混合Active Directory网络抗风险能力现状

本报告基于最近对430位Quest客户和Active Directory (AD)用户的调查，旨在探索组织目前在AD安全方面面临的难题

Quest

当今的组织如何处理Active Directory安全性问题，他们在哪些方面遇到了最大的难题？

为了回答这个问题，我们通过The Experts Conference (TEC)在2023年9月开展了“混合Active Directory网络抗风险能力现状”调查，收到了超过430份来自IT专业人员和IT高管的回复。

主要收获很有启发性：

绝大多数IT专业人员都知道他们应该关注哪里，以及如何更好地保护他们的组织 — 他们只是并不总是拥有相应的资源和支持来做到这一点。

我们的三大调查结果：

1. IT团队表示，他们面临的首要难题是识别和限制安全风险，包括不当配置。
2. IT团队知道，优先考虑第零层资产（控制平面）的安全模型对于保护其组织最关键的IT资产是有效的，但该模型基本上没有得到利用。
3. IT组织没有足够的人员来支持其所有AD安全需求，而预算缩减并不是唯一的原因。

主要调查结果1：IT专业人员面临的首要难题是评估风险敞口。

到目前为止，IT专业人员遇到的最大难题是识别错误配置和其他风险。查明这些弱点对于Active Directory安全至关重要，因为它们会为外部攻击和内部威胁打开大门。

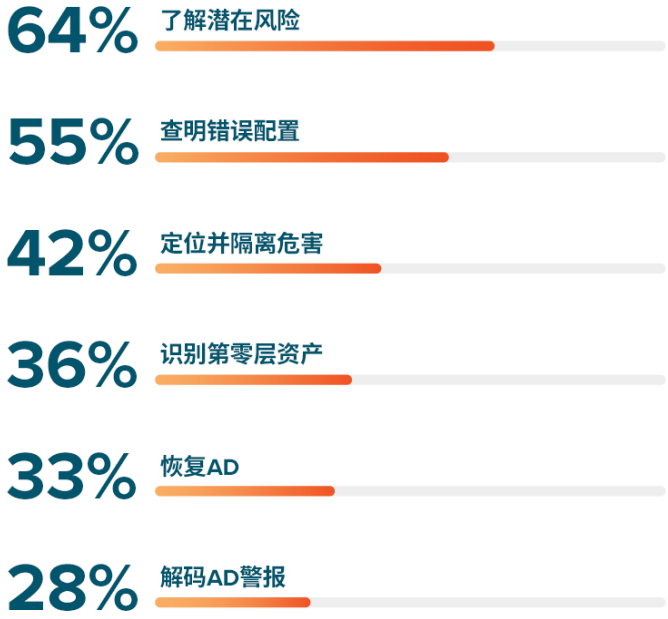
在您的角色中，哪些与AD安全相关的问题让您夜不能寐？

“平台的安全状况和网络安全弱点、威胁检测和攻击路径模式、潜在网络安全事件、跟踪使用该平台的应用程序和基础架构的能力、与Entra ID (Azure AD)平台的混合集成、AD平台恢复和恢复后流程。”

高级基础架构工程师 – 身份服务 – ETS – 技术和创新，大型企业专业服务公司

uevi.co/7780VLXB

当今组织中与AD安全相关的首要难题包括：



uevi.co/6201DFAN

主要调查结果1：IT专业人员面临的其他主要挑战是威胁检测和AD恢复。

IT从业人员还表示，很难检测到安全危害和理解警报。这些任务对于及时消除威胁以限制其影响至关重要。

此外，IT专业人员在灾难后很难恢复Active Directory，而这项任务对于网络抗风险能力至关重要。事实上，如果没有合适的工具，恢复AD可能需要数天或数周的时间，在此期间，业务将陷入困境。

