实现对网络安全旅程的管理、自动化与编排 (M.A.P)

通过六个步骤为无处不在的工作空间打造一个全面的网络安全解决方案

目录

为什么要阅读这本电子书？	2
前言	3
是时候对你的网络安全旅程加以 M.A.P. 了	4
第 1 步：全面掌握资产状况	5
第 2 步：实现设备管理现代化	6
第 3 步：建立设备安全体系	7
第 4 步：保护用户安全	9
第 5 步：提供安全访问	10
第 6 步：管理合规性与风险性	11
对您的网络安全旅程加以 M.A.P	12
关于 Ivanti	13

为什么要阅读这本电子书？

源自软件漏洞、恶意软件、凭证盗窃和其他一系列威胁途径的攻击在频率和复杂性上都急剧增加。使问题进一步恶化的是：无处不在的工作空间渐趋流行，并且我们在迅速转向远程工作方式。但是我们手头的预算及可用的专业安全人员数量却捉襟见肘，同时追踪跟进 每一个漏洞，这在以前就十分困难，而现在已经变成一件几乎不可能的事。

对于企业，最终对 IT 部门来说，这种情况需要通过实施全面的安全战略来加强安全态势、确保持续的网络风险管理并减少服务中断问题。这意味着要打破为个人电脑和数据中心主导的世界设计解决方案，转向为无处不在的工作空间设计解决方案，其中的移动-云技术是最重要的部分。

这份指南作为一个起点和框架，通过一系列步骤引导你在这个网络安全旅程中不断前进。通过遵循本指南中的建议，你可以应对无处不在的工作空间中不断增加的威胁，朝着保护用户、设备、网络、应用和数据的方向不断推进。

前言

当前的网络安全格局

威胁不是在渐渐逼近，而是就在眼前。我们是如何走到这一步的？

无处不在的空间迅速发展壮大，随之而来的是易遭受攻击的风险漏洞急剧增多。尽管最初认为这种向远程数字化业务环境的突然转变不过是权宜之计，但如今无处不在的工作空间将长久存在下去。根据Gartner[1]的数据，82% 的企业打算允许员工在部分时间远程工作，47% 的企业打算在未来允许员工全职远程工作。显然，疫情前我们所依赖的那种以个人电脑和数据库为中心的安全解决方案，如今面对分布式员工队伍和个人移动设备和云应用广泛使用的情况，已不再适当。

二维码就是个很好的例子。它们如雨后春笋般出现，从餐馆到医院无处不在，而且往往员工用来扫描这些二维码的移动设备也同时用于工作。但二维码的这种普遍性和易用性也使其成为网络钓鱼攻击的理想工具。仅需借助电子邮件网络钓鱼解决方案，就能轻易向用户以及企业发起攻击。

更糟糕的是，各类威胁已经变得越来越狡猾——往往专门针对远程工作性的漏洞——正在以惊人的速度发生着。例如，网络钓鱼企图同比增长 85%（74% 的组织成为受害者），59% 的组织报告称在 2021 年受到勒索软件的侵害。考虑到全球安全专家的短缺，加上各地预算紧张，现在对漏洞加以整理和排序这样的简单工作就消耗了安全和 IT 部门很大一部分时间——高达 53%[2]。

这是一场完美风暴：工作场所在发生变化、要保护的东西太多，而手头资源却不足。硬抗下去不是办法。不采取行动的企业可能会遭遇更多的数据泄露，包括勒索软件、网络钓鱼、黑客攻击和内部员工（有意或无意）造成的漏洞，并有可能违反不断变化的合规要求。对品牌的影响更是天文数字，包括意外停工、合规问题、声誉和客户损失，据估计每次数据泄露的成本约为 424 万美元[3]。勒索软件攻击造成的中断期平均持续 22 天[4]。合规违反事件已经给公司造成了超过 13 亿美元的损失……而且这个数字还在不断增加。[5]

“这是一场完美风暴：工作场所在发生变化、要保护的东西太多，而手头资源却不足。”

是时候 M.A.P 你的网络安全旅程了。

M.A.P 是 Manage、Automate 和 Prioritize（管理、自动化和优先级编排）的首字母缩写，是一个三阶段过程，其最终目的是为无处不在的工作空间构建一个符合整体框架目标的全面性可扩展网络安全战略。

