jamf

纵深防御：

通过整合和分层解决方案弥补安全漏洞

网络安全并不重要。

保护组织免受针对设备、用户、数据和资源的不断变化的威胁和攻击**至关重要**。

过去，信息安全只不过是在每台计算机上安装防病毒解决方案，并为少数不在办公室工作的员工（如出差的销售团队）提供 VPN 客户端。

但时代变了，我们处理网络安全的方式也随之改变。

在本白皮书中，我们将介绍：

- 威胁形势的演变
- 保护所有设备类型和操作系统的重要性
- 安全的关键不仅在于保护资源
- 实施深度防御战略的关键性
- 集成安全方法对企业的重要性

不断变化的威胁形势

该行业已经走过了漫长的道路，移动技术的进步向用户和组织机构发出了信号，即工作方式已经准备好改变。这种演变并没有停止。威胁行为者也改变了他们的策略，通过不断发展的威胁和攻击来适应变化。使它们更加复杂——这意味着最终用户更难发现它们，也更难被安全专业人员防御。

简而言之：现在的威胁来自方方面面。针对所有设备类型和操作系统，可通过任何网络连接部署。

您会问，为什么？因为基于边界的 "单一解决方案战略" 曾经可能在确保数据和端点安全方面取得过相对成功，但现在已经失效。网络边界
被以下因素有效侵蚀：

- 转向基于云的服务和应用程序

- 向远程/混合工作环境过渡

- 将个人拥有的设备纳入工作范围

- 使用不受信任的网络连接进行通信

- 依赖共享工具开展协作

毫无疑问，上述每一点都为用户随时随地在任何设备上通过任何网络连接工作提供了可能，而不受物理位置、架构或软件偏好的限制。由于暴露了更多的设备攻击面，它们还增加了潜在的攻击载体。

以下是威胁形势因移动技术和分布式员工的增加而发生演变的一些不同方式。

APT、融合威胁和攻击复杂性的增加

威胁形势已经发生了变化。任何有价值的安全专业人员都知道这句话是正确的。但是，究竟情况发生了怎样的变化，这才是本节的目的所在。恶意代码就是恶意代码——无论它是包含在冒充应用程序的封装程序中，还是通过被入侵的网站执行——其结果始终是一样的：感染您的设备，让它执行攻击者希望它执行的任务。

我们所看到的是与多年来所依赖的 1 + 1 = 2 公式的背离。攻击的复杂性与日俱增，往往与其他威胁结合在一起，或通过其他手段进行部署，如入侵目标的可信伙伴，进而提供后门访问目标资源。其中一些复杂的攻击仅可以追溯到一到三年前，例如：

- 两年内发生的两次攻击通过泄露了他们的 PII (个人身份信息) 影响了超过 **1 亿**客户。
- 2023年，供应链攻击增加了两倍 ，已知漏洞达到**21 亿次下载次数**（当时已有修复版本）。
- 赌场和酒店遭受了由社会工程活动引发的勒索软件攻击， 影响了运营，泄露了客户数据，并导致了经济损失。
- 在社交媒体平台的 API 遭泄露后， **540 万用户**的相关数据以及另外 **4 亿用户**的公共和私人数据在暗网上被出售。
- 高风险个人不断成为民族国家的目标，他们使用 Pegasus 间谍软件通过未经授权监视个人拥有的移动设备来影响隐私。

融合威胁

它也被称为 "网络-物理融合"，其名称源于我们的数字领域和物理领域日益交织在一起的性质。由于这两个领域似乎越来越紧密地结合在一起，它们之间的界限不断模糊，因此对一个领域（网络）的影响会对另一个领域（物理）产生非常真实的影响。除了对系统、流程和资源造成实际破坏外，网络威胁还扩大了攻击范围，加剧了连锁反应，从而引发更大的影响：

- 实现持久性
- 权限升级
- 横向移动
- 恶意软件部署
- 数据外泄

我们在各行各业的公司中都能看到这种情况，因为它们对技术的依赖已经成为业务连续性的关键，例如，如果遭受网络攻击，用户无法访问电子邮件，那么在恢复访问之前，业务几乎就会停止。如果时间足够长，对运营的影响可能会导致更严重的问题，如生产和/或收入损失，甚至迫使受影响的企业永久关门。