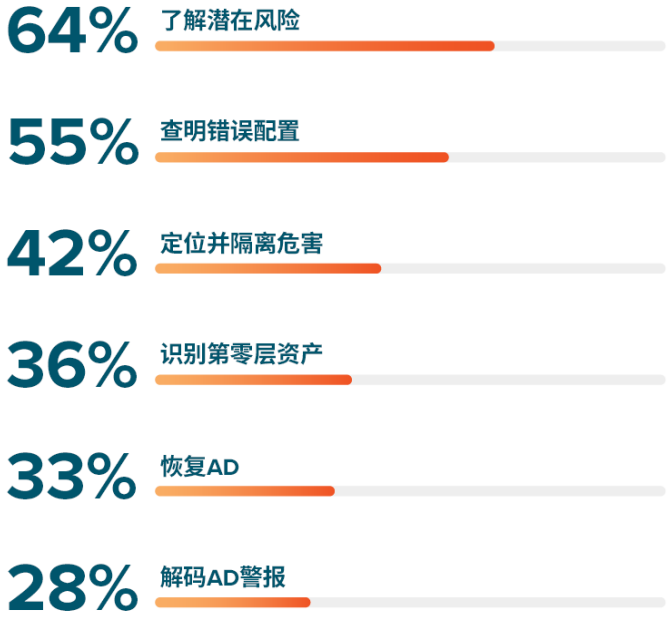
在您的角色中，哪些与AD安全相关的问题让您夜不能寐？

> **快速识别外部来源的未经授权的入侵，并可在检测后实现恢复。**

大型企业专业服务公司

uevi.co/4949XYWI

当今组织中与AD安全相关的首要难题包括：



uevi.co/6201DFAN

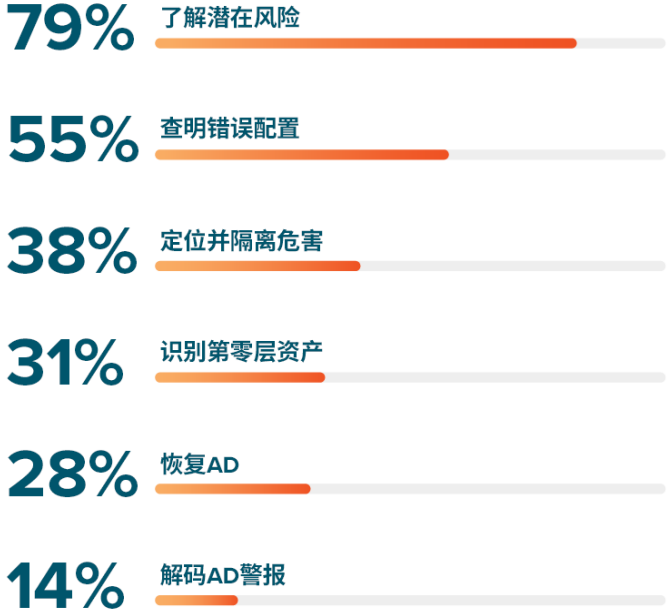
主要调查结果1：IT高管提到了同样的问题，但更关心风险。

IT专业人员和IT高管有着不同的关注领域，因此他们在优先事项上并不总是一致。但是谈到AD安全难题，他们的看法一致：两个群体以完全相同的顺序对主要问题进行了排序。

显著差异之处是反应强度。近8/10的IT高管表示，评估风险是一大难题，而持相同看法的IT专业人员的比例为64%。

然而，这并不奇怪：IT高管敏锐地意识到，未能解决AD风险可能会对公司品牌造成严重而持久的损害。没有人愿意成为新闻中下一次毁灭性网络攻击的受害者。

79%的高管表示，“评估潜在风险”是他们面临的首要AD安全难题。



uevi.co/1457CVQW

主要调查结果1：为什么IT团队如此担心AD安全风险?

为什么从实际操作人员到高管在内的整个IT团队都如此担心AD安全风险?

答案很简单：Active Directory已经存在了20多年，随着时间的推移，AD部署的规模和复杂性都呈爆炸式增长。因此，在AD中找到暴露指标(IoE)、确定其优先级并了解如何修复它们以限制攻击面并非易事。

与此同时，对手花了几十年的时间来发现该平台的弱点，并磨练利用漏洞进行攻击的能力。

这也难怪“网络抗风险能力现状”调查发现，无论组织规模或行业如何，评估暴露风险敞口都是IT从业者和IT高管最关心的问题。

在您的角色中，哪些与AD安全相关的问题让您夜不能寐?