管理，作为第一阶段，目的是建立你的网络安全基础。通过它，你的目标是从未知境地前进到已知境地。这意味着要深入洞察谁是你的用户，以及他们正在使用的设备和应用，以更好地了解你的漏洞所在。这也意味着要摒弃那些可能置组织于风险之中的做法，例如让未受管理的设备访问业务资源（尤其是云资源）或不跟进最新的补丁。

自动化，作为第二阶段，目的是减轻负担。知道如何应对问题了，下一步就是通过自动执行重复性手动流程（如维护库存、设备配置入网以及部署工作空间和应用）来释放资源。你还可以增加自我修复和自我服务解决方案，以进一步减少 IT 干预需求。

最后，优先级排序的目的是抵达有序境地，即 IT 部门有信息和能力来识别和解决最紧要的风险领域。尽管实现了自动化，但仍会有一些领域需要 IT 插手。不同于非战略性、依靠猜测的风险处理方法，先后排序的做法使 IT 部门获得正确的数据及风险评分，并据以采取智能化战略性方法来应对风险并予以修复。

M.A.P 对每个组织各有不同，但在任何情况下都应该建立在用户、设备、网络、应用和数据这些关键支柱之上，并包含一致因素，如：

- 发现。
- 管理。
- 安全配置的执行和验证。
- 保持更新、基于风险的补丁系统。
- 通过包括身份核验证书在内的方法减少员工导致的风险。
- 自适应控制和生命周期管理。

虽然这种方法不能完全阻止攻击，但它可以最大限度地减少受攻击面，实现主动的智能化风险管理，让你尽可能地提前做好准备。当威胁确实出现时，持续网络风险管理可以快速投入行动，减少安全风险敞口并减少业务中断。

潜在收益还包括可见性的提高，未纳入管理及不合规设备访问业务系统的情况减少，打补丁时间缩短，审计失败风险大大降低，以及财务成本降低。借助正确的工具，所有这些都可以在减少（而不是增加）手动干预的情况下得以实现。

让企业陷入进退两难的困境——以及脱离困境的六个步骤

虽然上述情形听起来不错，但我们明白它也会让人有些担心。首先，它看似是一个没有明确出路的两难困境。我们需要加强安全、减少威胁、提高生产效率和节约资源，但由于我们的战线很长，而且威胁局面和受攻击面不断扩大，以至我们眼下没有余地来实施新的计划。

这就是为什么我们制定了六个步骤来引导组织展开他们的安全旅程。每个步骤都涵盖了一项对当今有效网络安全治理至关重要的组成部分，综合起来，就构成了一个全面且可扩展的网络安全管理战略之基础。

步骤 ①

深入洞察资产状况

你没法管理你不了解的东西。未准确地通盘掌握云和资产清单（硬件和软件），会让组织容易陷入安全风险、合规问题、过于复杂的跟踪和混乱的数据的困扰。

在全球 IT 资源紧张的情况下，现在是时候投资于自动化平台了，它能最大化你的团队能力。一个全面发现项目可以帮助你找到网络上的所有资产，包括企业所有及员工自带设备，并将它们连带关联信息一起呈现出来，这样你就知道谁在使用什么设备、他们如何以及何时使用该设备与你的组织互动，以及他们可以访问什么。

发现带来的收益包括：

- 全面且实时掌握所有接入设备和软件及其关联信息。
- 实现对各处资产的有效管理、保护和服务。
- 梳理每个来源的所有数据。
- 跟踪及回收软件许可证。
- 优化 IT 资产（硬件、软件、云）的整体支出。

发现解决方案中的重点注意事项：

- 发现、管理和保护连网和未连网设备的能力。这其中包括连接到云服务的设备。
- 自动发现和 M.A.P 关键软硬件资产与依赖这些资产的服务及应用之间的关联关系。
- 一个综合性资产数据库，可以从各种系统中提取信息，如统一端点管理 (UEM)、网络网关、云服务和 ITSM。
- 将 IT 部门采购的设备与实际连接企业服务的设备进行核对
- 连接到数据源的连接器（供应商、合同数据库、硬件保修等）。
- 集成 ITSM 和安全流程，以实现 IT 问题和安全漏洞的主动修复。

