个月。您的IDPS合作伙伴还将确保关键系统得到24/7全天候监控，持续不间断的更新，并且一直正常运行。

安全信息事件管理(SIEM)

并非所有的威胁都值得同等对待。

大多数网络安全攻击的形式都是部署恶意软件，比如勒索软件，或者未经授权访问（黑客侵入）数字系统或网络。

网络攻击的意图并非总是相同。

但攻击或威胁的载体却是相同的。威胁载体，也就是被利用来实施攻击的途径或方法。

威胁载体有两种常见类型：

A

A类威胁载体

- 社会工程攻击
- 漏洞利用
- 拒绝服务(DOS)
- 分布式拒绝服务(DDOS)

B

B类威胁载体

- 网络（固定线路） 无线
- 便携式媒体/移动设备(PMMD)
- 供应链
- 物理访问

Type A

A类威胁载体代表攻击方法，比如向传输控制协议(TCP)或互联网协议(IP)网络发送大量请求，导致系统无响应，这就是DOS攻击。此列表中并未列出窃取访问凭证的网络钓鱼以及勒索软件攻击等方法。

Type B

B类威胁载体代表攻击者用来传递有效载荷、获取系统访问权限、加密信息，或使数据不可用的途径。无论是方法还是途径，攻击的表现基本相同。

用SIEM对威胁进行优先排序

SIEM可对应用程序和网络硬件所生成的安全警报进行实时分析。它将该数据存储在单一的中心位置，方便您识别威胁，并分析威胁严重性。
这样，您就可以对每天出现的威胁进行优先排序，并即刻采取措施保护公司免受最严重的威胁。

如果耗时甚久才能确认发生了数据泄露，公司就无法恢复了。

如果在数天内检测不到威胁，公司的破产风险会更高。

"超过40%的企业在经历重大自然灾害后将永远无法东山再起"——Gartner[37]

SIEM系统能够帮助您即刻洞察到威胁，让公司能够迅速恢复。

"因为黑客攻击不再是'会不会出现'的问题，而是'什么时候出现'和'有多频繁'的问题。我相信，只有两种公司：一种是已经遭到黑客攻击的公司，一种是即将遭到黑客攻击的公司。甚至这两种公司也正在合并为一类：已经遭到黑客攻击，并将再次遭到黑客攻击的公司。"

Robert S. Mueller, III
前美国联邦调查局局长

（于2012年1月的RSA网络安全会议上发言）36

SIEM有三种模型可供选择，具体取决于您能向所选模型投入多少内部资源：

- **如果您想购买可以在现场自主管理的SIEM解决方案，那么已部署的SIEM就是最理想的选择。**
- **您可通过共同管理SIEM购买SIEM解决方案，并获得安全管理服务提供商的支持帮助。**
- **即服务SIEM是针对SIEM和运营的全运营支出(OPEX)模型。**

如果您缺乏内部资源，无法管理SIEM部署和执行实时警报监控，那么即服务模型可以提供全天候的安全保护，帮助您满足威胁管控和合规性的要求。

ERP应用安全

您的ERP中存储了业务各个领域的敏感数据，因此是黑客的主要攻击目标。

根据一项ERP网络安全调查，89%的安全专家预测，针对SAP系统的攻击将会增加。[38]SAP被侵入会导致公司平均损失500万美元，但如果考虑到客户和利益相关方会丧失信心，后果可能会更严重。

与安全管理提供商合作，可以帮助您保护公司最敏感的数据。您应寻找可以提供三级安全方案的合作伙伴：

1. 一流的数据中心，实现物理安全
2. 逻辑安全，具有多重身份验证、联合身份和军用级加密功能
3. 数据主权，帮助您全面了解并控制所在网络环境

重要的是，企业组织要采取基于角色的访问方式，确认员工的岗位应该具有何种安全访问权限：该员工可以访问哪些数据，可以执行哪些操作？物理和逻辑安全的思路也一样，因此您可以从安全的角度来确定哪些员工可以访问哪些数据，以及可以执行哪些操作。

