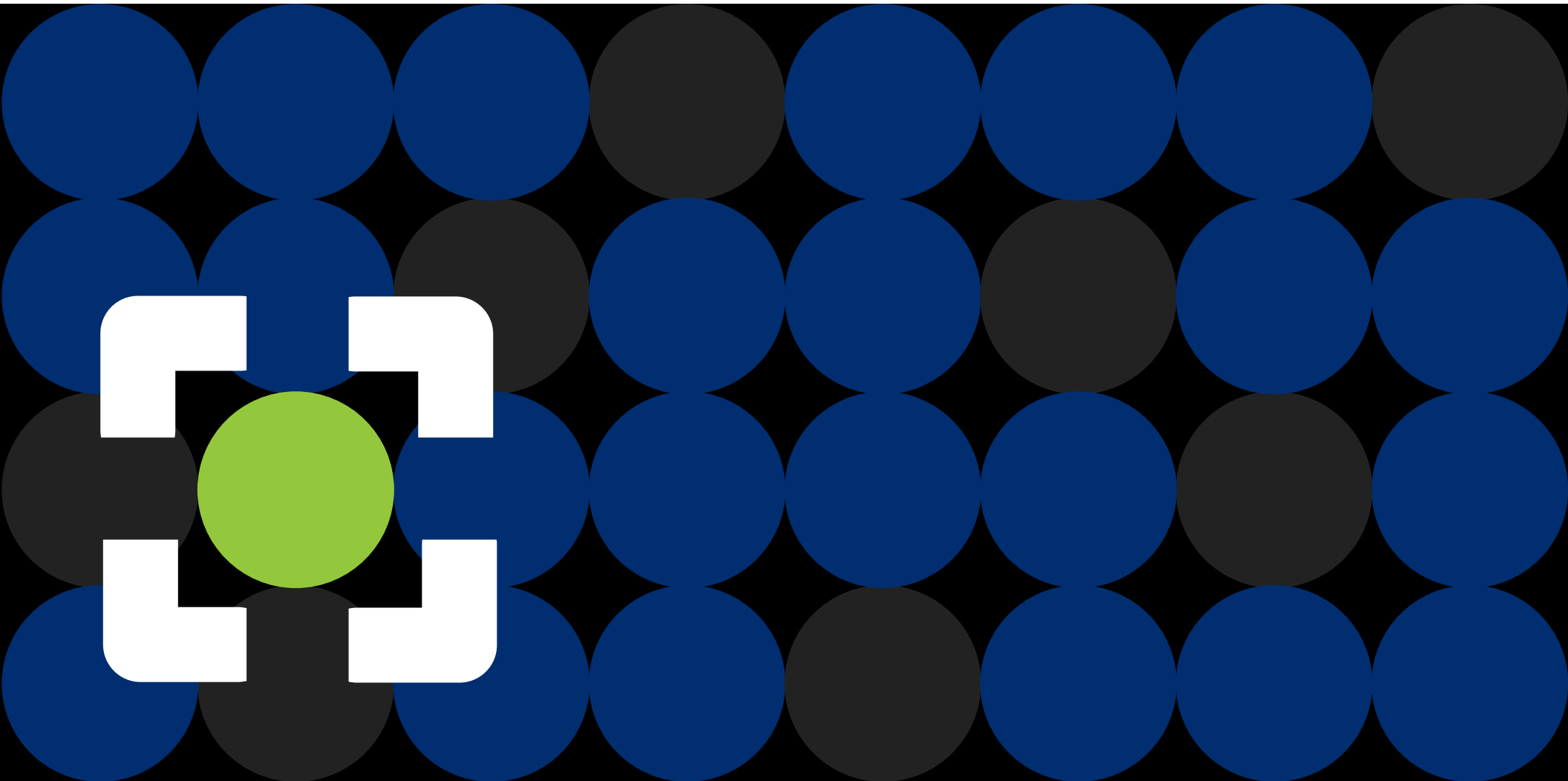
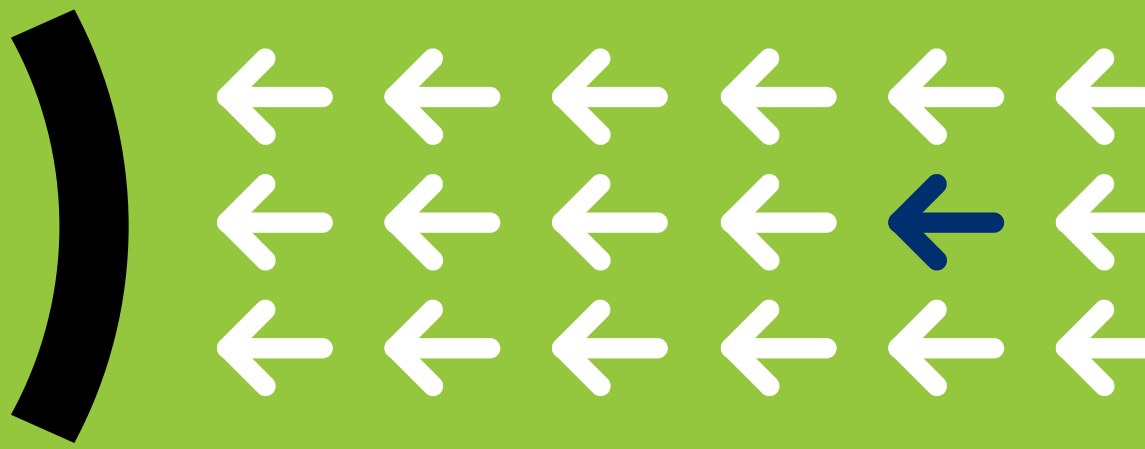
FORESCOUT
Active Defense for the Enterprise of Things™