步骤 ②

利用统一端点管理实现设备管理现代化

随着越来越多的组织继续转向混合工作环境，端点安全和管理对 IT 人员和员工来说从未如此重要。现代化设备管理对于提高用户和 IT 生产力必不可少，它使 IT 管理员能够自动执行设备配置和软件部署任务，以及快速修复用户问题。

为了缩短支持用时，确保所有设备按照相同标准得到管理，所选择的 UEM 解决方案应当能够管理各种各样的操作系统，包括 iOS、Android、Windows、macOS、Linux、ChromeOS、一线员工专用设备、可穿戴设备和物联网设备，同时支持现代化管理和基于客户端的管理。

统一端点管理解决方案应该既可供本地部署使用，也可作为 SaaS 服务满足企业的部署要求。UEM 通过对终端上的企业和个人数据分别管理，帮助保护员工隐私。UEM 还全面支持 BYOD 计划，同时最大限度地保护用户隐私和企业数据安全。

使用统一端点管理方法来管理设备带来的收益包括：

- 对你的所有设备提供统一的管理和保护。
- 大规模轻松完成应用和设备的登记入网、预配置及配置工作，提高 IT 生产力和用户体验。
- 监测设备状态，并始终确保合规。
- 以远程方式迅速修复问题。
- 自动执行软件更新和操作系统部署任务。
- 提供详尽的仪表板和实时情报，以改善 IT 决策
- 检测和修复操作系统和第三方应用漏洞。
- 减少对终端用户的干扰，提供无缝化配置入网体验。

设备管理解决方案中应重点关注的功能：

- 通过利用 Apple Business Manager (ABM)、Google Zero-Touch Enrollment 和 Windows AutoPilot 等服务，为用户提供自动化设备登记服务，简化 IT 部门配置入网流程。
- 能够发现、管理和保护任何运行 iOS、Android、macOS、Windows、Linux 和 ChromeOS 设备的端点，以及如 HoloLens、Oculus 和 Zebra 等其他沉浸式和耐用设备的端点。
- 支持多种设备所有权模式，以便你能够管理、配置和保护企业所有、BYOD 和共享设备。
- 能够赋权一线员工并保护其设备上的业务应用，无需设备管理权限。
- 能够安全访问任何设备上的数据和应用。
- 通过自定义报告和自动修复操作，深入洞察并控制所有受管设备。

步骤 ③

建立设备安全体系

良好的设备健康制度涉及采取积极主动的方法确保只有符合安全规定的设备才能访问企业资源。这包括要有一套系统可以自动给设备打补丁，或隔离存在软件漏洞（包括操作系统和/或应用中）的设备。建立良好的设备健康制度需要使用值得信赖的解决方案减少数字攻击面。

另一方面，糟糕的设备健康制度会使你的组织容易遭受勒索软件等网络攻击。对于设备健康制度不佳的组织来说，不得不依靠 IT 部门而不是专门的解决方案，去主动跟踪漏洞和保护组织免受网络攻击。

移动设备的安全保障

71% 的专业人员认为移动设备对他们的工作至关重要，同时安全部门领导几乎一致认为，远程工作人员比办公室内的工作人员面临更多风险。然而，四分之三的安全专家已经屈服于压力，准备为了权宜考虑而牺牲移动设备的安全。[6]

这可是个大问题。良好的移动设备健康制度对于防止设备漏洞（如越狱、Root检测、易受攻击的操作系统版本等）、网络漏洞（如中间人攻击、恶意热点、不安全的 Wi-Fi 等）和应用漏洞（高安全风险评估、高隐私风险评估、可疑的应用行为、侧载应用等）至关重要。

建立移动设备健康制度带来的收益包括：

- 通过自动化、可用于实际操作且基于风险的情报，限制人为错误和节省 IT 投资。
- 实现0Day检测和修复，因此你不必费心猜测会发生什么。
- 即使在关闭或未连接网络的设备上也能检测和修复问题
- 通过减少受攻击面来保护你的数据、你的资源和你的品牌。