由于ERP系统的安全做不到“一步到位”，因此合作伙伴应当连续扫描您的系统，提供漏洞数据，并且针对如何更有效地保护您的企业提出建议。

据89%的安全专家预测，针对SAP系统的攻击将会增加。

ERP网络安全调查[38]

您应寻找可以提供下列安全服务的合作伙伴：

- 端点保护解决方案，实时拦截威胁。该方案应该覆盖您的所有网络领域，从ERP基础设施到域名系统(DNS)层面，再到移动设备。
  - 下一代监控和警报。与安全管理提供商合作，该提供商可以利用您的ERP自定义工具提供24/7全天候主动监控和警报。您的合作伙伴应当监控您系统的各个方面，并针对以下情况发出警报：
  - 数据库，包括日志和备份 数据质量
  - 业务功能表现
  - 最终用户活动，包括可能导致风险的用户行为变化
  - 日志，比如访问控制（物理和逻辑）、造成重新配置的关键活动、对关键或敏感数据的访问，以及未授权/异常的活动
  - 希望进行自定义监控和发送警报的任何区域
- 一个安全平台，可供您对自定义监控进行定义，对ERP环境中出现的新威胁做出响应。

重要的是，在安全漏洞出现时，您必须拥有工具可以查看问题、了解威胁，并建立监控功能，查看哪些系统需要打补丁，以及应当赋予每个系统的优先级。

如果您有能力在平台内确定并抵御亟需修补的漏洞，您的企业组织就能创建解决方案。如果您没有这件工具，就无法知道问题在哪里，也不知道如何通过策略快速予以解决。

心脏出血漏洞(Heartbleed)是一个很典型的例子。

心脏出血漏洞(Heartbleed)是2014年4月被人发现的一个漏洞。攻击者可以利用这个漏洞访问敏感信息，它潜藏在数千个网络服务器上，包括运行雅虎等大型网站的服务器。心脏出血漏洞的产生源于OpenSSL中的一个缺陷，这个缺陷是执行传输层安全(TLS)和安全套接字层(SSL)协议的一个开放源代码库。39黑客可以向某个易受攻击的网络服务器发送敏感信息，其中包括用户名和密码，以此展开欺骗。

公有云中的安全性

企业在将云系统集成到自己的业务环境中时面临着巨大的挑战，特别是在安全和合规性方面。如果您没有采取正确的安全措施，网络就会被侵入。

为了避免被侵入，您必须评估每个云服务的安全性，以及该云服务使用的托管应用程序。然后，必须弥补应用程序与云之间的任何安全漏洞。方法介绍如下：

- **不要以为您的公有云服务具有开箱即用的安全性。**

  您的提供商会指望您来采取措施保护云中的数据。

- **确保公有云中的系统与您的私有云和传统解决方案至少拥有相同等级的安全和合规性。**

  由于公有云位于公共空间，因此，如果您尚未在云中全面落实安全要求，很快就会发现这一点。在云端犯下的错误更加显眼，也会让黑客有更大的利用机会。比如，在内部网络上，配置错误的IP地址无法实现互联网路由。而在公有云上，只需单击两次，就能向公众开放访问，并可以公布报告数据。

- **加强对所有云资产的持续监控和配置验证。**

  数据暴露往往归咎于人为失误。

- **针对公有云帐户的管理访问要加以控制。**

  如果有心怀不轨的人访问了这些账户，他们只要几个小时就能毁掉您的整个企业。或者，他们可能会利用这些账户来布设加密货币，而您的公司要损失数千，甚至数百万美金来为此埋单。

- **每个设备为员工设置了不同的访问权限，而这些设备的登录都要关联身份与访问管理(IAM)服务。**

  然后，为合规性和安全审核创建详细记录，尤其要记录信息访问者的身份以及他们使用信息的方式。

数据保密性

信息隐私和数据保护新法律禁止披露或滥用个人信息。现已有80多个国家和独立地区（包括加拿大和欧洲、拉丁美洲、亚洲和非洲的诸多国家）都采用了综合的数据保护法案。

但值得注意的是，美国没有全国实行的综合信息隐私法，而是制定了限制性的行业法律。比如，根据加州的隐私法案要求，如有企业的用户和/或收入超过特定阈值，就必须披露自己收集的个人数据。