2021 年，美国最大的成品油管道（每天能够输送 300 万桶燃料）在遭受勒索软件攻击后被迫关闭五天。对这一关键基础设施的影响？报道最多的是向威胁行为者支付了 500 万美元赎金，以重新获得对加密系统和数据的访问权。此后的几年里，袭击事件引发了一些变化。美国司法部采取更积极的方式来打击勒索软件攻击背后的基础设施和犯罪分子就是其中之一。然而， 威胁行为者也发展了策略，因为“超过 90% 的攻击不再加密受害者的设备，而只是泄露数据并勒索所有人。”

社会工程学

在现代威胁环境中，基于社会工程的威胁似乎无穷无尽。曾几何时，人们唯一担心的是偶尔会有冒名顶替者试图冒充公司员工，或者是一位慷慨却又忧心忡忡的王子发来的电子邮件，他急需你的银行账户来保住他的百万家产。

哦，时代变了。

如今，社会工程学几乎是一个分层的流程图，详细列出了一个永无止境的攻击类型列表，数量太多，无法完全列出。在每项新技术发布的同时，几乎都会增加新的内容。毫无疑问，"一环套一环 "的就是网络钓鱼及其衍生的所有变种。

虽然每一次新的迭代，如二维码网络钓鱼，或被亲切地命名为 "quishing "的网络钓鱼，都会以一种多态的方式出现在我们的安全词汇中，但社会工程学的演变有两个层面——一个是表面层面，另一个是表面之下。前者很容易发现。这是五大冒充威胁，网络钓鱼针对我们的工作方式进行了调整：

1. 电子邮件网络钓鱼
2. 鱼叉式网络钓鱼
3. 鲸钓
4. 短信钓鱼和网络钓鱼
5. 灯笼式网络钓鱼

不过，后者本身并没有一个巧妙的名字。这使得这些新型威胁更加危险.....而且终端用户、IT 和安全团队都很难发现。

Jamf 威胁实验室（Jamf Threat Labs）最近发现了这些篡改技术的两个例子，它们的概念验证（PoC）对当前和未来的移动安全造成了惊人的影响：

伪造飞行模式

一种漏洞利用后持续（post-exploit persistence）技术，可显示功能飞行模式。然而，透过表象看本质，你会发现在成功利用设备后，威胁者编辑了控制用户界面的系统文件，以显示飞行模式图标，同时禁止除攻击者的应用程序外的所有应用程序访问互联网。这样，即使用户认为自己已成功将设备离线，攻击者也能保持对设备的访问（持续）。

假锁定模式

在此之前，我们提到过 Pegasus 间谍软件，以及民族国家是如何利用该漏洞追踪高危人员的。虽然我们在下一节中将介绍民族国家/赞助的威胁，但减少攻击面的一个重要工具是 Apple 的锁定模式。

假设您认为自己的移动设备已被入侵，您可以启用 "锁定模式 "来保护自己免受进一步的威胁。结果却发现，您的设备依旧同样易受攻击，因为威胁者已经有效地绕过了这一最后的保护措施。

这些正是社会工程学威胁的类型，它们欺骗用户，让他们相信自己受到了保护，而实际上他们被误导，产生了虚假的安全感，同时威胁行为者还能继续访问和控制他们的移动设备。

民族国家/目标攻击

在数字时代，无论是在公共场合、办公室还是在家中，人们对自己的一举一动、一言一行、一则信息的回复都充满了疑虑，因为技术已经渗透到我们生活的方方面面。

即使您像 Christopher Walken一样采取了不拥有电脑或智能手机的政策，您仍然有可能被周围使用移动设备的人影响隐私。

民族国家/支持的或高级持续威胁 （APT） 组织不仅对某些行业的企业构成威胁。在现代威胁形势下，APT 的攻击范围已从关键基础设施扩大到任何能促进民族国家利益的个人、组织和/或地区。

以下是一些民族国家的数字数据：

90% 的安全警报来自关键基础设施以外的部门

三大全球最受关注的行业是：
教育 **16%**

政府 **12%**

智囊团/非政府组织和信息技术并列，各占 **11%**

每 10 个中就有 9 个 组织认为它们已成为与国家有关的威胁行为者的攻击目标

给各组织造成的损失平均为**每起事件 160 万美元**

迄今已观察到**5 个 APT** 将人工智能武器化以增强威胁能力

对任何威胁行为者来说，经济利益当然是最重要的动机之一，但民族国家和与国家有关的威胁行为者的主要目标是窃取数据。这绝不是说间谍活动和破坏网络系统与服务的目标不那么重要。在现代威胁形势下，APT 越来越多地将外泄敏感和机密数据作为收集情报、实施其他恶意攻击以及影响社会和政治活动的一种手段。