如何保护物联企业
五大安全挑战



目 录



介 绍

如今企业网络上的设备已经失控。无论是数量（数十亿）还是种类（IT、OT、IoT、BYOD），都在爆炸性地增长。有一些是有托管且已知的，但其他的则无人知晓、无人发现，成了漏网之鱼。至于设备用户，他们遍及天下——这毫不夸张。员工、承包商、合作伙伴和消费者从各处全部连接到数据中心或云端，但安全与否却不能一概而论。

所有这些都让每个网络环境变得复杂起来，成为一个名副其实的物联企业(EoT)，需要缜密的计划和果断的行动来保护设备和企业自身。

接下来是五个关键性的EoT挑战，这是如今的首席信息安全官们和其他安全及运营领导们要思考的，同样还有如何战胜这些挑战的实际建议。

挑 战　1

如何盘点和管理激增的非托管设备？

> **专家们估计，仅2020年一年，全球就会安装310亿台IoT设备。**
>
> **今日安全，2020年1月13日[1]**
>
> **“62%的受访者表示，他们的公司能否实现更成熟的安全态势，将越来越取决于IT和OT控制系统的融合。”**
>
> **波耐蒙研究所，2019年2月[2]**

与加入网络的数十亿无代理IoT和运营技术(OT)设备相比，搭载安全代理的托管设备，如企业自有的PC、笔记本电脑和智能手机，正变得稀缺。IT-OT网络融合也在同时进行——提高了生产力，简化了网络管理，但也增加了风险。掌握当今异构网络的受攻击面比以往更难。

建议：

- 确定哪些工具可以给您提供100%的设备可见性——没有盲点
- 精简您的选择流程，只囊括可提供无代理、实时设备态势评估的解决方案
- 使安全运营和IT员工能够实时盘点资产

挑 战　2

在如今的企业环境中，风险位于何处？

> **“智能建筑、医疗设备、网络设备和网络电话是风险最大的IoT设备群体。”**
>
> **FORESCOUT研究，2020年5月[3]**

> **“IoT和支持网络的设备技术已经给网络和企业带来了潜在的危害……安全团队必须持续隔离、保护和控制网络上的每一台设备。**
>
> **FORRESTER研究，2020年6月[4]**

风险分析的概念正在随着您的受攻击面而改变和发展。最近Forescout物联企业分析认为，IoT设备带来了最大的风险。“它们不仅在监测和控制方面具有挑战性，而且还通过弥合过去存在于网络和现实世界之间的差距创造安全漏洞。IoT设备可以成为进入网络的秘密网关，也可能成为专门恶意软件的主要目标。”[3]

建议：

- 采用多因素风险分析来了解您的受攻击面
- 转向包含零信任的主动防御策略
- 根据风险等级对警报进行优先排序，从而加速威胁响应
- 同样，100%的设备可见性是关键

挑 战　3

网络边界已经消失。现在如何是好？

> **“必须采用新的最佳实践来保护企业网络边缘的安全。”**
>
> **高德纳，2020年5月[5]**

开放且安全？在跨越园区、数据中心、云端和OT环境的网络上如何实现？现在，企业网络已经扩展到世界上任何有工作量和工人的地方，因此，组织周围不存在可防御的边界。我们已经到了边界必须包围每个连接的设备和每项工作的地步。安全始于资产的边缘。

建议：

- 使用零信任等最低权限模式限制访问企业资产
- 对所有访问网络的设备，无论其位于何处，进行持续发现和态势评估
- 对所有本地、BYOD和远程资产实施严格的基于策略的合规措施

