安讯士公司“网络安全”期刊

合作伙伴皆受保护

来自网络安全领域的
见解与启发

进入 >

AXIS COMMUNICATIONS

引言

稳健的保护框架

正如您可能知道的那样，面对网络安全方面的挑战，没有固定的单一解决方案，也没有产品能够拥有坚不可摧的网络安全。相反，网络安全是值得信赖的合作伙伴关系，其中的各个相关方——从子供应商到制造商、从安装商到集成商、再到最终用户，各自都扮演着重要的角色。它还是持续的过程，而不是一劳永逸。

作为负责任的网络安全合作伙伴，我们在这里为您提供一系列有用的文章、窍门和启发。我们认为，它们可能对您紧随先进技术的发展步伐以及实现自我保护是有帮助的，我们也希望您觉得它们的确有用。

但在转到下一页前，我们还要花点时间来简要介绍一下美国国家标准与技术研究院 (NIST) 的风险管理框架。由于网络安全在本质上是风险管理，所以先利用风险管理框架，在概率和潜在危害等级方面，评估您企业或机构的潜在风险，当然，这涉及许多风险。

安讯士的网络安全策略便是依据NIST框架制定的。NIST准则在全球有着广泛的使用，不仅适用于大型企业和机构，还适用于中小型企业和机构。即使您的企业使用其他框架，也有可能与NIST框架兼容。

NIST框架主要围绕五个方面：识别、保护、检测、响应和恢复。若想详细了解每个方面、安讯士作为网络安全合作伙伴的角色、以及您自己的角色，请访问安讯士网站 www.axis.com/cybersecurity。

同时，希望您喜欢本期刊！

目录

1 常见网络威胁
2 确保健康网络的 10 大窍门
3 生命周期管理
4 零信任网络
5 AI 与网络
6 协作
7 值得信赖的相关方
8 合规
9 安全供应链
10 为什么选择安讯士？

网络安全能够从物理安全中学到什么

对于大多数人而言，物理安全风险是较容易理解的。如果不锁门，外人擅入的风险就会增大。目光所及之处，贵重物品可能被洗劫一空。错误和事故可能危害人员、财产和物品的安全。

物理安全和网络安全在处理方式上大致相同。无论您是负责企业的物理安全还是网络安全，都需要应用相同的原理：

- 识别并分类资产和资源（要保护什么）
- 识别潜在威胁（要防范什么）
- 识别可能被威胁所利用的潜在漏洞（可能性）
- 识别因破坏所致的预期成本（后果）

风险通常被定义为威胁概率乘以危害性结果。一旦确定了风险，就必须问问自己，要怎样预防负面影响。

关注您的资产和资源

在连接了视频系统的情况下，需要保护的资源明显是来自摄像机的视频。资产是视频管理系统 (VMS) 中的视频录像。相关访问通常根据用户权限来进行管控。其他要考虑的资产有，用户帐户和密码、配置、操作系统、固件和软件、以及联网设备。

阅读更多 >

应提防哪些威胁?

针对网络威胁的自我保护的第一步是，知道自己面对哪些威胁。保密性、完整性和可用性被视为IT系统保护的关键要素。对这其中任一者有负面影响的因素都被视为网络安全事件。那么，我们来看看常见的网络安全威胁及其可利用的漏洞。

阅读更多 >

1 非刻意的人为操作和错误

无论所采用的网络保护技术有多先进，只要有一个人单击了电子邮件中的恶意链接，攻击者便能够侵入。因此，对于网络罪犯来说，这是简单（因此也是较偏好）的攻击方式。为网络攻击打开大门的人为错误的类型包括：

- **社交工程：**通过心理操纵，诱骗用户发生安全错误或者泄露敏感信息。网络钓鱼和恐吓软件便是社交工程的例子
- **密码误用：**其中包括所使用的密码强度不够、或者未适当执行密码保护和/或更新。
- **关键组件的管理不当：**丢失或错放了某个东西，导致系统能够被非法访问。门禁卡、电话、笔记本电脑和文档就是其中一些例子。
- **系统管理不当：**未安装系统更新和安全补丁。
- **不成功的改善：**有人尝试修复某个东西，导致系统性能降低。

漏洞和人为错误

因人为错误所致的某些常见的漏洞是，缺乏网络意识，以及缺乏用于风险管理的策略和长期过程。如要降低因人为错误所致的威胁，必须对企业中的所有人开展网络安全实践教育。您还应限制视频访问权限，通过 VMS 将重要的权限仅授予少数可信任的人员。

阅读更多 >

系统的故意误用

2

另一种非常常见的网络威胁是，具有合法访问权限的人员故意误用视频系统。故意误用的类型包括：

- 未授权访问和操作系统服务及资源
- 窃取数据
- 故意危害系统。

漏洞与故意误用

重要的是，执行合理的政策和长期流程，以帮助管理漏洞并减轻系统故意误用导致的威胁。为相关人员恰当地授予敏感信息访问权限就跟限制此类权限的授权人数一样重要。应针对管理和日常操作客户端 (VMS)，在设备上分别创建帐户，且设备应使用临时帐户来执行维护和故障排查。如果这三种帐户都是相同的帐户，密码就可能被企业内部的其他人发现，为故意或意外误用创造机会。

阅读更多 >

3

物理篡改或破坏

从网络安全角度讲，IT系统的物理保护是非常重要的：

- 在物理上暴露的设备可能遭到篡改。
- 在物理上暴露的设备可能被偷盗。
- 在物理上暴露的电缆可能被非法断开、转接或切断。

漏洞与物理威胁

摄像机自身不仅容易遭到篡改，而且它们的网络电缆也暴露在外。这就可能为网络入侵创造机会。可被利用且可能为威胁创造机会的其他常见漏洞包括网络设备，诸如未安置在锁闭区域内的服务器和交换机、可轻松触及且未配备防护罩的摄像机、未受墙体或导管保护的电缆。

注意负面影响

视频系统不处理财务事务，也不保留客户数据。这就意味着，对视频系统的攻击可能难以挣钱，因此对有组织的网络罪犯而言，攻击价值较低。但缺乏抵抗力的系统可能对其他系统构成威胁。因此，所招致的开支难以估算。遗憾的是，在许多情况下，企业都是吃过苦头了才明白。保护就跟质量一样，付出与收获成正比。如果购买廉价品，就长期而言，最终所需的开支可能要多得多。

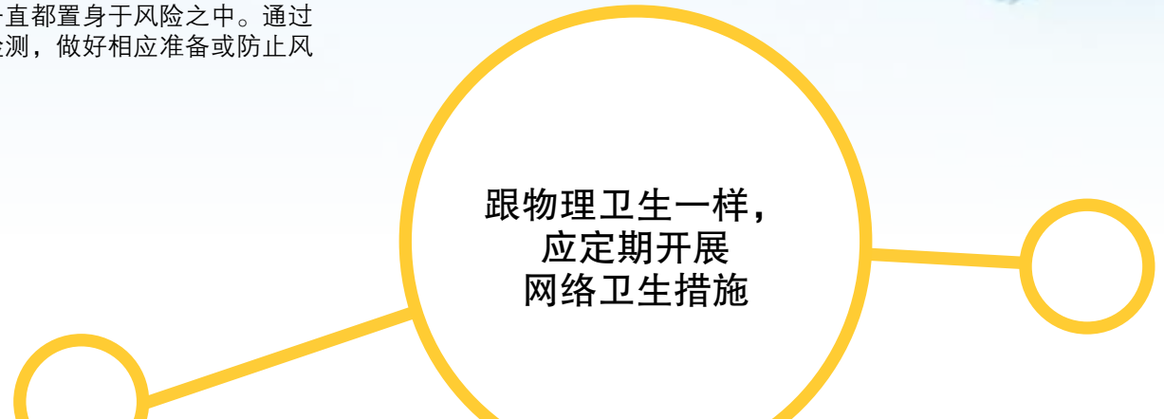
保持良好的网络卫生

良好的网络卫生是指，系统和设备用户为保持系统健康、提升网络安全性而采取的措施。良好的网络卫生通常是总体内部流程的组成部分，它有助于确保身份信息以及可能遭到窃取或破坏的其他信息的安全性。跟物理卫生一样，网络卫生也应定期执行，以便帮助消除自然衰退和常见威胁。