重要的是，要了解您掌握的是哪些人的数据，以及这些信息的存储和共享方式。

信息隐私和数据保护新法律禁止披露或滥用个人信息。现已有80多个国家和独立地区（包括加拿大和欧洲、拉丁美洲、亚洲和非洲的诸多国家）都采用了综合的数据保护法案。

但值得注意的是，美国没有全国实行的综合信息隐私法律，而是制定了限制性的行业法律。比如，根据加州的隐私法案要求，如有企业的用户和/或收入超过特定阈值，就必须披露自己收集的个人数据。

重要的是，要了解您掌握的是哪些人的数据，以及这些信息的存储和共享方式。

务必遵守隐私法，这一点至关重要。

“美国有80%以上的大型企业是完全依赖技术的，或依赖技术的程度很深，一旦遇到系统故障，一家公司平均会在六天后损失掉25%的日收入。”

特拉华大学灾害研究中心报告[40]

敏感数据的处理有一些常识性的方法。

▷ 用便于理解的词句解释术语：敏感、私人或受保护

员工、承包商、供应商和客户必须了解什么是私人数据，这样他们才能在处理数据时具有敏感度，遵守流程，并确信信息受到了保护。有些客户可能对受保护的数据具有专门或独特的定义，因此请务必澄清。

▷ 明确并传达正确的存储和传输方法

通过电子邮件、票务系统附件，以及面向互联网的网站进行传输和存储不应被视为具有安全性。请确保需要进行存储和传输的人员可以使用通过审核的安全存储和传输方法。安排短期培训，或创建如何获取信息的文档，介绍如何访问并使用安全工具。

> “数据泄露涉及隐私和安全。无法保证安全，就无法拥有隐私，因此安全极其重要。如果有人对此持不同意见，他们绝对不正常！”
>
> **Larry Ponemon博士，**
> **波耐蒙研究所**
> **创始人兼主席[41]**

▷ 记录到期日、时间设置，以及删除程序

为受保护数据开发保留流程，当需要销毁数据时，为该流程确定安全的执行方法。

▷ 定期审查其他安全和加密选项，尤其是敏感或私人数据选项

安排定期安全审核，确定可能存在的变动或新功能。应考虑加密选项和其他新方法，进一步保护敏感数据。

漏洞评估和管理

对于企业而言，安全不再是可选可不选的选项。信息安全一度被视作IT中的次优环节，现在却具有高优先级。如果一家公司对安全置之不理，后果可能是毁灭性的，阿什利·麦迪逊(Ashley Madison)、美国国税局、塔吉特公司、索尼、易趣和印象笔记就是鲜活的例子。

这些公司都在数据泄露事件中使数以百万计用户记录遭到入侵，而且它们不是个例。还有很多公司忙于应对Cryptowall或CryptoLocker，这是一种木马病毒，它会对数据进行加密，然后用解密密钥勒索赎金。

常见的误解有哪些?

对任何公司来说，最大的误解就是：漏洞评估和安全无足重轻。他们认为自己不是（或以后也不会成为）攻击目标。但事实是，任何公司都有可能成为目标，无论公司规模大小。

黑客们想要的是数据。您的公司不过是黑客待窃清单上的一项任务，他们只想尽量收集更多信息，再在黑市上卖掉。

这一切与个人无关。对他们而言，这只是生意。另一种误解是：已经完成了渗透测试和审核，所以网络很安全。

每一天，都会有新的威胁发布。它们可能是新的病毒，也可能是曾经攻击过公司的同种病毒的变种。这也表示，去年安全，现在不一定得到保护。渗透测试、漏洞评估和审核是持续性的、定期安排的工作。它不能保证100%的保护。但它可以阻止原本会得逞的攻击。