就后者而言，间谍活动，特别是 用于监视高风险个人的移动恶意软件的扩散 ，已经与通过移动设备中包含的无数传感器进行未经授权的监视的隐私问题相结合，以监视用户。不仅如此，民族国家还会利用收集到的数据进一步锁定受害者，如记者、政客和高管——未经他们同意，也不知道他们的设备已被入侵。这类间谍软件具有隐蔽性强的特点，专为远程部署和从受害者的移动设备中提取任何数据类型而设计，通常依靠零点击安装和零时差漏洞来感染目标设备。

一刀切并不适用

除了我们在第一部分中讨论的网络威胁的演变性质之外，这些要点中的每一个都有助于引导我们走到目前的位置。传统解决方案、程序和工作流的临界点旨在保护：

- 公司拥有的台式电脑
- 运行一个支持的操作系统

这一点已被信息技术部门锁定：

- 只能运行有限的软件应用程序
- 限制执行任何与业务目标不符的任务
- 位于公司网络边界的相对安全范围内
- 通过企业防火墙路由网络流量
- 使用反恶意软件解决方案保护数据
- 通过 VPN 安全隧道进行远程访问

为保护静态终端而开发的传统解决方案不足以确保计算机在当今威胁环境中的安全态势，更不用说在包含代表动态工作环境的所有有影响的变化的现代企业中了。

现代安全战略得益于其强大而灵活的特性。仅仅引用禁止使用移动设备、特定操作系统类型或个人设备的管理政策，并不能降低与这些硬件或软件相关的风险。事实上，这样的政策甚至无法阻止用户试图从 "受限终端 " 访问企业资源。它们将风险引入网络的可能性非常大，更糟糕的是，管理员直到发生事故后才会意识到这一点。

那么，最好的办法是什么？

IT 和安全团队能够依靠同类最佳的解决方案对终端及其安全性进行最佳管理。管理和安全解决方案旨在原生支持其各自的设备类型和操作系统。这不仅确保了硬件和软件最大程度的兼容性，还为 IT 和安全团队提供了所需的工具，以便在其基础设施中对终端进行最佳管理和保护。

企业中的 macOS

考虑企业环境。您可能管理基于 Windows 的工作设备，但您对 macOS 计算机和笔记本电脑的立场是什么？根据 最近对中小型企业的一项调查，无论何种行业，“**55%** 的企业自己使用 Mac 设备或明确批准在公司内部使用它们”。

在进一步讨论之前，我们先来看看 macOS 的市场份额（截至 2024 年 2 月）：

全球：	美国：
15.46%	**25.02%**

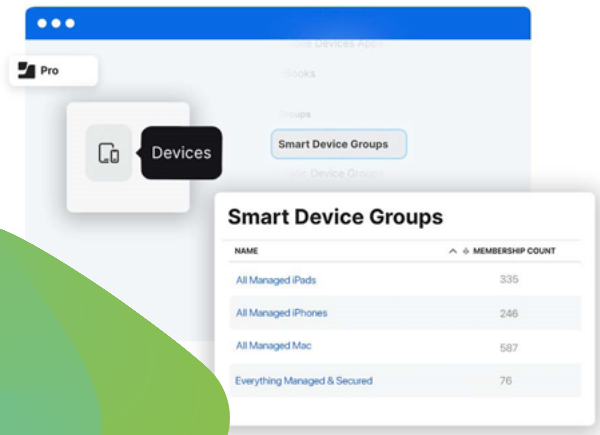
仅在美国，macOS 就占据了四分之一的市场份额，其中一半以上用于商业用途。因此，更好的问题可能是，当企业使用 macOS 终端时（而不是如果使用），如何确保它们的安全？因为无论您是否喜欢，您的最终用户都可能在某种程度上使用 macOS 来执行与工作相关的任务。无论是公司认可的企业配发设备、员工选择计划的一部分、BYOD/COPE 计划，还是用户使用的个人设备（即使未经认可）。

如果 IT 和安全团队不使用专为满足 Mac 独特需求而设计的本地管理和安全工具，就像对待基于 Windows 的设备一样，Mac 不仅会加速增长，而且会影响工作中的采用，并将对企业安全造成严重后果（任何硬件或软件都会如此）。

移动设备：无法控制的风险

普通用户只有一台电脑，但经常使用多种类型的移动设备，如智能手机、平板电脑和智能手表。事实上，根据 Statista 的一项调查，到 2023 年，全球每个用户的平均设备数量 将增至 3.6 台。