良好网络卫生所带来的收益

为您的设备和软件实施日常网络卫生程序有益于开展维护和保障安全。

- 维护能够确保设备和软件以其尽可能高的效率运行。分段的文件和过时的程序会增大漏洞风险。维护程序有助于提早发现这些问题，并能够预防严重问题的发生。获得良好维护的系统不太容易遭受网络安全风险的侵害。
- 从黑客到身份信息盗窃者、到病毒和智能恶意软件，企业一直都置身于风险之中。通过预测威胁，实施良好的网络卫生措施，就能够有助于提早检测，做好相应准备或防止风险实际发生。



阅读更多 >

使用保密性强大的唯一性密码

这可能听起来理所当然，但网络罪犯非法访问系统的常用方式便是利用弱密码。大多数基于 IP 的设备随附有默认密码和设置。因此，必须根据 IT 或公司策略，立即更改这些密码和设置。企业需要使用保密性强大的唯一性密码（至少包含 8 个字符）来确保良好的密码管理，这些密码应定期更改，切勿在不同站点之间共享密码。计算机系统无法强制实施密码策略。企业必须确保员工接受相关培训并理解企业在密码方面的做法。同时还建议使用证书来加密密码和用户名。

如果密码只是一个常用字或名字，那么无论其长度如何，都可能在数秒内被破解。

根据 IT 或安全网络策略部署和安装设备

部署设备时，切勿让未使用的服务保持在启用状态。这会导致网络罪犯能够轻松攻击和安装恶意应用。禁用未使用的服务，仅安装可信的应用，能够减少潜在攻击者利用系统漏洞的机会。设备也同样必须遵守正确的物理安装规程，网络端口和 SD 卡插口切勿公用。

阅读更多 >

定义清晰的角色和所有权

需要制定清晰的规则和规程，确保员工对自己的责任区域拥有正确的访问权限。企业应遵守“最少特权帐户”原则，这就意味着，用户仅有权访问其执行工作时所需的资源。切勿使用默认帐户。如果出于维护目的使用临时帐户，请确保在任务完成后删除这些临时帐户。

切勿依赖于设备的默认设置，尤其是默认密码。常用设备的默认管理帐户 ID 和密码通过简单的谷歌搜索，就能轻易被发现，这就让黑客的入侵变得非常简单。务必启用并配置设备保护服务，并且仅出于演示目的而使用默认设置。

61%
的工作人员在其设备中混合执行个人任务和工作任务

80%
的员工承认在其工作中使用了未经许可的软件即服务 (SaaS) 应用

75%
的网络入侵利用了弱或窃取的凭证

阅读更多 >

使用最新的适用固件

您的设备是否更新到最新可用固件？系统和设备中的漏洞或缺陷使企业易受攻击，并且黑客很可能会窃取服务器私钥或用户密码。必须制定充分成文的软件/固件更新管理计划，并始终确保网络设备更新到最新的固件和安全更新。

开展风险分析

企业应在资产保护方面花费多少开支？通过分析潜在的内外部威胁、以及关键资产遭受破坏或损失的可能性，您能够确定这些资产的保护重心。也有一些风险管理框架，如 NIST（美国国家标准与技术研究院）网络安全框架，有助于为风险管理提供相关过程和指南。

入侵记录
数量在 2019 年
显著攀升，超过
85 亿次
——相比 2018 年
增加了 3 倍以上。*

*“2020 年 IBM X-Force 威胁情报指数报告”中有关系统保护和可能威胁的数据

阅读更多 >

您的供应链有多安全?

通过与整条供应链密切合作，您能够更好地了解自己的网络和联网设备所面临的潜在威胁。当今，许多 IT 制造商都提供了成文的实践或指南，旨在增强其设备在您网络上的防御能力，同时还提供了安全的供应链文档。如果没有这些可用，必须就此与您的制造商展开洽谈，或者获取其他用户生成文档。设备应符合您的 IT 策略——无论是作为个体设备，还是作为成套系统。

始终使用加密连接

无论什么行业，数据都需要安全加密。此外，网络，甚至是局域网或内网，也应使用加密连接。在恶意代码“监听”寻找未加密传输的地方，身份验证协议可确保信息在跨网络传送之前得到加密，并有效减少攻击机会。

安全协议

- HTTP 摘要（访问）认证是其中一种协定方法，Web 服务器可以利用它来确认凭证和用户身份，如用户名或密码。
- HTTPS（安全超文本传输协议）是常用的数据加密协议。HTTPS 与 HTTP 相同，但所传输的数据利用安全套接层 (SSL) 或传输层安全 (TLS) 进行了进一步加密。
- SRTP（安全实时传输协议）能够加密视频流，从而增强对视频本身的保护。如果使用 VMS 或 SD 卡对视频进行本地存储，请确保这些 VMS 或 SD 卡也被加密。

阅读更多 >

获得良好维护的系统对于总体系统健康非常重要

保护网络周界

您了解自己的防火墙和过滤机制吗？通过强有力的保护网络，您能够更好地支持用于实施网络安全实践的其他措施。在物理安防设备上使用网络分段，如 VLAN（虚拟局域网），有助于降低敏感信息遭受侦听的风险以及个体服务器和网络设备遭受攻击的风险。此外，ACL（访问控制列表）能够有助于控制网络上的恶意活动。在投资新设备之前，请向供应商获取网络端口列表，以确保解决方案能够在整个网络上有效工作。

维护系统和过程

获得良好维护的系统对于总体系统健康非常重要。应定期监视设备和系统日志，检测是否有非法访问企图。当今技术飞速发展，新更新、新特性以及新的实践不断推出，因此，您应将维护规程记载成文，使相关人都理解相关过程。

设备管理软件，如 AXIS Device Manager，能够帮助企业实时快速地汇总联网设备和软件的完整详细目录。它扫描整个网络，捕捉关键信息，包括型号、IP 和 MAC 地址、固件版本、证书状态等。

为什么必须实施有效的生命周期管理

众所周知，网络的安全性与联网设备的安全性息息相关。当企业积极实施分层保护措施以保护其网络时，还需要以有效的方式管理其物理资产的生命周期。但即使有新固件可用，企业通常也会忽视软件更新。这往往是因为，他们缺乏对其网络上各项技术的全面了解。

一台设备——两种生命周期

对于基于软件的设备，有两种类型的生命周期。

1. 设备的功能寿命——或者说，设备实际上能够工作和运行多长时间。例如，网络摄像机的功能寿命通常为 10-15 年。
2. 设备的经济寿命——在设备维护所需的费用开始高于采用更高效的新技术所需的费用之前，设备能够运行多长时间？虽然IP摄像机的功能寿命可能是 15 年，但鉴于网络安全环境的快速变化，其实际寿命将比这个时间要短。