漏洞评估的第一项益处是识别存在风险的资源。您应该聘请专业人员来识别每一个易受攻击的资源，无论它们看起来有多无害。一旦完成对易受攻击的资源的评估，就可以对每种资源进行优先排序，对资源进行价值评估，并对保护资源需要花费的成本进行评估。

漏洞评估最有价值的部分是对网络的保护策略。应确保您使用的是深度防御策略，可以保护您的资产。漏洞评估有助于识别基础架构当前面临的风险，然后提出通过行业审核的问题补救措施，以减少威胁的覆盖面。

即使防御保护做不到100%有效，也能尽量降低后果的严重性。

安全风险最小化是一项复杂的任务，需要不间断的监控、打补丁和升级。切勿坐视数据遭到入侵，应聘请专业人员对网络进行彻底的漏洞评估。

为了企业组织的安全，设备打补丁是必需的。您可以强制员工安装补丁程序，提高设备的安全性。

您可以强制要求员工为自己的台式电脑和移动手机打补丁。比如，如果员工不给手机打补丁，他们将无法访问自己的电子邮件帐户。

> “60%的数据泄露是由于没打补丁而造成的。如果打好补丁，就能杜绝60%的数据泄露，甚至不需要人工智能或区块链的支持！打补丁就是这么有用。”
>
> **Ricardo Lafosse**
> **晨星首席信息安全官**[42]

您的IT安全策略欠缺哪些层面的措施?

采取综合、多层的措施来实现IT安全，这是保护企业免受威胁的关键。

大部分公司还没认识到风险评估和影响评估的价值，因为这些评估漫长而枯燥，但实则非常值得。

不能仅仅依靠技术来解决安全性挑战。

用对策略和计划，选对合适的人员，您就可以防止网络入侵，保护您的企业安全。

网络安全人才短缺让企业面临风险

尽管威胁持续增多，但许多企业的内部都缺乏用来抵御攻击的技能或资源。

根据黑帽安全大会的一份报告，IT领军企业没有足够的人手或预算来充分抵御前文提到的威胁。[43]

这一发现与其他报告也相吻合。例如，有68%的安全专业人士表示，网络安全技术的短缺正在影响他们掌握漏洞的能力。[44]

这种短缺现象在下列方面影响着各个企业：

- **60% 的企业表示，这种短缺现象损害了其对事件的检测和响应能力。**
- **53% 的企业表示这会导致配置不安全。**
- **42% 的企业表示无法将安全数据转化为情报。**

对没有预算可以支付高薪的中小型企业而言，网络安全技术的短缺影响尤为严重。即使只有一、两个人的小型安全团队，这些企业通常要付出很大的努力去维持其运作。这些团队往往过度工作，压力很大。

其实，黑帽安全大会发现，有40%的安全专业人员都认为自己已经疲惫不堪。与此同时，有54%的安全专业人员认为安全专家的焦虑、抑郁和成瘾程度高于普通美国公民。

如何克服网络安全技能的差距

令人遗憾的是，网络安全技术的短缺只会愈演愈烈。据分析师预测，截至2021年，全球网络安全岗位将出现350万个空缺，高于2014年的100万个空缺岗位。[45]

但即使找到网络安全专家，也不能保证他们一定会留在企业。ESG研究[46]显示，有49%的网络安全专业人员每周至少收到一次岗位挖角。对于想在网络安全领域拼搏发展的人来说，这是个好消息，但对于需要用合理的薪水留住专业人才的首席信息官来说，却十分头痛。

有些方法可以在不雇佣新员工，或不加重内部团队负担的情况下提高安全性。

有许多首席信息官会请安全管理服务提供商(MSSP)来克服企业内部的技能差距。

与MSSP合作既可以增强企业安全，也不会加重内部员工的负担。与合适的合作伙伴携手，就可以快速获得投资回报，同时让您的内部团队全心投入创新工作，而不是疲于日常维护。