每个用户的攻击载体是原来的四倍。对于企业来说，确保基于桌面操作系统的设备安全是 "毋庸置疑 "的，但如果移动设备在企业中不受检查，就意味着它们很可能被允许连接到企业网络，并作为员工工作流程的一部分，在没有保护措施的情况下访问业务数据和资源。



存在哪些类型的移动威胁？

桌面电脑上存在许多相似的安全软件，只是没有专门的终端安全软件来提供对移动设备独特文件系统的可见性。

以下是常见类型的移动风险对企业的影响：

- **未经授权的访问：** 社会工程活动通过短信和社交媒体收集受害者的凭证，使威胁行为者能够访问业务服务。
- **恶意软件介绍：** 从不受支持的应用程序商店下载的应用程序或侧面加载的应用程序在启动时会执行恶意代码，从而影响业务和个人数据。
- **不合规：** 缺乏以政策为基础的执行，会使企业在设备不合规时承担责任，增加受监管行业的后果。
- **数据外泄：** 业务、个人和隐私数据被盗后，敏感和机密信息就会直接落入威胁者手中。
- **横向移动：** 基于网络的攻击利用被泄露的凭据将攻击扩展到整个基础设施，从而扩大数据泄露的规模。
- **绕过保护：** 错误配置的安全和应用程序设置会导致攻击面增加，使威胁更容易在设备上执行有效负载，而无需采取缓解措施。
- **权限升级：** 过时软件中的漏洞可能会被利用，从而为威胁行为者提供进入设备的途径，进而进入网络。

不仅仅是保护资源

在谈到弥补安全漏洞时，安全专业人员在设想各种降低风险的方法时会自然而然地产生这样的想法。完善补丁管理流程，使软件和操作系统始终保持最新并抵御已知威胁是一个普遍的想法。另一种方法可能是拥抱最近的人工智能（AI）趋势，将机器学习（ML）技术纳入安全堆栈，以更快地响应事件或通过自动化简化威胁捕猎。

虽然这些都是弥补安全漏洞的绝佳方法，但除了实施更新的控制措施来更好地保护设备、用户和数据的安全之外，还有其他一些因素。这些基本要素虽然不像技术或逻辑控制那样华而不实或 "有趣"，但通过精简、自动化和整合构成整体安全战略的程序、流程、工具和工作流程，为企业带来价值。此外，它还将所有这些要素与负责确保设备、用户和数据合规并高效运行的 IT 和安全团队汇聚在一起。

在本节中，我们将深入探讨这些要素，并将其称为 "四个合"，以强调它们如何相互配合，在最大限度地提高效率的同时，最大限度地减少对企业整体安全态势的挑战。

合一

在企业安全方面，各组织应同等对待所有用于工作和连接业务资源的设备类型，以及在这些设备上运行的各种操作系统。毕竟，如果一家公司向员工发放 Windows 计算机，并部署终端安全控制以确保计算机的管理和安全，但却没有实施移动威胁防御，以保护业务数据不受同一员工使用未经批准的移动设备的影响，这实际上会使他们面临可能导致数据泄露的移动风险。

尽管 Apple 的设计是安全的，而且 Apple 加倍努力保护用户的安全和隐私，但威胁者还是会像攻击 Windows 或 Android 设备一样，经常攻击 Apple 设备（macOS、iOS 和 iPadOS）。合一的问题不在于只关注每个操作系统与其他操作系统的不同之处，而在于它们的相似之处。毕竟，台式机、笔记本电脑、平板电脑或智能手机尽管占地面积不同，但仍是计算工具的典范，它们在操作核心上的共同点要多于视觉差异的总和。

这就是合一的关键所在：
对访问企业资源的所有
终端一视同仁——无论：

- 设备类型
- 外形尺寸
- 操作系统
- 应用和服务

合规

遵从的定义是屈从于愿望、要求、建议、制度或胁迫的行为或过程。

根据企业所处行业的不同，合规可能具有不同的含义。对于受监管行业，有专门的法律规定应如何确保数据、流程和工作流的安全，以防止受保护数据类型的泄漏。 对于不受监管的行业，企业可能有自己的合规要求。其中一个可能与内部业务政策相一致，和/或与他们希望业务运营遵循的标准或框架相联系。或许两者都有。

谈到合规，因为它涉及到消除安全漏洞，这意味着要解决两个突出问题：

使用基线

第一点是基线。更具体地说，它们的创建是为了确定基础设施正常运行水平的界限。由于基线 的设计，基线还为管理员提供了一个分界点，当终端偏离基线的可接受参数时，基线会向管理员发出警告，表明 可能已经不符合要求。