资产的前瞻性管理

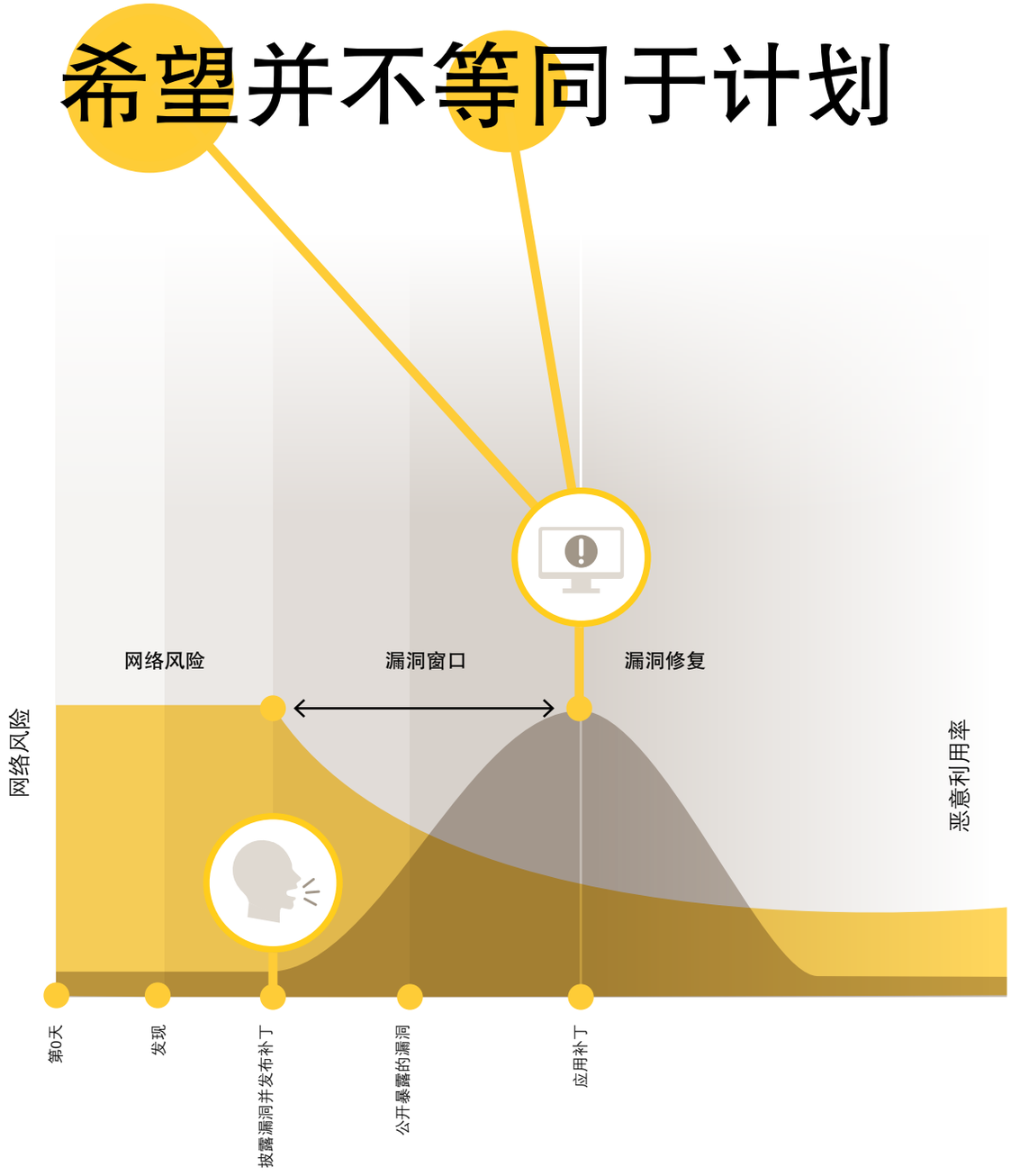
生命周期管理是对物理资产的功能寿命和经济寿命的有效管理。企业需要全面且清晰地了解网络上所部属的技术，以便密切监视其网络和关键数据，确保这些网络和数据是安全的，不会遭受威胁，也不存在漏洞。

英国信息专员办公室 (ICO) 指出

“60% 的入侵涉及的漏洞都有现成的补丁，但是却没有安装。”

阅读更多 >

希望并不等同于计划



有时，为了防止攻击者利用已知漏洞并破坏现有保护，需要更新和修复技术组件——从网络摄像机到 VMS。

更新和补丁是改进网络安全的较理想的方式，但它们并不始终兼容较早的技术。这是因为，它们可能不再受到制造商支持。从网络安全角度讲，较早的未打补丁的技术存在巨大的安全隐患。企业必须紧随威胁的演变步伐，确保始终遵守最新的网络安全实践。被忽略的设备都可能轻易成为攻击者的入侵点。

紧跟威胁演变步伐

有效的生命周期管理能够帮助企业保持商业安全。而且它还能够帮助企业以更好的准备应对未来需求。它要求明确风险所在，不断更新可能遭到恶意利用的区域。这对于安防系统尤其重要，因为如果网络监控摄像机发生故障，后果可能非常可怕。

物理设备也需要更新

制造商定期发布能够处理漏洞、修复错误以及解决其他性能问题的固件更新和安全补丁，以帮助确保系统的稳定性和可靠性。虽然企业明白修复操作系统和应用程序的重要性，但他们通常未能切实更新硬件运行所依赖的固件。这就使得这些设备容易遭受网络攻击，其结果可能是丢失宝贵的客户信息，甚至可能是来自监管部门的大笔违规罚款。

阅读更多 >

精简的生命周期管理

有序的生命周期管理计划有助于企业面向未来做好充分的准备。它利用合适且先进的技术，尽可能减少安全威胁和漏洞。设备管理软件，如 AXIS Device Manager，能够帮助企业自动完成这个任务，从而有效管理企业资产。

节省时间和精力

设备管理软件能够帮助企业在网络安全风险的管理方面节省大量时间和精力。这类软件可用于维护系统，因为它让您能够：

- 同时向适用的设备推送系统更改、固件更新和新证书。
- 轻松创建或重新配置安全设置，并将这些设置应用到整个网络中，从而确保设备都符合安全策略和实践。
- 确认所有设备都在运行最新且安全的固件版本。
- 跨整个网络管理用户权限级别，配置修改。

工作原理

设备管理软件能够快速地汇总摄像机、编码器、门禁控制、音频以及其他联网设备的完整详细目录。它能够扫描整个网络，当发现新的或经更新的设备时，它会捕捉关键信息，包括型号、IP 和 MAC 地址、固件版本、证书状态等。

总览全局

通过高度细致地总览整个网络生态系统，能够更轻松地跨设备实施一致的生命周期管理策略和实践，并安全管理重要的安装、部署、配置、安全和维护任务。

阅读更多 >

实时洞察

设备管理工具让企业能够实时分析其生态系统的状态。例如，您可以查看哪些设备已拥有最新的补丁、固件更新和证书。而且您还将知道，在不再受制造商支持的情况下，相应设备是否已被打上移除标记。这一宝贵的信息能够帮助您判定恶意软件是否有可能感染您的设备。您将能够访问所需的信息，以便解决一系列其他漏洞问题，从而防止这些问题妨害您的网络。

前瞻性生态系统安全

自动开展设备管理过程有助于保护网络不遭受威胁、也不存在漏洞。但企业应务必遵守有意义的网络安全策略和实践。例如，您的企业是否就密码强度制定了相关策略，用户需要多久更改一次密码？建议关闭未使用的服务，以便减少暴露给潜在攻击的区域？多久进行一次设备漏洞扫描？您是否制定有相关规程，以用于在制造商发布已知漏洞时评估风险级别？这些是您要考虑的其中一些问题，它们有助于您明确并实施相应的措施，为您的网络生态系统提供前瞻性保护。

5
自动化生命周期管理所带来的收益

1. 时刻关注应用环境中的关键技术
2. 事先获悉技术生命周期
3. 避免出现需要突然更换主要系统组件的情况
4. 为设备更换制定相应的计划
5. 每年就可预测的设备剩余生命周期（百分比）制定预算