事实上，与安全管理服务提供商合作的企业中有81%的感染率为3%或更低。而使用其他安全方法的公司（比如协调响应团队或分布式事件响应团队）中只有63%到65%的公司的事件响应率为3%或更低。

重要的是，要了解您的核心业务是什么，并任用善于充分利用安全管理服务提供商的经验和才能的内部安全专家。

将反恶意软件和端点保护工作外包出去的企业，感染率会低于靠自己处理这些工作的企业。

IDG 调查[47]

在雇佣安全管理服务提供商(MSSP)之前，您应该问的10个关键问题

MSSP可以巩固您的网络安全，同时减轻您内部IT团队的负担。但要实现上述结果，您必须找到合适的合作伙伴。在您选择MSSP之前，需要了解10件事。

选择合适的MSSP是一种必然的趋势。很多家MSSP表面上很雷同，因此很难确定它们是否能满足您的业务和IT需求。

下面的10个问题可以帮助您找到适合您的MSSP：

1 他们是否具备丰富的ERP系统经验吗？

您的ERP存储着公司最敏感的数据，是黑客的主要攻击目标。确保您的MSSP有适合的经验和工具来保护ERP免受威胁。

应选择获得了SAP、Oracle或JDE合作伙伴资质认证的MSSP。MSSP的团队还应该拥有您的ERP提供商的相关技术认证。

而除了技术专长，寻找MSSP时也要看他们是否提供正确的工具。例如，MSSP应该提供专门为您的ERP定制的监控工具，主动监控您的ERP环境，并针对潜在威胁向您发送警报。

2 他们会怎样处理您的数据?

在与MSSP洽谈之前，请先明确您对安全的目标和要求。例如，您是否需要在内部存储任何数据？您的某些数据是否需要不同水平的控制和保护？您是否必须遵守GDRP?

另外，应明确如果MSSP被黑客攻击会怎样。MSSP将做出何种响应？他们会过多久通知您数据泄露？关于MSSP有哪些法律要求?

3 他们提供数据库加密吗?

传统的磁盘和数据库级加密无法指定数据类或特定的用户权限，因此访问控制是一个要么全盘采用，要么全部放弃的问题。

您的MSSP提供的现代加密工具应该支持特定领域加密和用户访问粒度控制。寻找提供以下服务的MSSP：

- **您的ERP和其他数据实现军用级加密**
- **您的ERP支持的各类平台实现列级透明数据加密**
- **具备加密静态和传输中的数据的能力**
- **对哪些人对哪些字段和列拥有解密权限执行细粒度控制**

4 他们能否分享客户的成功案例?

MSSP是否帮助过与您同样的客户？能否讲述一下？确认MSSP是否与具有相似IT环境的业内其他公司或个人进行过合作。此外，询问他们是否帮助首席信息官实现过您希望达成的同样结果。

通过这些案例，您可以了解MSSP解决问题的能力。例如，他们是否只会做最低限度的工作，例如报告数据泄露？还是会采取措施进行处理？寻找以合作伙伴态度对待您的MSSP，而不仅仅是等待解决的又一张故障报告表。

5 MSSP能提供哪些可信的、详细的参考资料?

您可能无法与MSSP的客户交流，因为大多数企业不愿因为探讨自身的安全问题或正在合作的MSSP，而将自己置于风险之中。

但还有其他方法可以确定您的MSSP是否可信。例如，MSSP可以向您出示一流IT供应商的背书。他们还可以出示一份证书清单，证明自己的技能和技术紧跟前沿。

另外，务必要去谷歌用MSSP名称加“泄露(breach)”进行搜索，确认他们的客户是否遭受了网络攻击,或其他形式的数据丢失。谷歌的快捷搜索可以查出新闻中不会播放的内容。毕竟，您不会愿意雇佣了某家MSSP，之后却发现他们曾卷入过一起重大的数据泄露事件。

6 MSSP的数据泄露检测和补救流程是否会分析每张故障报告单?

许多MSSP会设置数据泄露检测和补救流程，从单纯的被动（而非主动）服务开始计费。例如，他们可能使用工具来跟踪趋势，并且只在某一趋势影响到您的环境后才声明问题。

应确保您的MSSP可以自动生成故障报告单，并记录他们所有的工作。这就增加了您的责任并确保您的MSSP基于技术，而非基于经验来声明问题。这样，您的MSSP就不能忽略问题，且不能让其转变成安全事件。

7 MSSP是否使用领先的端点保护技术?

您的MSSP不仅应该提供最新的技术，还应在内部使用最新的技术。如果他们依靠的技术沿袭了三代，又如何为您提供优质的服务呢?