挑 战　4

必须要进行细分，但如何正确细分而不影响企业运营？

> **“我们估计，在与我们聊过的公司中，有90%在今年的计划中都有细分项目。这是每个人都想做的事情，但并不总是很清楚要从哪里开始、风险是什么，或者是否值得花钱和为之努力。”**
>
> **FORESCOUT研究，2019年1月[6]**

多年来，网络细分的口碑一直很差。直到最近，现有的细分工具部署起来很麻烦，而且不能跨网络管区，导致业务中断和环境分散。当企业增加新设备并进一步扩展其网络时，问题只会变得更糟。然而，今天，可靠的细分解决方案已经出现。坚持使用易受攻击的平面网络已经失去了意义。

建议：

- 可视化细分，并在部署前模拟策略，以防止不必要的中断
- 确保您的主要解决方案能够简化零信任对任何地方的任何设备（包括IT、IoT和OT设备）进行细分
- 加快在整个企业环境中实施零信任
- 选择一个便于网络细分的现代NAC平台

挑 战　5

如何应对“花小钱办大事”的悖论？

> **“企业在减少零散的网络管理工具集方面取得了进展。然而，64%的企业仍然使用4到10种工具来监测和排除其网络故障。”**
>
> **2020年网络管理大趋势，2020年4月[7]**

> **“董事会层面对安全和风险管理的兴趣达到了前所未有的高度。”**
>
> **高德纳研究，2019年7月[8]**

当公司的安全和网络管理使用零散的、针对具体工作的遗留工具大杂烩时，很难将您的安全运营部门称作一个高效的堡垒或是节约成本的提供者。尽管如此，即使是最好的转型计划也会带来麻烦：即部署迟缓、ROI缓慢、学习曲线陡峭以及对所选解决方案的满意度有限。幸运的是，通过选择正确的平台，您可以让所有相关方满意，包括首席财务官。

建议：

选择一个能够协调现有工具并满足这些标准的平台：

- 快速、灵活、非破坏性的部署
- 快速实现价值和快速的ROI
- 与供应商无关——使用您现有的基础架构
- 避免强制软件或硬件升级
- 提供与领先的IT和安全产品的集成
- 无代理设备发现、态势和风险评估
- 避免802.1X复杂性、部署延迟和成本
- 根据企业的可扩展性适应增长
- 提高安全运营生产力
- 提供无代理的可见性、控制、细分和零信任

这五大挑战背后更大的挑战

我们在这里提到的五个挑战中，每一个都可能令人怯步。但每个挑战，如果得不到解决，都可能导致最终的挑战：网络攻击，从而带来运营问题、数据被盗、品牌声誉受损、巨额罚款、公共安全问题——这样的例子不胜枚举。

预防是关键，这意味着一个有效的解决方案必须能够具有100%无代理设备可见性、持续监测和自动威胁响应。

*注

1.*2020年IoT概述：统计、风险和解决方案，今日安全，2020年1月13日*
2.IT、OT与IIoT互联世界中的安全与隐私，波耐蒙研究所研究报告，2019年2月
3.物联企业安全报告，2020年IoT安全状况，Forescout研究实验室，2020年5月
4.用零信任减轻勒索软件的影响：用零信任原则和技术加强您的防御，2020年6月8日，弗雷斯特研究公司
5.*保护企业的新边界，高德纳，2020年3月27日*
6.*网络细分，Forescout博客，2019年1月*
7.*2020年网络管理大趋势，企业管理协会研究报告，2020年4月*
8.*安全和风险领导者必须准备好回答的五个董事会问题，高德纳研究，2019年7月*

不要视而不见。要保护。

马上联系我们，主动保护您的物联企业。

关于 FORESCOUT

Forescout是物联企业安全的领导者，提供一个整体平台，该平台可以持续识别和细分任何异构网络中的每一个连接事物，并强制其合规。Forescout平台是部署最广泛、可扩展的企业级解决方案，用于无代理设备的可见性和控制。它可以在您现有的基础架构上快速部署，无需代理、升级或802.1X认证。财富1000强企业和政府机构信任Forescout以减少安全事件或违规行为造成的业务中断风险，确保并证明安全合规性，提高安全运营生产力。

forescout.com/platform/eyeSight　　china@forescout.com　　zh.forescout.com

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
美国加利福尼亚州圣何塞，95134

电子邮件 china@forescout.com
电话（国际）+1-408-213-3191
支持+1-708-237-6591

访问Forescout.com了解更多

© 2020 Forescout Technologies, Inc. 保留所有权利。Forescout Technologies, Inc. 是一家特拉华州公司。访问 www.forescout.com/company/legal/intellectual-property-patents-trademarks，查看我们的商标和专利列表。其他品牌、产品和服务的名称可能是其各自所有者的商标或服务标志。版本 08_20