什么是零信任网络？

网络正越来越容易遭受攻击。它们不仅要面临着越来越先进且种类繁多的网络攻击，而且联网设备的数量也呈指数级增长态势，这两种现象都为网络攻击额外打开了入侵之门。因此便诞生了“零信任”的概念，零信任网络和架构也随之出现。对于硬件制造商（包括安讯士在内）而言，必须要为零信任的未来做好准备。这样的未来将来得比我们想象的要早。

网络中无一可信

顾名思义，零信任网络中的默认观点是，联网实体以及网络中的实体，显然无论是人还是机器，都是不可信的。这无关于这些实体所在的位置以及连接方式。相反，零信任网络的要义是“从不信任，始终验证”。

谨遵“最小必要访问权限”原则

这要求以不同方式多次验证访问网络的或网络内的实体的身份，具体取决于相关行为以及网络中被访问的特定数据的敏感度。就本质而言，向实体授予的权限是他们完成任务所需的最小访问权限。

零信任网络中的默认观点是，联网实体以及网络中的实体都是不可信的。

阅读更多 >

防火墙能力不足的 3 大原因

一直以来，企业都依赖于确保企业防火墙尽可能稳健，但出于多方面的原因，这种方法所存在的问题正日益突显。

1 破坏可能性高

虽然防火墙看似能够确保网络访问安全，但如果有人能够突破防火墙，那么他便能够在网络中相当自由地活动。

2 防火墙不再足够

联网设备的绝对数量在不断增加，这就意味着，仅依靠一套解决方案，已无法再满足网络周界保护的需求。

3 更具“渗透性”的网络带来了收益

对网络外的云服务的使用、以及无缝连通的客户供应商系统所带来的收益使网络安全的性质发生了改变。

> “曾经，在网络内部，造成潜在不可修复损失的数据丢失是切实的风险，但不良分子在被发现（如果他们能够被发现的话）之前，可能已持续活跃了数周或数月之久。
>
> 安讯士公司区域架构与工程经理 **Wayne Dorris**

阅读更多 >

零信任的工作方式

零信任采用了诸如颗粒化网络周界安全以及网络微分段等的技术。前一项技术以用户和设备为基础。它利用它们的物理位置及其他标识数据来判断它们用于访问网络的凭证是否可信。后一项技术涉及对较关键数据所在的特定网络部分应用不同的安全级别。

进一步增强安全

仅针对个体完成其任务所需的网络部分和数据，为个体授予访问权限，能够带来显著的安全收益。但为与这些身份相关的行为打上异常标记，进一步提升了安全级别。例如，网络管理员可能对研发或财务服务器的维护拥有较大的网络访问权限。

红色安全标记

如果该网络管理员的凭证在半夜被用于下载特定关键文件或数据并将这些文件或数据发送到了网络之外，那么将打上红色安全标记。在零信任网络中，可以使用以上任一种附加身份验证，或者也可以实时标记异常活动，并提交给安全运营中心以便开展调查。

行为异常可能表明安全凭证被窃取、有员工存在不满或者有人在从事企业间谍活动。

阅读更多 >

策略引擎解析...

策略引擎是零信任网络的核心：它是一种软件，让企业能够创建、监控并实施与如何访问数据和网络资源有关的规则。策略引擎将网络分析工具与经编程的规则相结合，依据多方面的因素，授予基于角色的权限。

接受或拒绝请求

简言之，策略引擎将每个网络访问请求与其策略情景进行对比，告知执行器是否允许该请求。在零信任网络中，策略引擎定义并跨托管模型、位置、用户和设备实施数据安全和访问策略。

定义并应用规则

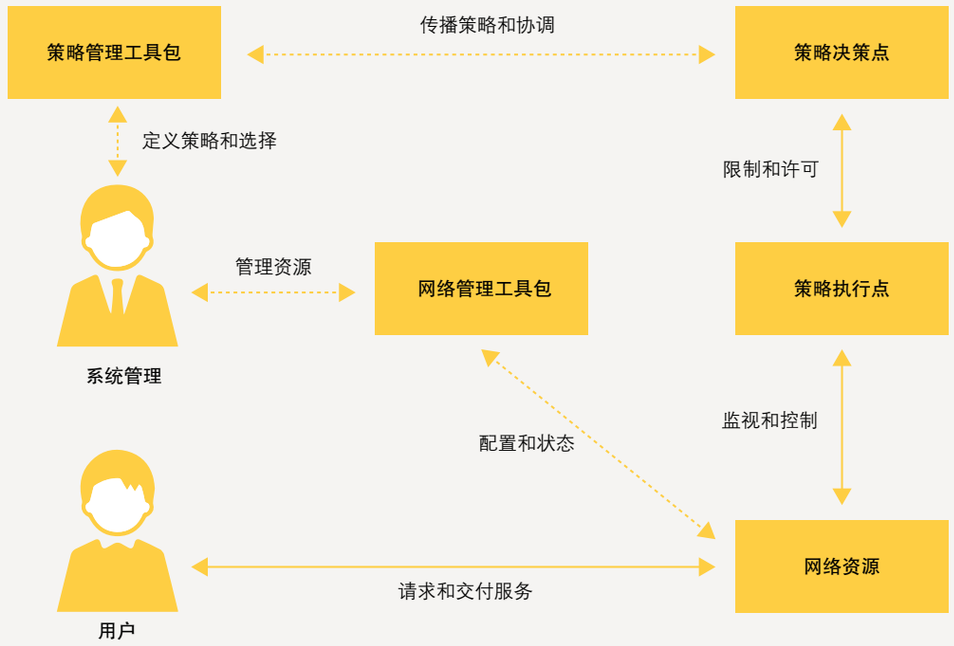
为了确保策略引擎的有效工作，企业必须谨慎定义关键安全控制方案内的规则和策略，如下一代防护墙 (NGFW)、电子邮件和云安全网关、以及数据丢失防护 (DLP) 软件。这些控制方案组合到一起，共同实施超越托管模型和位置的网络微分段。

如何访问数据和网络资源？

策略引擎让您能够：

- 创建规则
- 监控规则
- 实施规则

策略引擎——概览



现今和未来的策略引擎

当前，可能必须在每个解决方案的管理控制台中设置策略，但集成化程度越来越高的控制台能够跨产品自动定义并更新策略。

身份识别与访问管理 (IAM)、多因素身份验证、推送通知、文件权限、加密以及安全方案，全都影响着零信任网络架构的设计。

阅读更多 >

零信任网络与视频监控

联网实体当然包括人，但当今，更普遍的网络连接是设备连接。其中就包括网络监控摄像机以及相关的联网设备。随着企业向零信任网络架构的转型，网络设备将必须遵守“从不信任，始终验证”的原则。

哦，真讽刺！

如果设计用于保护企业物理安全的监控摄像机成为了网络安全漏洞，岂不是够讽刺的？同样，传统的设备安全形式已经不再足够了。正如上文所说，不良分子可能窃取员工的访问凭证，也可能破坏设备的安全证书。在零信任网络中，需要为设备采取新的方法来向网络展示其可信性。

有点出乎意料的解决方案

能够为所连接的硬件设备提供不变信任根的一项技术是区块链技术。许多人会将区块链与声誉不太好的加密数字货币相关联。但区块链本身是一种开放的分布式账本，能够以可验证的方式高效永久地记录双方的交易。企业可以借助私有区块链来使用硬件信任根，从而在设备内部建立不变的信任密钥。

预测显示，将有超过

750 亿

IoT 设备在 2025 年之前投入使用

区块链技术为什么有用

鉴于区块链的构造，事务全都加密链接到一起，如果许可节点未同意先前的所有事务，就无法更改链中的数据事务。因此，如果将硬件设备的可识别部分的信任密钥构建到了区块链中，便会为设备自身创建不变的凭证。