> **AD已有20多年的历史，攻击者对它了如指掌，这使得为其提供保护非常困难。**
>
> *大型企业媒体公司身份与协作副总裁*

uevi.co/6668BKWD

主要调查结果1：哪些AD问题令您的同事感到担忧?

在您的角色中，哪些与AD安全相关的问题让您夜不能寐?

> **对变更的管理不当，访问不当，这些本质上都是人为错误问题。**

高级技术官，
中型企业多元化金融服务公司

uevi.co/6712HKTU

> **内部威胁、心怀不满的员工或对恶意软件放任不管的终端用户。**

网络防御高级经理
大型企业航空航天与国防公司

uevi.co/6008BWMF

> **特权帐户数量过多，而且依赖信任升级权限和授予访问权限。**

大型企业专业服务公司首席工程师

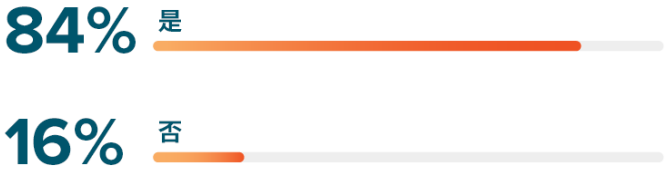
uevi.co/5976HYGO

主要调查结果2：IT专业人员非常清楚，优先考虑第零层至关重要...

十年来，Microsoft一直在推动组织采用以第零层为中心的AD安全模型。第零层包含组织所有最关键的IT资产，包括域管理员等特权帐户和域控制器(DC)等关键服务器。