向审计员提供证据

无论贵组织是派遣内部审计员，还是作为监管义务的一部分接受独立第三方审计，都需要某种形式的证据来证明合规性得到了维护。在证明终端合规时，审计人员的一般经验法则也适用于此："如果没有记录，就说明没有发生"。

管理基线和收集审核证据的关键在于遥测数据。它为管理员提供了终端健康状况的可视性，并可随时参考，以深入了解用于访问、处理、存储、修改、传播或共享公司数据的设备是否符合安全计划或监管治理所规定的准则或要求。

合并

第三个 "合 "也是最容易被误解的一个，因为它常常被误认为是指解决方案的整合。

> "网络安全远不止是 一个信息技术问题"。
>
> — Stephane Nappo

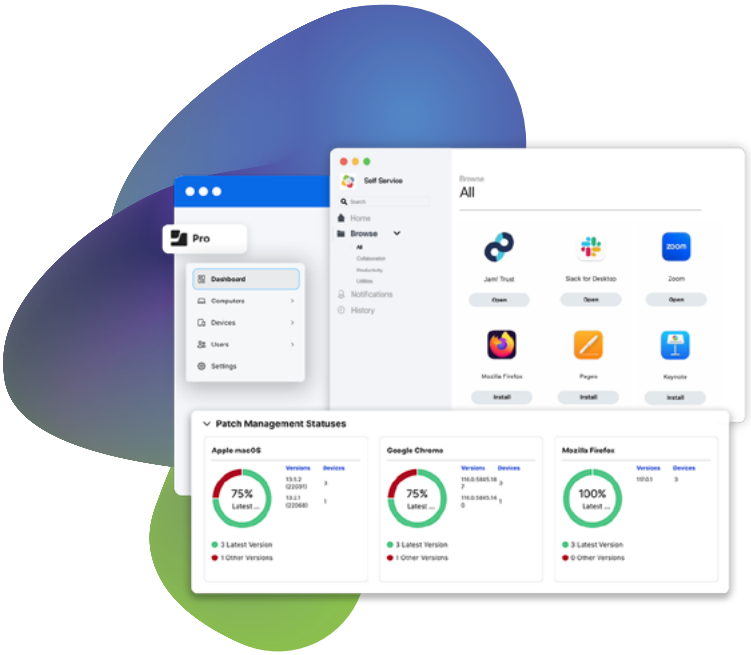
这里所说的 "合并 "是指将信息技术和安全专业人员合并成一个有凝聚力的团队。这改变了两支队伍各自为战的局面。尽管这两个部门都属于信息技术的范畴，但出于各种业务原因，企业通常会将这两个部门的业务分开。

考虑到现代威胁形势，这种操作方法的问题在于每个部门都要管理自己的一套软件、供应商合作关系、流程、政策和工作流程。从理论上讲，它们的不同方法都是为了加强设备和整个组织的安全态势。但实际情况往往是，这种结构取得的效果恰恰相反。

有效的整合需要对网络安全架构和流程进行现代化和整合，以便：

- 集中最佳解决方案，原生管理支持的平台
- 减少供应商和合作伙伴的数量
- 打破各自为政的局面；加强信息共享
- 通过建立知识管理实践，消除把关现象
- 整合管理和安全方法
- 统一威胁预防，加快事件响应
- 将保护扩展到整个基础设施

通过转向综合安全+管理方法，企业管理员的任务是确保设备和用户在访问和处理敏感业务数据时始终受到全面安全的保护，并在企业资源中进行整体扩展。



合算

在 IT 和安全协作的同时，还应考虑投资回报率（ROI）的重要性。如果企业选择的解决方案 "最适合 "持续满足其在合规道路上的独特需求，那么投资回报率的一个特别之处就是可以节省成本。这不仅需要了解解决方案相对于成本的价值，还需要平衡其他因素，这些因素对与深度防御战略相关的投资回报率有着直接（和间接）的影响。

影响投资回报率和更大安全战略的一些直接和间接因素包括：

- 选择既能为组织内的设备和操作系统类型提供原生支持，又能整合形成整体解决方案的工具
- 将耗时的手动任务自动化，提高效率，同时解放管理员，使其专注于增值项目
- 简化安全流程和工作流，将其扩展到整个基础架构，并对其进行优化，以大规模支持终端和应用程序
- 降低解决方案和事件响应之间的复杂性，最大限度地减少安全事件的发现和修复时间 = 减少停机时间，提高生产率
- 主动监控和报告使管理员能够实时掌握丰富的遥测数据，在合规性受到影响之前主动检测/纠正风险向量，从而在合规性受到影响之前主动检测/纠正风险向量