在网络空间中，AI 军备竞赛已然开启

随着技术发展，不良分子无疑将能够快速找到有助于实现其犯罪目标的潜在突破口。当网络罪犯计划实施勒索软件攻击或者窃取财务信息时，或者当某些民族国家着力打击敌手的关键基础设施（如果并不糟糕）时，新技术就有着强化其攻击力度的潜力。

这些组织拥有雄厚的资金支持，正如一切合法企业那样。他们能够以创新的方式利用新技术，如人工智能 (AI)、机器学习 (ML) 和深度学习 (DL)。他们不遵守任何国家或国际法律法规、道德或伦理规范，

仅着眼于这些技术为他们实现犯罪目的所带来的机遇。

罪犯总是能够找到新技术（包括 AI 在内）的利用途径。**幸运的是，新技术也可以被目标企业用作防御武器。**

阅读更多 >

隐藏在显眼处

网络入侵者正越来越多地利用人工智能来提升其攻击的复杂度。大型分布式拒绝服务 (DDoS) 攻击通常成为头条新闻，因为它们能够造成大型网站和网上服务瘫痪。它们是如何做到的?

尽可能长时间躲避侦测是大多数网络罪犯的主要目标。他们的行为在本质上与入室盗窃者相似。他们在不同房间之间辗转，小心的规避着摄像机和报警器，搜刮贵重物品，然后像来时一样悄悄地离开。同样，网络罪犯也寻求渗透机会，到处活动，在不被侦测到的情况下离开网络。

1

其具体的操作方式之一便是，尽可能表现得像网的合法用户（无论是人，还是设备）。而这也是AI和ML作为宝贵新式武器的用武之地。它允许网络罪犯学习人和设备的网络行为，快速开发新的恶意软件和网络钓鱼策略，然后大规模部署这些软件和策略。

2

但非法网络访问的简单的方式仍是，以特定方式迫使合法用户点击链接，为其开启攻击之门。假冒老板的电子邮件在语气和风格上几乎与真邮件不相上下，通常可能是有效的突破口。

人工智能 (AI) 是一组算法，允许计算机存储和分析某个操作的结果。于是，在下次遇到类似的请求时，它能够相应地调整该操作。在成百上千的此类请求中，它能够逐渐优化自己的响应和操作。

阅读更多 >

条条大路通罗马

网络罪犯在攻击期间会用到多种 AI 工具，从通过虚假社交媒体用户引诱员工上当的“聊天机器人”，到用于识别高价值数据以供提取的神经网络，不一而足。

在实现了访问的情况下，内网漫游就是一项这样的技术。其关键在于，网络入侵点（其可能是不受保护的远程设备）几乎不是最终攻击点。

最终，入侵者将转移到更敏感的网络区域，一路窃取用户凭证，尤其是网络管理员等权限用户的凭证，从而获得打开网络访问之门的主要钥匙。

阅读更多 >

IT 与 OT 之间的危险联系

在当今世界，联网设备以及所谓的物联网 (IoT) 呈爆炸式发展的形势下，风险也在快速增加——因为信息技术 (IT) 网络与运营技术 (OT) 环境的集成越来越紧密。

简言之，IT 网络管理数字信息的流动。相比之下，OT 管理企业或特定场所的物理过程、机械和物理资产的运营。对于那些以扰乱和破坏而不是盗窃为目标的不良分子来说，OT 访问才是关键。不难想象，若发电站、炼油厂或医院的设备遭到非法访问，由此造成的潜在损失会有多大。

阅读更多 >

侦探般的慧眼

网络罪犯对 AI 的潜在利用令人毛骨悚然。但这些技术当然也能够用来保护网络免遭渗透。防御者可以采用很多方法来防范攻击者，占据优势地位，先发制人。

DARKTRACE

Darktrace 是一家享誉全球的企业，专注于网络安全领域的 AI 应用。正如您预料的那样，他们同样擅长理解犯罪组织对 AI 的日益增多的使用。Darktrace 不断推进 AI 和 ML 创新，争取及早拦截罪犯。

防御者可以采用很多方法来防范攻击者，占据优势地位，先发制人。

阅读更多 >

攻守兼备的 AI 技术

下面几页涉及我们对 Darktrace 公司执行副总裁 Jeff Cornelius 的采访，由此，我们将详细了解他的公司是如何使用 AI 和 ML 来及早拦截罪犯的。

采访 Darktrace 公司的 Jeff Cornelius

问题

攻守现状如何?

“首先，除了通过媒体报道获得的认知，AI 和 ML 的开发其实并不容易！虽然致力于网络攻击的犯罪组织和某些民族国家是强大的敌手，但也有许多对我们有利的方面。

“这其中更主要的是，在客户为我们授予了访问权限的情况下，我们能够总览网络活动。”我们由此来了解每台设备和每个用户的行为。相比之下，不良分子所依赖的仅是部分活动的有限视野。从踏入初始入侵点开始，他们的动作都是单方面的盲目前行，因为他们所在的环境是我们了解而他们不了解的。

“最后，他们的目标包括合法企业通常不会实施的活动。我们的主要目的是，发现并处理这样的网络行为异常。我们需要广泛搜索，因为我们不知道敌手将于何时何地出现，以及他们具体将采用什么新方法、有着什么新目标。”

阅读更多 >

有趣的比方

采访 Darktrace 公司的 Jeff Cornelius

问题

您能说得明白些吗?

“打个比方，有人在我家屋外研究我每天的活动，从而对我的习惯有了相当详细的了解：我每天通常几点离开家、上班走哪条路线、在哪里吃午餐等。他们也许能够较成功地模仿我生活的这些部分。

“但由于没有细查我家的内部布局，如果他们试图模仿我的早餐口味，那么几乎肯定会出错，而这样的错误会很容易被我亲密的家人捕捉到并视为异常。通常，互联网上面向个人的那些狡猾的鱼叉式网络钓鱼邮件都看似正派，但一旦给了可趁之机，他们便会喧宾夺主。”

阅读更多 >

受监督的机器学习...

采访 Darktrace 公司的 Jeff Cornelius

问题

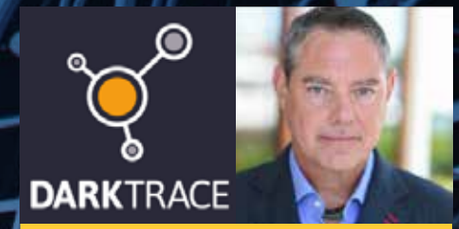
请详细介绍一下机器学习。

“这里涉及对有监督ML和无监督ML 的重要区分。在前者中，针对一系列已知数据训练计算机。它们不断比对这些数据，以判断所记录的结果是否是预期结果。

“从网络安全角度讲，学习模型建立在已知恶意软件的基础之上。这是罪犯与网络安全切实竞赛的地方：不良分子使用ML来创建新的恶意软件版本，而我们会看到这些版本的指数级增长。网络安全公司着力于紧随此步伐，编写新模型以用于有监督ML 防御。这有点像拼写检查，努力跟上每天都有新字、甚至新语言不断涌现的时代步伐。而这种步伐紧随，即便可行，也正变得越来越难。

阅读更多 >

...与 不受监督的机器学习”



采访Darktrace公司的Jeff Cornelius

问题

不过，还有别的方式吗?