询问您的MSSP，他们会为客户和IT环境使用哪些工具。此外，还要询问他们如何保持采用最新的安全最佳实践。

例如，要对严重依赖反病毒工具的供应商提高警惕，因为这些供应商几乎无力抵御如今复杂的威胁。相反，选择提供高级端点保护的MSSP，就可以防止恶意软件侵入企业的计算机和设备。

除了端点技术，MSSP还应当会灵活运用功能繁多的安全工具包。应确认您的MSSP会使用哪些工具来降低风险，解决威胁。

8 MSSP在您的企业所在地聘有经验丰富的员工吗?

员工办公期间，安全风险会加大。因此应选择一家办公时间相近的MSSP。这样，当企业最易受攻击的时刻，MSSP会立即到岗。

9 MSSP的员工资质合格吗?

IT技能的短缺不仅影响企业，也会影响MSSP。许多供应商很难找到有资质的员工，因此谁有时间工作就雇佣谁，报酬按时计费。

确保您的MSSP为您的帐户指派技术纯熟的技术人员。如果您使用的是SAP或Oracle等技术，就请寻找经过认证的合作伙伴来担任MSSP。这样可以保证您的MSSP拥有熟知如何实施并运行核心系统的员工，让您高枕无忧。

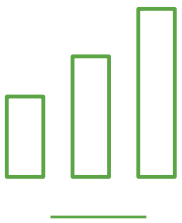
此外，MSSP团队也应该保持其技能的敏锐性。网络安全世界瞬息万变，因此MSSP必须紧跟最新发展趋势。请询问MSSP是如何拓展自身知识的。例如，他们是否会通过参加安全大会来了解最新的威胁和最佳实践?

10 MSSP的产品和服务是标准化的吗?

应寻找一揽子解决方案价格透明的MSSP。当您增加更多服务或IT环境扩展时，他们还应该针对定价的变化方式作出解释。有很多MSSP底价较低，但随着您的环境发展，他们的费用也会迅速攀升。

从您的IT资源中攫取更多价值

缩小网络安全技能的差距并非一朝一夕可以做到。根据网络安全风险投资公司的预测，截至2021年，全球将短缺350万名合格专业人员。[48]



与MSSP合作，可以帮助您保护自身环境的安全，同时解放内部IT团队，使其全心投入更具策略性的项目。
合适的MSSP会帮助您确定安全漏洞，引导您实现风险最小化，从而增强您的内部专业技术。

面对新一代网络威胁，您是否未雨绸缪?

信泰宜合的端点安全解决方案提供针对您公司96%真实风险的防范技术。它通过先进的检测技术(包括用户行为分析)来防止和识别恶意软件、网络钓鱼和黑客工具。

SYNTAX

信泰宜合的安全管理服务可以在几分钟/几小时内部署完毕。 防范数十亿威胁并控制您的环境。 我们的综合安全服务包括:

▷ 端点安全

在端点处阻止高级攻击。信泰宜合可提供24/7/365全天候不间断的安全保护，节省了聘用全职安全专家的高额费用。

▷ ERP 安全

信泰宜合提供了一套完整的SAP、JD Edwards和Oracle EBS迁移、管理和安全服务。我们是SAP全球合作伙伴，拥有45年以上的复杂系统管理经验。

▷ 入侵检测和预防系统 (IDPS)

更加深入地洞察您的网络行为，才能调整安全性。信泰宜合可以帮您将可执行事件与杂务分开，提高运营效率，降低日常开销，从而更有效地区分威胁的轻重缓急，改善安全态势。

▷ 安全信息和事件管理 (SIEM)