在调查中明确收到以下信息：84%的调查受访者表示，他们了解第零层对于确保网络安全和网络抗风险能力的重要性。

84%的受访者了解AD第零层结构（或控制平面）在确定最关键IT资产的优先级并为其提供保护方面的重要性。

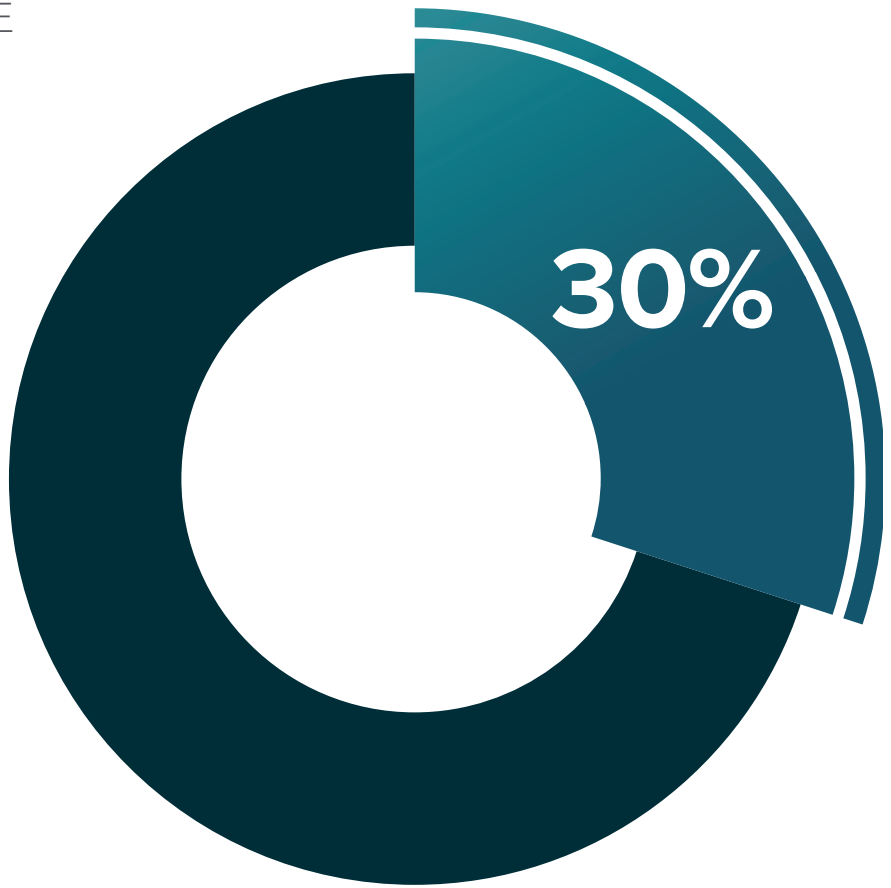


uevi.co/3915HSMV

主要调查结果2：...但只有30%的受访者在使用第零层安全模型。

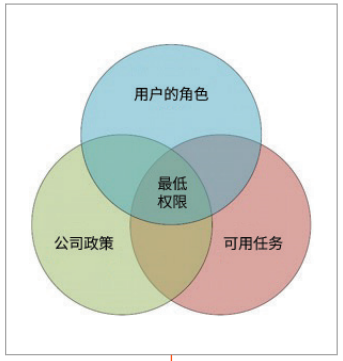
令人震惊的是，只有**3/10**的调查受访者表示，他们正在积极使用第零层结构来保护AD环境的安全。

uevi.co/9945VLXB



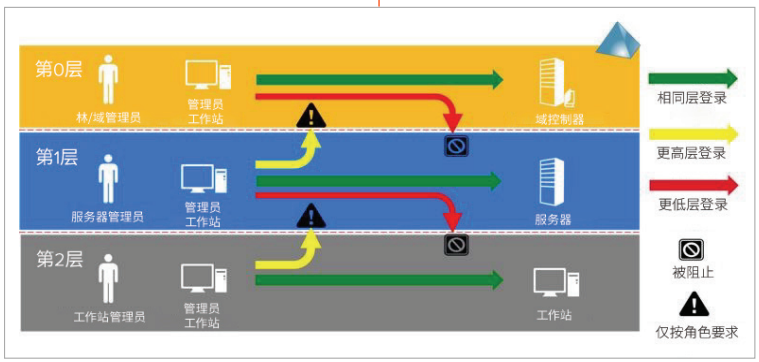
主要调查结果2：安全目录管理的演变

1999年：最低特权

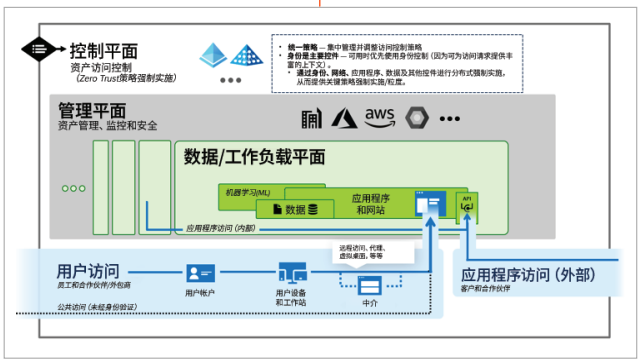


2014年：ESAE/Red Forest

现在



2012年：最低权限



2020年：企业访问模型

主要调查结果2：这些年来目录安全性发生了怎样的变化?

第一个AD安全模型植根于最低权限原则，该原则要求向每个帐户准确授予其所需的访问权限，不多也不少。当然，这一原则仍然是IT安全的基石，但事实是，并非所有IT资产都需要相同级别的保护。尝试均等地锁定所有内容会使其无法随着AD环境规模和复杂性的增长而扩展。

第零层于2012年出现，作为新模型的一部分，其中IT资产根据其保护要求分为不同的层。Microsoft很快将这种方法改进为ESEA (Red Forest)模型，该模型更清楚地说明了第零层应包含哪些内容以及如何对其进行保护。

随后，IT环境开始发生更加巨大的变化，特别是由于云技术的快速采用。为了满足由此产生的安全需求，Microsoft在2020年推出了企业访问模型，这也是它推荐当今大多数客户使用的AD安全模型。