“有的。相比之下，无监督ML算法不依赖于对过去威胁的了解，而是独立分类数据并侦测典型模式。它们对网络数据进行规模化的分析，仅基于自己所见的证据，执行数十亿次的基于概率的计算。由此，它们便了解了特定网络上属于设备、用户或者设备组或用户组的“正常”行为。然后，它们能够检测与这种不断演变的“行为模式”之间所存在的、可能指向潜在威胁的偏差。这种预警系统将让我们能够及早拦截罪犯和不良分子。”

多方协作，减少网络安全威胁

保护公司、企业、关键基础设施和城市并不是一个人就能做到的。没有灵丹妙药——没有单一解决方案。准确地说，要成功保持网络安全的合格水平，离不开大量坚定利益相关者（包括最终用户）的共同协作。

打造网络安全文化

这里也离不开多方协作。您应该将企业内的每个人都视为网络安全团队的成员。需要考虑：

- 为员工安排网络安全培训
- 新员工入职后，对他们开展相关教育
- 鼓励高层领导实施网络安全策略
- 不断了解所出现的网络威胁，并及时告知大家
- 选择新网络设备时，必须审查相关网络安全
- 实施自带设备 (BYOD) 策略
- 制定并应用网络安全事件响应策略

通过在整个企业内推行网络安全计划，能够更好地确保网络和设备的安全性。

阅读更多 >

共同的责任

网络安全涉及产品、人员、技术和正在进行的过程。很明显，我们需要多方协作，才能确保网络安全链的环节都尽可能坚固。网络安全是一种共同的责任，需要以下利益相关者（包括最终用户）共同协作：

集成商和安装商

他们需要确保所有已安装的设备都拥有最新的更新且运行有先进的病毒扫描器。利益相关者应协力确保针对密码、远程访问管理以及随时间推移的软件和联网设备维护，实施稳健的策略。

经销商

对于不直接接触其经营产品的经销商，网络安全就变得相对简单。然而，如要成为增值型经销商，就需要考虑与集成商和安装商相同的方面，尤其是当他们从制造商那里进货然后再重新贴牌（以他人或自己的品牌）销售时。透明性是关键。设备来源必须清楚。

顾问

他们帮助指定系统要求，还应帮助指定相应的生命周期维护要求，在潜在相关成本方面，他们必须保持透明。OEM/ODM 设备的网络安全责任通常不清晰，在讨论总体网络安全时，还应考虑使用这些设备所带来的挑战。

设备制造商

这是网络安全的起始地。制造商应在设计、研发和测试中应用网络安全实践，以尽可能降低缺陷风险。内置的安全特性、自研芯片以及对自身供应链的仔细控制，也非常重要。同样，以工具促进经济实惠的自动化设备管理、以及将已知漏洞告知渠道商和合作伙伴，也非常重要。

研发人员

他们通常发现设备漏洞。如果漏洞不是刻意引起的，研发人员通常会告知制造商，这样，在产品发布前，制造商便有机会修复这些漏洞。但如果关键漏洞具有刻意性质，研发人员通常会做出公示，提起用户注意。

最终用户

由于企业都有自己特殊的网络安全需求，因此没有通用的网络安全配置。相反，必须制定一系列信息安全策略，来界定所需的安全范围。删除默认帐户，设定唯一的强密码并安全存储、定期更改这些密码，有区别地分配权限，始终安装补丁和更新，就是其中一些应采取的措施。

阅读更多 >

合作伙伴皆受保护

只有通过共同协作，我们才能够确保以更好的准备应对不断变化的网络安全威胁，并在威胁实际到来时，快速采取应对措施。各利益相关者都影响着网络安全解决方案环节的正确落实——从设备制造、系统设计和安装，到维护和设备管理。这就是我们保持警觉的方式。

在互联环境下，网络安全如何增强信任

互联互通的世界

随着时间进入 2021 年，网络“前端”的计算持续增长。数十亿台所谓的 IoT 设备已经连接到网络，而且这个数字还在加速增长，这一事实本身并不是新闻。但是这些设备的性质和需求确实暗含了一些严重的网络安全问题。

IoT

IoT（物联网）是指由设备组成的网络，这些设备连接到互联网，并能够彼此“通信”。它们包括小型高科技设备（如智能电话、可穿戴设备）、智能家居设备（如智能仪表）、以及工业设备（如智能机器）。IoT 设备利用传感器和处理器收集并分析从其应用环境中获取的数据，并相应地执行操作。

飞速增长

预测显示，**到 2025 年之前，**将有超过 750 亿物联网 (IoT) 设备投入使用。相比 2019 年的 IoT 安装基数，这个数字增加了将近三倍。

阅读更多 >

互联互通的世界

> “摄像机自身内部的数据处理和分析呈日趋增多的趋势。

简而言之，连接到网络的“东西”中，有更多需要即时感知正在发生什么、决定要做什么并采取行动这样的能力，或会从这些能力中受益。

无人驾驶汽车就是一个明显的例子

无论是涉及到与外部环境（例如，交通信号灯）进行通信，还是通过检测风险（例如，突然出现在汽车前方的对象）的传感器，决定都必须在一瞬间得到处理。数据跨网络从汽车发出以在数据中心进行处理和分析，与返回要采取的措施的决定之间存在着让人难以接受的延迟。

视频监控也是如此。

如果我们采取主动而不是被动方式——预防事件发生而不是事后做出反应，摄像机本身需要进行更多的数据和分析处理。但随着前端设备的不断增多，加之这些设备在安全和安防方面起着更为重要的作用，多方面的后果随之而来，我们将在后文对此做详细介绍。

阅读更多 >

专用设备的强大能力

专为特定应用设计的经过优化的专用硬件和软件，对于向更高级别的边缘计算迈进至关重要。所连接的设备将需要更强大的计算能力，并且在设计和制造过程中，需要从一开始就融入网络安全理念。

这也说明了为什么自研的集成处理芯片非常重要。例如，安讯士设备采用了公司自研的“片上系统”，它能够保护设备免遭网络攻击——比如，可能创建“后门”的未授权恶意“固件”升级。新一代 ARTPEC-7 处理器专为满足当今和未来的视频监控需求而设计，从一开始就纳入了安全考量。

全新 Axis ARTPEC-7 芯片专为视频监控而设计，其性能比初代产品提升了 50 倍以上。我们控制自有芯片的设计和制造，这意味着安讯士能够打造契合客户需求的产品，同时还能够应对外部因素的演变（如网络安全威胁）。

> **“ARTPEC-7 让我们提供的网络摄像机不仅有着出色的图像品质，而且还拥有高性能、良好的带宽效率以及在前端运行分析工具的能力。**
>
> 安讯士公司专家工程师 **Stefan Lundberg**

阅读更多 >

迈向可信赖的前端

信任有多种形式：

- **相信企业将以负责任的方式收集并使用我们的数据**
- **相信设备和数据是安全的，不会遭受非法访问**
- **相信数据本身是准确的，且技术本身的应用将达到其设计水平**

前端将是建立或破坏这些信任的一个点。

贯穿整个供应链的信任至关重要。尽管将间谍芯片嵌入硬件本身的可能性相对较小，但通过后续的固件升级将间谍“后门”安装到设备中要比在制造时安装相对容易。

阅读更多 >

迈向可信赖的前端

围绕个人隐私的话题会在全球范围内继续争论。虽然可以在前端使用诸如动态匿名化和屏蔽等技术保护隐私，但是在各个地区和国家之间，态度和法规并不一致。监控领域的公司会不断需要穿行于国际法律框架中。

网络安全比以往都更重要

随着设备本身对数据的处理和分析的增多，网络安全将变得愈加重要。即使面对越来越多也越来越复杂的网络攻击，许多企业仍然未能履行哪怕是基本的固件升级措施。要构建安全系统的基础，需要依据清晰的硬件、软件和用户策略，既对个体设备进行管理，也对整套监控解决方案进行全方位生命周期管理。

不合规威胁

近些年，British Airways、Marriott International 等企业因违规支付了巨额罚款。罚款威胁振荡了整个商界，现在正影响着企业的网络安全预算。