对应用程序和网络硬件所生成的安全警报进行实时分析。信泰宜合为您抵御威胁，提高您的法律合规性，并帮助您避免内部部署的SIEM解决方案的资本费用和运营复杂性。

▷ 漏洞管理和分析

信泰宜合的安全评估服务可以识别漏洞，并对您开展预防措施培训，帮助您保护关键系统和数据。评估中将核查您的内部和面向公众的漏洞，并对您的员工进行安全意识培训，以免员工犯下使企业面临风险的错误。

▷ 高可用性和灾难恢复

信泰宜合的高可用性和灾难恢复解决方案可依靠同类型最佳的复制技术，保护您的系统和用户免受意外延迟和停机的影响。更重要的是，我们基于云的解决方案在发生灾难时也能保证业务不间断。我们还提供部分业界最具主动性的恢复点目标(RPO)和恢复时间目标(RTO)功能。

后续行动

想进一步了解如何保护您的公司吗?

关注信泰宜合官方微信（信泰宜合 SYNTAX ASIA)，获得更多咨询。

为何选择信泰宜合?

- 自1972年便开始提供了综合技术解决方案
- 迄今已拥有超过1000位客户
- 全球1200多名IT专家为您坐镇
- SAP全球合作伙伴，管理着6,000多个SAP系统
- 是全球首批SAP客户之一(#7)
- 业内客户满意度排名最高中的一员
- AWS高级咨询合作伙伴
- 多云，多ERP管理经验
- 7*24小时不间断服务与保障
- 先进的管理和监测工具
- Tier IV最高级别数据中心

自1972年以来，信泰宜合一直为各种规模的企业提供综合的技术解决方案，成千上万的客户相信信泰宜合能够满足他们的IT服务和ERP需求。如今，信泰宜合是面向任务关键型企业应用的领先云管理提供商。信泰宜合在安全、灵活、弹性、公共或混合云中实施和管理企业资源规划部署方面具有无可争议的优势。凭借强大的技术和功能咨询服务，以及世界一流的监控和自动化，信泰宜合为不同行业和市场的公司提供服务。信泰宜合在世界各地都有办事处，并与SAP、AWS、AZURE，IBM、HPE、思科和其他全球技术领先公司合作。 如需了解信泰宜合的更多信息，请访问www.syntax.com。