移动威胁防御解决方案中需要重点关注的事项：

- 优先考虑能够抵御所有移动攻击类型的软件，包括网络钓鱼攻击，以及针对设备、网络和应用层面的攻击。
- 对 Android 和 iOS 设备的保护是关键。寻求单一应用，且应带有设备内置机器学习引擎并与 UEM 客户端捆绑在一起。用户更愿意采用单一应用而不是两个或更多。
- 所寻求的解决方案应提供多层次保护，能防御设备、网络和应用层面的威胁——以及网络钓鱼威胁——并且兼具设备内置和基于云的威胁检测功能。设备内置保护无需连接互联网仍可检测威胁并修复漏洞。
- 务必采用分层合规策略，以便能提醒终端用户和管理员他们的设备存在合规问题。对不合规的设备将采取分级行动，从阻止访问企业资源到隔离，再到停用设备和删除所有 UEM 配置的应用、内容、设置等

台式机/笔记本电脑设备的健康制度

在勒索软件攻击和其他数据泄露成为历史之前——根据其目前的发展趋势，这一天可能永远不会到来——企业必须采取措施来保护它们。按通用漏洞列表 (CVE) 逐个打补丁是组织机构对抗勒索软件攻击最好的办法之一。遗憾的是，来自 Ivanti[7] 的研究显示，71% 的 IT 和安全专业人士认为打补丁过于复杂和耗时。这可能是因为现存漏洞实在太多了。

美国国家漏洞数据库 (NVD) 中列出的漏洞远远超过 10 万个。虽然这些漏洞中只有一小部分与勒索软件有关，而流行/活跃漏洞的比例还要更小，但确定哪些漏洞对组织构成最大风险仍是很棘手的。来自 Ivanti 的一份报告显示[8]，从 2018 年至 2020 年，使用CVSS v3 评分，如果一个组织只修补关键漏洞，其对勒索软件的覆盖率将只有 35% 左右。自动化、基于风险的补丁策略对于台式机/笔记本电脑的健康至关重要。

建立台式机/笔记本电脑设备健康制度带来的收益包括：

- 与移动设备安全体系一样，通过自动化、可付诸实际操作且基于风险的情报来限制人为错误、节省 IT 投资。
- 根据实际风险等级通过打补丁来修复 CVE，从而减少勒索软件攻击的可能性。
- 利用威胁自动排序功能，从战略角度打补丁并优化资源分配。
- 要比打补丁更进一步，做到自动响应，这样不必人工干预就能应对威胁

台式机/笔记本电脑设备健康解决方案中应当重点关注的事项：

- 对于台式机/笔记本电脑设备，务必要定期更新软件以消除——或至少限制——漏洞。由于打补丁任务可能变得过于繁重，所以所寻求的解决方案应能自动评估风险并提供实用情报，然后给最紧迫的漏洞以优先考虑。
- 基于风险的优先编排让你能够清楚了解环境中风险最大的薄弱环节。这使企业能够锁定最要紧的补丁需求。活跃威胁全局背景——即把漏洞与基于威胁的真实信息加以对应——是至关重要的，因为它可以帮助 IT /安全团队确定补丁的先后顺序，以防止可能造成最大破坏的威胁。

步骤 4

保护用户的安全

现在还喜欢密码的人似乎只剩下需要利用它非法获利的黑客了。除了给用户带来负担外，基于密码的身份验证还缺乏设备、应用、网络和威胁的关联状态。你无从知道输入密码的人是员工还是获得员工密码的攻击者。即使是最复杂的密码，也可以通过暴力破解、网络钓鱼和其他类型的攻击手段相对容易地予以破解。

密码之类的凭证仍然是泄露事件中最受青睐的数据类型之一，涉及61% 的数据泄露事件[9]。凭证比任何其他类型的数据都更容易泄漏，这在网络钓鱼中尤其突出，后者拿到凭证是为了用于获取访问权限，以进一步侵入其选中的受害组织。

SSO 解决方案创造了单一破损点，可以被黑客利用来侵入大部分或全部企业应用。根据调查[10]，42% 的人在不同账户中重复使用相同密码，17% 的人在所有账户中循环使用两到五个密码。这意味着，如果有人在工作环境之外的个人账户被泄露，但他们在工作中使用相同的密码，那么你的组织就会面临风险。

随着远程工作的兴起，人们可能会认为企业收紧了密码协议，但在 Verizon 的调查中[11]，超过三分之一的受访者表示他们的公司放松了身份验证要求以应对 COVID-19 限制措施。