企业也受到其他针对性攻击的威胁，如勒索软件、恶意软件和网络钓鱼等。这可能导致系统关停、数据丢失、运行中断、声誉受损、客户流失、收入锐减。

什么是合规？

合规通常是指符合政府法律法规和国际标准。但这仅是合规的部分含义。企业还需要实施并遵守内部管控章程和实践，同时确保自己的合作伙伴也做到合规。

企业现在有责任确保他们的客户数据得到充分的保护。

有三个方面需要考虑：

1. **符合法律法规**
   政府法律法规（如 GDPR）以及国际标准和框架（如 ISO 或 NIST）
2. **内部合规**
   公司内部策略和实践
3. **外部合规**
   供应链内部的合规

阅读更多 >

守法是我们的义务

数据保护法律，如欧盟一般数据保护法案 (GDPR)，旨在管控机构、企业或政府对消费者个人信息的使用方式。在网络安全方面，这样的法律通常与企业现行的安防解决方案密切相关。虽然 GDPR 是欧洲法律，但从某种程度上说，全球许多企业都需要遵守该法律。例如，在欧盟地区存储数据的美国公司需要遵守 GDPR。同样，如果某个企业与执行数据处理的第三方订有合同，这些相关方也将需要遵守 GDPR。在美国，50 个州在数据保护方面有着各自的法律法规，这就使得跨州的工作难以开展且非常耗时。

内部管控的成本较高

黑客并不会攻击标准，他们的目标是公司，黑客会判断公司的具体漏洞是什么以及在哪里。企业可能一不小心就将预算花在了网络安全上。但，企业的目标应该是提供充足的保护，而不是妨碍其创新工作。这需要平衡，具体取决于企业对风险的管控力度要求。一些企业的控制力度甚至大于法律要求的力度。因为，如果网络安全遭到破坏，企业需要证明其采取过正确的商业保护措施。

供应链内部的合规

拥有复杂供应链的企业还将有着其他的合规要求。例如，与美国政府做生意的欧洲企业需要遵守特定标准，如“网络安全成熟度模型认证”，此标准要求基于内部网络安全管理规程进行审查认证。在糟糕的情况下，第三方（如供应商）也可能为违规承担部分责任，因此要承担一定比例的罚款。

虽然外部义务非常重要，但仍建议企业内部策略优先于这些外部规则。原因在于，在一天的工作结束后，要由企业负责确保合规性，并保证数据受到保护，不受入侵。

阅读更多 >

哪些法律法规适用于您?

保持合规需要坚持不懈的努力。适用于您企业的网络安全和数据管理法律法规通常取决于您所在的行业。然而，有些法律法规是跨多个行业和国家的。

企业需要持续关注即将施行的条例以及可能的法律修订。通过审查当前的威胁和攻击，掌握即将推行哪些适用于自身的法律法规，企业能够明确自己需要做出的改变，确保通过新的合规检查。

网络安全审查

一旦明确了自己企业需要遵守的法律法规，您就需要评估总的合规状态。通过开展内部网络安全审查，您能够评估企业的 IT 安全管控流程。一般来讲，企业需要每年开展一次网络安全审查。但建议持续监控管控措施，以便有助于确保及时调整不当的管控措施。还建议企业定期记录对安全管控措施进行的这种持续评估。在将来的审查中，可能用到这些信息。

网络安全审查期间的一些注意事项：

- **风险管理：**您的企业采用什么样的流程来发现并管理与合规相关的风险？例如，您如何通知风险，以及采用什么样的流程来确保风险评估?
- **内部审查流程：**企业需要制定内部审查流程，以便持续监控合规性。例如，您采用什么样的既定流程来发现、评估和控制网络安全实践的变更?
- **安全和隐私保护培训：**您的员工是否有此能力且接受过相关培训，能够发现与 IT 安全需求之间的差距？例如，您是否就如何处理电子邮件网络钓鱼制定了培训计划？制定这样的培训计划仅是其中一部分。内部管控将判断培训的有效性。如果某个区域对于企业而言是高风险区域，那么将会每季度（而不是每年）开展一次检查。

阅读更多 >

合规监控

可以依据内部审查的结果，制定合规监控计划。这个计划可用于持续评估企业的总体合规措施，处理在审查期间发现的风险。应优先处理对企业有着巨大威胁的风险。通过评估企业现行的合规管控措施，您可以发现网络安全管控措施中不合规的地方。

在确定谁来负责监控网络安全风险时，应根据所需的专业知识，指派人手。通过判断哪些员工具备所需的技能，以及可以组合哪些风险监控活动，能够优化人手分配。

您是否保持更新了？

制造商通常会定期、以及在新法律法规有所要求时，发布固件更新，以修复漏洞。然而，清晰地总览各设备及生命周期状态，也是非常重要的，这有助于您时刻做好准备，以防某个产品不再兼容。设备管理工具，如 AXIS Device Manager，可帮助确保产品处于已更新且合规的状态。这些工具会发送与许可证订阅续期、维护时间或认证有关的通知，有助于确保企业满足合规要求，始终保持在新状态。此外，如果需要审查，这些工具还能够提供所需的文档资料。

合规证明

设备制造商通常需要应客户要求，提供有关网络安全级别的调查报告。企业需要回答与其持续性计划、认证实施方式以及网络数据保护方式有关的问题。通过确保对这些信息的分享，企业可以快速证明自己是如何开展尽职调查的，从而让其客户放心。

> “违规的代价非常大。如果您认为合规成本太高，试试违规吧。”
>
> 前美国司法部副部长 Paul McNulty https://youattest.com/

阅读更多 >

文档资料、文档资料、文档资料

为了确保您能够证明自己符合法律法规，文档资料非常重要。您的内部策略可能包括众多说明，诸如：

- 为什么要录像，以及会录下什么?
- 是否设置了指示牌，向公众告知其正受到监控?
- 您的监控系统会显示具体的人吗？这侵犯到了他们的隐私，必须加以考虑并记录成文。谁有权访问监控影像?
- 数据如何存储，以及存储多久？数据存储在物理和网络安全方面是否都安全？您如何确保删除较早的影像?

您还应该针对某些特定的场合，提供文档资料。例如，如果有人入侵，应该如何处理—谁负责管控数据，遵循什么样的流程？此外，还建议向监管工作组告知在内部审查期间发现的不合规情况，以及企业为消除这些不合规而采取的措施。

合规是一个活动的目标

法律法规在不断变化，必须认识到，即使是高度严格的合规监控计划，也无法全面保护您免于罚款。企业必须持续监控自身的合规性，能够有信心地证明合规。

行动时机就在当下

毫无疑问，合规是网络安全的一个关键组成部分，在这里，有关合规性的担忧始终存在。企业和消费者开始注意到这一威胁，意识到如果不迅速采取行动，他们的系统和数据很容易受到攻击。虽然企业希望追求稳健的创新和增长，但他们也需要尽可能降低网络犯罪带来的风险。另一方面，消费者希望保持自己数据的安全性，希望相关企业能够想办法处理好这方面的问题。政府法律法规也是一大问题，只有以共同协作的方式，才能满足这些法律法规的要求，亦即，供应商、制造商和最终用户要共同担起责任，确保网络安全有效性。这最终将有助于尽可能降低遭受破坏性入侵的风险。

毫无疑问，合规是网络安全的一个关键组成部分，在这里，有关合规性的担忧始终存在。

您需要对自己的监控供应商以及这些供应商的供应商有什么样的了解?