另一个与节约成本和现代威胁形势有关的考虑因素涉及工作中使用个人拥有的设备。许多组织正在实施 BYOD 计划，特别是在远程/混合环境中，以便与团队成员保持联系和协作。毫无疑问，BYOD 对雇主大有裨益，这也是 Zippia 最近报告 称美国近 **70%** 的 IT 决策者赞成 BYOD 计划的原因所在。

96% 连接到企业网络的移动设备为个人所有

80% 的企业高层领导认为移动设备是员工工作的必需品

可穿戴技术增强的员工人数将增加**30%**

对于实施员工选择计划的组织来说，这也是一个福音，允许员工选择他们认为最高效的硬件和软件，而不会对购买和维护数百、数千甚至数万台移动设备的库存以及电脑产生财务影响。这就为我们带来了巨大的优势和成本节约。

深度防御：有效的分层安全

美国国家标准与技术研究院（NIST）将深度防御（DiD）定义为 "整合人员、技术和运营能力的信息安全战略，在组织的多个层面和任务中建立可变的屏障"。

将其应用到网络安全计划中，会产生额外的保护措施，从而加强您的安全态势。但这种分层控制的方法可以说为组织提供了一个安全网。一种是实施权宜之计，防止企业资源受到威胁。如果威胁绕过了某一级别的控制，那么在攻击路径上遇到的下一级控制就能在风险演变成影响合规性的事件之前将其捕获并降低风险。

我们在本节中回答的一些问题包括：

- 整合对企业网络安全计划有何整体影响？
- 为实现 DiD，可以实施哪些类型的综合安全控制？
- 启用 DiD 的网络安全计划对满足合规要求有何影响？

管理 + 身份 + 安全

您可能对管理、身份和安全等设备管理概念并不陌生。就其本身而言，每一个都被视为基础要素，主要提供与各自类别相关的一套特定技术和最佳实践：

- **设备管理：** 计算机和移动设备的管理，包括管理设置、部署安全配置、安装软件和执行策略。
- **身份和访问：** 一个政策和技术框架，确保经过身份验证的用户和/或授权设备根据分配的权限获得必要的受保护资源访问权限。
- **终端安全：** 基于软件的技术，旨在最大限度地降低风险，保护设备和用户免受威胁和攻击，同时保护资源。

在设计丰富、深入的网络安全深度防御计划时，这三个基本要素的整合就起到了基石的作用，可确保企业资源免遭未经授权的访问，最大限度地减少终端风险载体，并保证用户的安全和生产效率。

在下面的章节中，我们将深入探讨一些技术，这些技术不仅可以通过集成使其成为可能，还能突出显示它们是如何最大限度地降低风险、防范恶意软件以及检测和减轻高级威胁的：

- 零接触部署
- 威胁捕获
- 零信任网络访问（ZTNA）
- 高级威胁响应

零接触部署：从一开始就确保安全

安全通常是一个被动的过程。“事件响应” 这一名称反映了等到发现威胁后再进行处理的反应性质。比如因果关系。

虽然管理员无法改变这种因果关系，但可以采取一些措施来减少攻击面，从而最大限度地减少威胁可以影响设备的 "方式 "和 "地点"。

还有什么比第一次打开设备电源更好的起点呢，对吧？这就是配置和零接触部署的神奇之处.....在管理 Apple 设备时，尤其容易利用零接触部署的优势。

这是因为企业零接触部署依赖于在初始设置屏幕上主动向设备提供管理和身份与访问工作流。具体来说，就是在用户使用企业凭据成功进行身份验证、完成设备注册并安装管理配置文件后。MDM 会立即开始部署用户完成工作所需的一切，并按照组织标准配置设备。

在零接触配置阶段可以部署什么？

- 加固设备安全
- 安装受管应用程序
- 配置应用程序设置
- 分配用户账户
- 策划自助服务选项
- 更新系统补丁
- 部署安全软件
- 设置强制策略

您可能会想，这对公司拥有的设备来说很好，但 BYO 设备呢？

零接触工作流程可扩展到任何所有权模式，包括个人拥有的设备。针对这些情况，Apple 公司设计了 " 用户注册 "功能，以便在不牺牲公司安全保护措施的情况下维护用户隐私。