是时候通过零登录实现无密码验证了。

零登录是一种使用零密码的身份验证方法（类似单点登录使用一个密码验证）。

通过无密码身份验证方法保护用户安全所带来的收益包括：

- 没有密码=凭证不会被盗取或钓鱼。
- 没有密码=更快乐的用户，他们不必记住密码，降低因为输错密码导致账户被锁定的几率。
- 提高了零信任安全的成熟度
- 节约以前用于管理密码重设和处理密码泄露的IT成本

“你无从知道输入密码的人是员工还是盗取员工密码的攻击者。”

身份验证解决方案中应重点关注的功能：

- 理想的解决方案将提供对设备、业务应用和云服务的无密码访问。
- 有效的无密码访问依赖多因素身份验证，包括物品（你拥有的东西，如移动设备）、遗传特征（生物特征，如指纹、Face ID 等）和环境（位置、时间等），而不是知识要素（如密码或安全问题）来构建身份验证。
- 对于采用上下文关联访问权限的零信任安全方法，利用能够与统一端点管理解决方案相集成的解决方案，从而能在授予访问权限之前验证用户、设备、应用、网络和威胁。
- 寻求能与现有身份解决方案（如 IdP/IAMs、MTD/XDR/EDR、SOAR、SIEMs 等）无缝集成的无密码认证解决方案。

步骤 5

提供安全访问

适用于办公室的网络边界在无处不在的工作空间中已不再适用。鉴于员工在不同的（而且往往是不可预测的）地点工作，当代网络边界必须反映这种动态，在确保安全的同时消除种种限制和复杂因素。

今天的网络应当建立在软件定义边界 (SDP) 的原则之上。SPD 提供了一个集成安全架构，而现有的安全产品（如反恶意软件）很难提供这种架构。它旨在利用那些成熟可靠、基于标准的组件，如数据加密、远程验证、相互传输层安全和安全声明标记语言。纳入这些组件以及其他基于标准的技术，有助于确保 SD P能够与您现有的安全系统集成。

虽然 SPD 是一个网络结构，但它仍然需要一个安全层来实现收益最大化。这正是零信任——确切来说就是零信任网络访问 (ZTNA)——的用武之地。Gartne r将 ZTNA 定义为一种产品或服务，它能在一个应用或一组应用周围创建一个基于身份和背景的逻辑访问边界。SDP 可以用来实现零信任网络。

建立无处不在的安全访问带来的收益包括：

- 确认只有受信任的、经过身份验证的用户才能访问资源。
- 允许网络模糊外部边界，允许为终端用户提供更灵活的部署和更轻松的工作流程。
- 避免传统网络边界的局限性和复杂性，包括其开放额外的、不必要的网络分段访问权限的倾向。
- 保持安全和可见性，同时便于访问。

零信任网络中应重点关注的功能：

- 数据主权：应用数据不借道供应商网络，也不暴露在互联网上。这种直接路径最大限度地提高了性能和用户体验。
- 全局可见性：每个用户、每个设备和每个应用的活动，包括 SaaS 部署资源。
- 对客户端安全态势进行持续自适应评估，并根据各种不断变化的全局上下文关联（如行为和地点）自动执行相关策略。

步骤 6

管理合规性与风险性

为了保持合规并减轻威胁，务必掌握治理、风险及合规 (GRC) 管理。

太多时候，企业……用电子表格手动管理合规问题，信不信由你。他们还往往花费大量资金购买零散的安全产品，却未真正了解如何整合和利用它们。这种方法就好比俗话说的“瞎猫碰死耗子全凭运气“。

务必对风险状况有一个全局把握 大多数安全态势评估都是攻击之后才做的，并且视角局限于攻击载体。这种被动反应的方法，加上 IT 人手紧缺，是现存的一个严重问题。

“太多时候，企业……用电子表格手动管理合规问题，信不信由你。”

了解合规和风险带来的收益包括：

- 用自动化合规流程取代手动任务。
- 为审计工作顺利开展创造条件。
- 主动缓解风险。
- 使预算与实际风险相一致，免除猜测。
- 创建一个更具战略性和可靠性的合规框架。
- 无需开发人员即可满足不断发展的需求变化。
- 腾出人力资源去专注从事更具战略意义的工作。