安全威胁始终存在。新威胁不断涌现，它们的性质能够在时间点发生改变。企业需要知道其系统供应商，在持续评估和统计这些风险——不仅是在他们自己的业务场所内，而且还要在其子供应商的业务场所内。

企业通常只关注自己的供应商在网络安全方面所采取的措施。但供应商的供应商呢？供应商如何管控并保持整条供应链，并确保在从部件层面到成品的一系列环节中，各产品都是安全的?

您的供应商是否重视尽可能降低安全风险?

- 他们设计和制造的产品是否以内置保护来确保安全?
- 他们是否为了实施保护措施而分享知识和工具?
- 在发现新漏洞时，他们是否提供快速的响应以及免费的升级?
- 他们是否管控从部件层面到成品的整条供应链?

阅读更多 >

寻找合适的合作伙伴

供应链安全始于通过严格的评估流程选择合适的供应链合作伙伴。评估流程应包括分析每家公司的质量和可持续性管理流程。至少，该公司应获得根据 ISO 9001 或 IATF 16949 进行的第三方认证。

评估子供应商

您的供应商也需要评估其子供应商的风险管理流程，以及他们的生产设施和流程。应开展实地考察，跟进现场审查，以便评估公司是否满足供应商资质认证的相关要求和标准。在评估潜在的新供应链合作伙伴时，供应商应深入分析企业的财务状况和所有权结构。

战略子供应商

就关键部件供应商和制造合作伙伴而言，合作关系往往格外密切长久。他们是战略子供应商，您的供应商需要与他们推进联合项目和开发进程、设定目标、许下长期的相互承诺和合作计划。因此，他们之间的协作和交流非常密切，实地考察也较频繁。

您供应商的产品中的所有关键部件都应直接采购自战略子供应商，并在存放在公司内部。非关键部件可以由制造合作伙伴采购，但只能从“认可供货商名单”上的供应商那里采购。

您供应商的生产安全水平如何?

- 他们是否拥有明确的制造流程并监控这些流程?
- 他们是否研发并生产关键生产设备?
- 您的供应商是否提供用于在生产期间测试部件、模块和产品的系统，以及是否提供相应的软件、测试计算机和其他IT硬件基础设施?
- 您的供应商是否全天不间断收集生产数据，以便开展实时数据分析、评估潜在安全风险、实施风险降低计划?

阅读更多 >

审查供应商

您的供应商确保子供应商符合相关要求的较佳方式是，定期开展现场审查——每年或每两年一次。

审查应涵盖一系列重要的方面：

- 流程合规，包括文档资料
- 设施安全
- 厂内物理搬运
- 库存转移
- 生产设备
- 质量控制
- 可追溯性记录

季度商业审查也是跟进性能是否符合预期的良好方式。对于战略子供应商，建议以最高的管理级别来开展这些审查。

物理安全

供应链所涉及的每个场所，从部件供应商到经销中心，都必须符合设施安全性方面的严格要求：

- 入口和出口必须受到持续保护，必须记录并留存门禁控制和访客登记。某些区域可能需要持续监控，甚至要使用防护栏来确保设施和周边安全。
- 应使用扫描设备来检测不期望的物体或材料。
- 只能由行业公认、声誉良好且实施严格安全章程和控制措施的承运商来负责运输事宜。汽车和卡车应在装卸货时应遵守安全规程。
- 所有空运货物应接收 X 射线扫描。通常还应在始发点对每批发货盖章，以防在未经检查的情况下，破坏货箱。
- 通常使用 CCTV 摄像机对来料和去料进行监督和记录。

阅读更多 >

数据传输与信息安全

必须通过安全协议，利用加密方法和身份验证，来保护供应链网络中的数据传输。子供应商和合作伙伴需要保持非常高的信息安全水平，以降低供应链中发生不合格情况的风险。

您的供应商应以系统性方法识别并管理敏感的公司信息。这套系统应涵盖人、流程、IT 系统和物理场所，并且应符合 ISO 27001 和欧盟一般数据保护法案 (GDPR)。这将有助于提升安全意识，实施有效的风险管理。

人员安全

了解您的员工是非常重要的，这不仅涉及教育、能力和工作经验方面，而且还涉及安全方面。例如，在安讯士，招聘过程的质量和安全是关键，相关措施包括身份验证、要求提供推荐信、以及在聘用前进行安全背景调查。新员工和顾问需要签署保密协议 (NDA)，承诺在雇佣期间和离职后保护知识产权和其他敏感信息。

提升员工能力，降低风险

在安讯士，我们确保员工保持较高水平的信息安全意识。我们认为，能力较强的员工掌握了相关必要信息，清楚需要做什么以及存在哪些风险。安讯士员工都为切实的安全和信任做出着贡献，员工都接受过信息安全意识方面的教育和培训，并被要求践行谨慎作风，保持警惕。对信息、系统和资源的访问是受到限制的，只有在执行任务时有相关需求的员工，才有权访问。同样，供应商和制造合作伙伴的员工在向安讯士分享信息、系统和资源时，也要遵守这一规则。

阅读更多 >

产品完整性

跟其他产品一样，监控产品的性能也必须达到设计和预期水平，同时还要保持相应的完整性。为此，产品的硬件和固件必须受到成功保护，在产品的整个供应链历程中不遭受非法更改或篡改。

质量控制

安讯士携手其供应商和制造合作伙伴，共同应用大量质量控制措施，以便保持和保护我们产品的完整性。部件始终依据安讯士指定的物料清单，采购自“认可供货商名单”上的供应商。未经安讯士许可，供应商不得对订单要求、工作说明或质量检查文档进行修改。经审批的修改都必须记录成文并保存。

可追溯性

物料搬运流程能够始终确保物料状态，揭露可能影响质量的不合规情形。供应商和制造合作伙伴需要保有一套可追溯性系统，用以确保从来料到成品部件的生产批料的可追溯性。在生产期间，物理部件将接受多次测试，验证其合规性，发现不合格情形。

检测伪造部件

自动光学检测 (AOI) 有助于确保不安装伪造部件。在安讯士，我们自研自制关键生产设备、以及用于在生产期间对各级部件、模块和产品进行测试的系统。这个过程有助于限制篡改风险。另一项安全管控措施是，全天不间断向安讯士提供测试数据，这样就能立即发现非法修改。

为什么选择安讯士?

贡献解决方案，助力打造更智慧、更安全的世界

质量是一切工作的要义：安讯士产品接受广泛的测试，让客户充分放心。

创新的技术：我们将技术与人类想象相结合，提升性能与可用性。安讯士产品建立在开放式工业标准的基础之上，灵活性好、可扩展且易于集成。

各层面的可持续性：安讯士承诺，始终坚持以对环境负责的方式，利用可持续物料开展产品研发。例如，80% 的安讯士摄像机和编码器都不含 PVC。

提升网络安全：我们持续监控威胁和相关后果，并采取快速果断的应对措施。即使在安装完成后，我们依然通过升级、更新和安装来增强设备的网络安全。

全球化部署，本地化支持：安讯士的网络视频产品在全球拥有庞大的安装基数，其员工广布 50 多个国家。我们分享见解和经验，紧跟发展潮流。

强大的合作关系网：安讯士拥有强力的合作关系作为支撑，成为了市场上享有盛誉的集成摄像机品牌。

关于安讯士 (Axis Communications)

安讯士通过打造网络解决方案，不断提供改善安防技术的独特见解并引入创新业务模式，旨在创造一个更加智能、安全的世界。作为网络视频行业的领导者，安讯士致力于推出视频监控和分析应用、访问控制、内通系统以及音频系统的相关产品和服务。安讯士在全球 50 多个国家和地区设有办事机构，拥有超过 3,800 名尽职的员工，并与遍布世界各地的合作伙伴携手并进，为客户带来高价值的解决方案。安讯士创立于 1984 年，总部位于瑞典。

关于安讯士的更多信息，请访问我们的网站：www.axis.com