参考文献

1. 波耐蒙研究所：2019年数据泄露成本损失研究（2019年）
2. 维基百科：GDPR罚金与通知
3. 火眼公司：大部分企业组织计划于2020年增加网络安全预算（2019年11月6日）
4. 飞塔公司：运营技术和网络安全报告的状态（2019年）
5. 操作技术网络安全联盟(OTCSA)
6. Infoblox: Infoblox经研究发现，个人和物联网设备在企业网络中的爆炸式增长带来了巨大的安全风险（2018年5月14日）
7. 802 Secure: 802 Secure802 Secure在2018年圣克拉拉世界物联网大会上分享了物联网威胁研究（2018年5月16日）
8. 圣达菲集团：第三方物联网风险：公司不知道他们不清楚的内容（2019年5月3日）
9. 弗雷斯特：北美企业物联网安全状况（2019年）
10. Malwarebytes实验室：网络犯罪的策略和技术（2019年恶意软件现状）
11. 迈克菲：迈克菲实验室2020年威胁预测报告（2019年12月4日）
12. Coveware：Ryuk、Sodinokibi继续肆虐，第四季度的勒索软件损失翻番（2020年1月22日）
13. SANS分析师计划：端点保护和响应，SANS调查（2018年6月）：
14. 美国商业资讯网：根据独立市场调查显示，在过去24个月内，64%的ERP部署遭到入侵（2019年10月2日）
15. 数据丢失会有什么样的后果？ 作者：Mark Campbell https://www.unitrends.com/blog/what-are-the-consequences-of-data-loss
16. 埃森哲咨询公司：从铅坠到发射台：实现数字目标的同时，兼顾传统体系的优化（2016年）
17. CPO杂志：2019年SANS研究所云安全调查揭露最大威胁，竟然不是DDoS攻击（2019年5月28日）
18. Cybersecurity Insiders: 2019年云安全报告（2019年）
19. 《华尔街日报》，Equifax数据泄露事件以7亿美金达成和解 https://www.wsj.com/articles/equifax-reaches-700-million- settlement-over-data-breach-11563798429
20. McAfee RP Enterprise超新星数据分布 https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-enterprise- supernova-data-dispersion.pdf
21. McAfee RP Enterprise 超新星数据分布 https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-enterprise- supernova-data-dispersion.pdf
22. McAfee RP Enterprise 超新星数据分布 https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-enterprise- supernova-data-dispersion.pdf
23. Security Week网: 合规不等于安全（2018年5月21日）
24. Iron网：新调查发现，绝大多数IT安全支持者都愿意共同应对互联网上的威胁，提升全网的集体防御能力（2019年5月15日）
25. 波耐蒙研究所：2018年网络安全全球大趋势研究（2018年）
26. 波耐蒙研究所：2018年网络安全全球大趋势研究（2018年）
27. 2020年网络安全20大语录https://www.secureworldexpo.com/industry-news/20-top-cybersecurity-quotes-for-2020
28. IDG: 为什么要在端点拦截安全漏洞？如何拦截？
29. 思科：以弱胜强——面对当今的威胁，中小企业如何加强防御（2018年）
30. 赛门铁克：移动威胁情报报告——回顾2016年（2017年3月23日）
31. 谷歌：多样化的生态系统需要多样化的保护：回顾2016年安卓安全工作（2017年3月22日）
32. IDG: 为什么要在端点拦截安全漏洞？如何拦截？https://info.syntax.com/whitepapers/2/block-security-breaches-at-the- endpoint
33. CPO杂志: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
34. IDG: 如何击退鱼叉式网络钓鱼
35. FBI: 商业电邮泄露，电邮账户泄露，一场50亿美元的骗局（2017年5月4日）
36. 贵公司的网络安全健康有多安全？https://www.withum.com/resources/secure-firms-cyber-health/
37. 对企业持续管理进行压力测试，2020年2月12日，投稿人： Jordan Bryan https://www.gartner.com/smarterwithgartner/ stress-test-your-business-continuity-management/
38. ERPScan.com: ERP网络安全调查（2017年）
39. 心脏出血漏洞是什么？它是如何发起攻击的？应该如何修复？ CSO杂志， https://www.csoonline.com/article/3223203/what-is- the-heartbleed-bug-how-does-it-work-and-how-was-it-fixed.html
40. 特拉华大学灾害研究中心，第256号设计概述《未来灾害趋势：对各项计划和政策的影响》，E. L. Quarantelli著（1997年），http://udspace.udel.edu/bitstream/handle/19716/199/PP256-%20Future%20Disaster%20Trends.pdf;jsessionid=2954239C39CE0C82B82698E4D50C5E12?sequence=1
41. 2020年网络安全20大语录https://www.secureworldexpo.com/industry-news/20-top-cybersecurity-quotes-for-2020
42. 2020年网络安全20大语录 https://www.secureworldexpo.com/industry-news/20-top-cybersecurity-quotes-for-2020
43. 美国黑帽安全大会：美国黑帽安全大会新研究：您的私人信息，罪犯们唾手可得；美国大选，关键基础设施也处于风险之中（2019年7月1日）
44. Tripwire: 2019年网络安全技能差距调查
45. 纽约时报：网络安全团队招募狂潮（2018年11月7日）
46. ESG: 网络安全专家们的生活和时代（2017年）
47. 在端点拦截安全漏洞白皮书 https://info.syntax.com/whitepapers/2/block-security-breaches-at-the-endpoint
48. Cybersecurity Ventures: 网络安全人才遭遇短缺，2021年全球将有350万个空缺职位（2019年10月24日）