合规解决方案中应重点关注的功能：

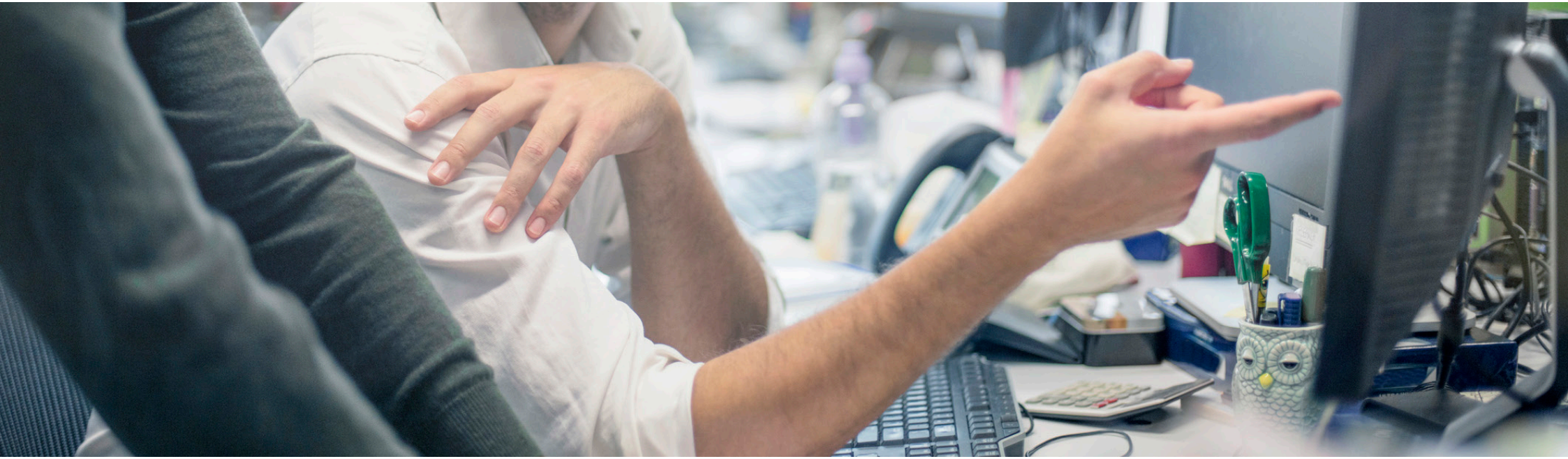
- 一个强大的解决方案将通过快速轻松地导入监管文档，然后以安全和合规控制手段来 M.A.P 其中引文，从而减轻合规负担。
- 主动风险管理能力意味着在正确的时间将注意力集中在正确的地方。
- 争取用自动化重复性治理活动取代手动任务，使你的合规过程像一台运转顺畅的机器
- 流程成熟度管理意味着你可以评估关键安全流程和控制举措的成熟度，并根据优先级和风险对其加以优化。
- 为了确保高效和准确的结果，请寻找一个能够自动引导你完成风险评估工作的解决方案。

对您的网络安全旅程加以 M.A.P

这些步骤的每一步对于达到网络安全之旅的管理、自动化和优先级编排目标都必不可少。太过繁重？不确定从何起步？关键在于寻找合作伙伴和利用解决方案来支持你的这个旅程。

合适的解决方案应是全面和综合性的，能够减轻 IT 人员的负担。最优解决方案还应保证为你的员工提供高效、直观且完整的用户体验，无论他们在何处、何时或如何工作。

随处工作。处处安全。



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”，员工使用各种各样的设备访问 IT 网络、应用和数据，以便能随时随地保持工作效率。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，通过单一管理界面让企业实现设备的自我修复和自我保护，让终端用户实现自我服务。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、以什么方式工作。更多信息请访问 www.ivanti.com.cn

ivanti

ivanti.com.cn
8610 85412999
ContactChina@ivanti.com

1. Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time
2. Ivanti: Patch Management Challenges. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges
3. Statista: Global average cost of a data breach 2021.
4. Statista: Average https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/ length of downtime after a ransomware attack 2021.
5. The biggest data breach fines, penalties, and settlements so far | CSO Online
6. 2021 Data Breach Investigations Report | Verizon
7. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges
8. https://www.ivanti.com/resources/v/doc/white-papers/spotlight_ransomware2021_risksensecsw?_ga=2.114312003.538830105.1638796042-898995573.1638285247
9. 2021 Data Breach Investigations Report | Verizon
10. Best Password Managers 2021 | The Strategist (nymag.com)
11. People and behaviors | Verizon