用户主动将个人设备注册到企业 MDM 的部分功能如下：

- 安全访问机构资源，如电子邮件、联系人、日历、Wi-Fi 和加密网络连接
- 业务数据存储在设备的独立加密卷中，个人数据不受影响
- 可以使用两个 Apple ID：一个个人 ID 用于个人数据和设置，另一个管理式 ID 用于机构数据
- 管理员只能查看、访问和删除 BYO 设备中的机构数据；个人数据和隐私数据仍无法访问，也不会受到影响
- 实现整个企业的安全标准化，确保所有设备保持相同的保护级别，而不管其所有权级别

威胁捕获：主动 > 被动

在管理团队有权执行的更专业的任务中，事件响应是其中之一。当终端安全软件提醒管理员恶意行为或威胁被标记时，即可开始检测和归类潜在问题。派遣响应小组确认、控制并最终修复问题。

虽然解决已知问题对响应者来说是理所当然的，但通过集成管理和安全解决方案以增强工作流程和过程，还可以增加一些组件，将主要是被动的过程转变为主动的过程。

建立安全基线

与网络安全有关的基准是指企业终端的正常运行。建立基线需要的不仅仅是测量性能，还包括安全配置、设置、终端安全软件、应用程序和服务，简而言之，就是用户安全可靠地履行工作职能所必需的东西。这也意味着遵守合规要求和/或与公司政策保持一致。

预防已知威胁

通过设置和捕获必要的参数作为基线，管理员可以更好地确定终端健康状况是否在可接受的范围内。如果没有，终端日志将提醒管理员注意任何差异，同时提供手动缓解的机会。或者，在与您的管理解决方案进行配置集成的情况下，两个解决方案之间共享的遥测数据将触发自动工作流的执行，对事件进行补救。

检测未知威胁

主动与被动是技术的核心主题，也是在威胁不断融合和演变的情况下保持终端管理和安全的关键。其中一种主动边缘化的做法就是威胁捕获。

有效完成这项任务需要

- 为您的环境提供出色的数据存储能力
- 强大的数据分析和模式识别技能
- 对硬件和软件的深入了解
- 强大的安全工具及使用方法
- 调查未知问题的时间、耐心和勤奋

ZTNA：永不信任，始终验证

随着时代的进步，曾经被认为是最前沿的技术逐渐被淘汰、过时，最终完全停产，取而代之的是更快、更好、更强的技术。零信任是一种安全模式，它能以 VPN 等传统技术无法解决的方式应对现代威胁环境的挑战。

以下是集安全、身份和管理于一体的 ZTNA 建立网络安全新范例的几种方式。

阻止网络威胁

作为一名技术专家，您肯定对防火墙不陌生。也就是说，它们的用途和功能。虽然防火墙是一种功能强大的设备，可提供基于边界的安全防护，抵御基于网络的攻击，但考虑到如今工作队伍向分布式迁移，并依赖于个人设备开展工作，保护局域网边界的防火墙对于保护远程工作的员工及其不受管理的个人设备并无太大作用。ZTNA 可在设备上和网络内提供保护，防止威胁和攻击。不仅如此，它还能在多个平台上提供保护，使运行 macOS、iOS、iPadOS、Windows 或 Android 操作系统的电脑和移动设备的安全性标准化。

隔离和加密连接

ZTNA 还对任何网络连接上的隧道进行加密，并通过始终保持开启状态进一步确保其安全性，甚至在用户或恶意软件禁用时自动启用。此外，ZTNA 还通过与身份和访问管理的集成增加了另一层保护：每次与受保护资源建立连接时，ZTNA 都会为该特定应用程序或服务生成自己独有的微隧道。这不仅能阻止使用公共热点时常见的中间人（MitM）攻击，还能防止网络横向移动，因为微隧道之间是相互隔离的。最后，它执行最小特权原则，要求用户进行身份验证，但允许他们明确访问分配给他们的资源——默认情况下拒绝访问网络基础设施的所有其他部分（与传统 VPN 不同，后者一旦通过身份验证就允许访问整个网络）。

验证终端健康状况和访问请求

零信任模式要求每次发出请求时都要验证终端和凭证的健康状况，而不是隐性地 "信任 "设备。它将终端当前的健康状况与组织可容忍的健康状况进行比较。如果两个检查点都通过，则允许访问请求的资源。如果身份验证或设备健康状况均不合格，则继续拒绝访问（默认行为），并部署补救工作流以纠正任何差异。补救完成后，再次执行检查点。只有在设备和凭证通过验证后，ZTNA 才允许访问请求的资源。