自2012年以来，第零层一直是Microsoft推荐的安全模型的基本要素。

主要调查结果3：IT组织没有足够的人员来支持他们的所有AD安全需求。

现在让我们解决这个极具价值的问题：

为什么组织难以应对诸如评估漏洞、发现主动威胁和确定第零层资产的优先级等重要AD安全任务？

核心原因是，只有一半的IT组织拥有足够的人员来处理AD安全问题。

紧张的IT预算显然是造成人员短缺的因素之一，但完整的原因要微妙得多。

50%的组织表示人员短缺

如今，一半的IT组织无法通过现有的人员配置来满足AD安全需求。

uevi.co/3729DZGY

主要调查结果3：因素A — IT专业人员不堪重负。

超过一半的受访IT专业人员表示，他们的首要任务是抽出足够的时间来完成一天中的所有工作。

当时间已经很紧张时，您可能不会考虑修改优先级和返工流程。因此，几乎没有机会从简单的最低权限模型推进到理解和保护作为现代企业访问模型一部分的第零层。

53%

的受访者表示，他们的首要任务是抽出时间来完成所有AD安全相关的必要管理任务。

uevi.co/2446KRCF

主要调查结果3：因素B — Active Directory方面的专业知识正在消失。

IT人员配置问题的另一个关键方面是，在Active Directory领域拥有深厚专业知识的IT专业人员日益短缺。这里有两个互补的趋势在起作用：

- 许多接受过AD安全培训的人员以及具有特定机构知识的人员已经开始离职或退休。
- 但通常没有人可以替代他们，因为新员工根本没有像前员工那样接受过有关AD安全要求和实践的培训。事实上，Microsoft已经取消了一些重要的AD培训课程和认证，而且未来几年还将取消更多课程和认证。

主要调查结果3：因素C — 通常不清楚谁负责AD安全。

在身份威胁检测和响应(ITDR)方面，只有4/10的组织表示他们的AD和SecOps团队之间达成了一致。因此，组织通常没有明确谁具体负责什么。

此外，17%的受访者表示ITDR决策由IT领导层决定。在这些组织中，一线IT专业人员甚至不太可能支持采用现代AD安全模型等举措。

只有41%

的组织在AD和SecOps团队之间就AD身份威胁检测和响应(ITDR)达成了一致。

uevi.co/2271lWKF

17%

的组织将ITDR决策交给IT领导层/CISO。

uevi.co/9320CFKX

其他值得注意的调查见解

另外两项调查结果也值得注意：

- 不到6/10的组织完全实施了NIST网络安全框架(CSF)，该框架提供了一个有价值且灵活的框架用于加强IT生态系统（包括重要的AD身份基础架构）的安全性。
- 许多组织现在都在密切关注供应链风险管理，这可能是因为毁灭性网络攻击产生的影响，例如侵袭SolarWinds的那一次毁灭性网络攻击波及到数千名客户，从Microsoft、Intel和Cisco等大型科技公司到美国国土安全部、国务院和财政部都深受其害。

只有58%

的组织已全面实施NIST网络安全框架。

uevi.co/1945OEXU

近2/3的组织评估供应链安全性

64%的组织会评估与其供应链中的供应商相关的安全实践和潜在风险。

uevi.co/1897KEWM

建议

如果您的组织面临着Quest调查中所报告的相同AD安全难题，以下是解决这些难题的可靠策略：

通过了解您的第零层资产，准备采用现代安全模型。

不要因为缺乏对第零层资产的了解而阻碍您采用现代企业访问模型。借助第三方解决方案，您可以获得最有价值的IT资产的全面清单，包括所有特权帐户、组策略对象、域控制器和其他关键服务器，例如托管Azure AD Connect的服务器。

发现并缓解使您的第零层面临风险的漏洞。

如果您最近没有进行过AD安全评估，请安排一次评估。了解您环境中的哪些地方最易受攻击是至关重要的事情。这不仅包括错误配置和其他可能让攻击者在您的环境中立足的问题，还包括您的环境中的任何弱点，他们进入内部后可利用这些弱点来升级其权限并横向移动以到达您的第零层资产。确保在应用所有修复程序之前都对它们进行彻底的测试，以避免出现意外后果。

通过与专家合作并选择有效的工具来缓解IT人员配备问题。

网络犯罪分子狡猾而又残忍，因此安全事件几乎不可避免。无论您是否准备好，都不要碰运气。通过与值得信赖的合作伙伴合作并投资涵盖NIST CSF中详述的所有功能的全面AD安全解决方案，您可以赋能有限的IT团队处理全方位的AD安全任务，从漏洞缓解到威胁检测和响应再到灾难恢复都包括在内。