这并不重要无论移动设备：

- 是公司发放还是个人所有
- 是连接到公司网络或公共热点
- 通过设备检查点，但未通过证书检查点

也没有关系，如果用户账户：

- 属于特定的工作角色，如首席执行官或行政主管
- 一小时前或五分钟前认证成功
- 通过凭证检查点，但设备检查点失败

"永不信任 - 始终验证 "表示默认情况下禁止访问。设备和凭证必须通过验证：每次请求都必须通过验证。

高级威胁响应：执行级保护

高级持续性威胁（APT）已经激增，目标是全球所有行业的组织。

在本节中，我们将讨论管理员在集成安全和管理解决方案时可能遇到的防御问题。凭借在这两种工具之间收集和共享的威胁情报数据，更全面的解决方案可提供强大的威胁响应和对高级威胁的修复，这些威胁越来越多地针对关键员工/角色目标网络攻击，例如首席执行官和其他高风险个人。

集成安全性和管理以降低高级威胁风险的主要优势包括：

获取移动攻击的可见性

移动威胁呈上升趋势。现代威胁环境不断演变，威胁直指移动设备，并逐年向移动设备用户倾斜。

但是，不要只听我们的一面之词，以下是一些 关键的研究结果 ，从数字上证明了我们的说法：

- 在所有被入侵的设备中，**43%** 的设备被完全入侵（未越狱或 root），同比增长 **187%**
- **80%** 的网络钓鱼网站专门针对移动设备，或者旨在同时在桌面和移动设备上运行
- 2022 年发现的关键 Android 漏洞增加了 **138%**，而 Apple iOS 占了 **80%** 的零日漏洞被积极利用
- 移动应用程序中不正确的云存储配置是主要的攻击面。 **±2%** 的 iOS 和 **±10%** 的 Android 移动应用访问了不安全的云实例
- 独特的移动恶意软件样本总数增加了 **51%**，检测到超过 **92 万**份样本

主动监控和可见性是深入了解移动攻击的关键。不仅要识别它们，还要了解访问企业资源的终端健康状况，并在被威胁者利用之前将风险因素降至最低。

完成任务后，终端安全解决方案会重新扫描设备，以确认威胁缓解情况。如果成功，则允许访问公司资源；如果不成功，则继续拒绝请求，并可能需要采取额外的补救措施。

消除先进的持续性威胁

> **“一盎司的预防胜过一磅的治疗。**
>
> ——Benjamin Franklin

了解威胁状况意味着要认识到，虽然预防威胁远比应对威胁更重要，但如果我们不指出有时威胁会影响设备并对网络造成影响，那就太失职了。说到 APT 背后的复杂程度，更多的是终端 "何时 "而非 " 是否 "会受到影响的问题。能否快速转向的关键在于团队的准备程度。为此，他们应对 APT 的准备程度无疑会受到他们正在使用的工具以及他们用于修复高级威胁类型的数据质量的影响。

安全与管理在此交汇，以创建先进的程序和工作流程：

- 侦测可疑行为
- 向管理员发出事件警报
- 评估威胁的入侵指标（IoC）或攻击指标 （IoA）
- 分析来自多个威胁情报来源的调查结果
- 验证威胁是否为真阳性
- 部署缓解战略
- 必要时执行补救任务
- 扫描设备以验证合规性

根据威胁的严重程度，安全与管理之间的集成可以增强人工执行的事件响应流程，也可以由集成解决方案提供商自动执行。

将调查时间从几周缩短到几分钟

并非所有威胁都是一样的，最近的一些威胁和概念验证（PoC）攻击所显示的复杂程度越来越高，这就要求响应团队和威胁猎手进行更深入、更彻底的调查，以发现未知威胁的全部影响。以往，调查可能需要数周时间才能完成，这取决于威胁的严重性和复杂性。

先进的威胁需要先进的工具，以 高效的方法检测和应对移动设备上的事件和攻击 。鉴于这些终端的 "移动 " 特性，事件响应必须能够远程执行，不仅要发现移动攻击，还要对移动攻击做出响应：

- 进行深入分析以识别 IoCs
- 构建可疑事件的时间线，显示设备何时以及如何被入侵
- 提供简单明了的事件摘要，揭示复杂的零日攻击（否则会被隐藏起来）
- 利用内置工具消除 APT，同时持续监控确保威胁被摧毁

摘要

要弥补安全漏洞，就必须采用现代网络安全方法。分层全面保护，将安全性和隐私性全面扩展到基础设施中的所有设备、用户和数据。集管理、身份和安全于一体的单一、强大的深度防御解决方案。

© 2024 Jamf, LLC. 保留所有权利。