



Zebra安全平台

保护您的 性能优势

互联互通加速了您的业务发展,但也可能使其暴露于潜在的安全风险之中。虽然设置防火墙是一个开始,但面对新出现的复杂威胁,这可能也不是一个万全之策。了解能够为您的组织和数据提供更佳保护的出色实践和企业解决方案。



如何防止阻碍业务发展的安全威胁



安全为当务之急

无论您是在为顾客、病人等服务与否，您都应该并且经常被要求对个人信息保密，如信用卡号码、健康记录、社会保障号码和密码等。



风险会上升

随着时间的推移，这只会变得越来越具有挑战性。例如，物联网和云技术将人和信息联系起来，为您的组织提供了卓越的运营控制和可见性。虽然前景令人兴奋，但也并非没有风险。

到2022年，预计将有500亿台¹设备实现互联，从而使组织和机密数据面临大量漏洞。受高回报和低过失成本（只有5%的黑客被起诉²）的驱使，网络犯罪没有放缓的迹象。



有什么危害？

仅仅一次数据泄露就可能让人付出惨痛代价，让您在生产力和利润方面损失惨重，同时也可能损害您的声誉。

你能做什么？重视安全。即使您的组织有一套安全流程，错误的理解也有可能破坏其可靠性并造成不必要的漏洞。

390 万美元：

数据泄露的平均成本³

25575 条记录：

数据泄露的平均数量³

12 小时：

88%的黑客突破网络安全防御的平均时间⁴

197 天：

一个组织意识到存在一个漏洞的平均时间³

目标：



零售：

80%的在线零售商登录流量被黑客用于窃取数据认证⁵



医疗保健：

第二大目标行业，占网络攻击的15%⁶

不要让错误想法 削弱你的安全防护

尽管有很多安全事件，并且也进行了广泛的宣传，但许多组织仍然对安全感到自满。不要被一种虚假的安全感所迷惑。事实是，如果你发现自己在说这些话，你可能发现自己有麻烦。

“我的组织并没有大到足以成为目标。”

43%的网络攻击目标是小企业。⁶ 黑客利用小企业缺乏资源和知识的弱点。他们甚至可以利用您的组织去获取您与更大组织间的联系。

“我们的网络为我们提供保护。”

一个可靠的安全体系是多层次和不断发展的。锁上大门并不会阻止小偷进入开着的窗户。事实上，一项研究表明，传统的应对措施，如防火墙和防病毒软件，几乎从来没有减缓黑客的速度，但 endpoint 安全技术阻止攻击方面更有效。⁴

“我们没有数据泄露，所以我们的安保工作很好。”

您可能没有意识到已经发生了数据泄露。研究表明，一家公司检测出一个漏洞可能需要197天。³

“我们已经有了一个正式的安全流程。”

太棒了。它是否在不断发展以跟上不断变化的威胁？它涵盖了您当前的技术吗？面对当今老练的网络罪犯，并没有一种一劳永逸的方法。

“安全太复杂了。”

精心设计的安全流程直观且易于实现。让您的员工可以顺畅使用并简化IT管理。

“安全会对生产力产生负面影响。”

不满的情绪，如安全系统过于繁琐，难以整合或拖延行动，都太普遍了。然而，一个漏洞可能使工作戛然而止，令人难以承受。解决方案是选择在设计中嵌入安全性的技术。这就是安全可以支持而不是阻碍生产力的方式。



通过多重防御 保护您的组织

可能并不是所有的安全措施都能满足您的需要。在考虑采用的技术时，请考虑Zebra Technologies固有的这些关键安全特性，并保持心态平和。



内置保护和出色性能：

选择旨在将安全性和生产力融入技术的品牌。您会发现，我们的解决方案旨在提高您的性能，同时与一系列高效的安全协议和功能顺畅集成。



轻松集成：

您可以利用Zebra获得平稳快速的集成体验。我们对您的行业 and 应用程序进行了深入了解，因此，我们的设计原则是对您的集成需求进行预测并满足集成需求。



自动安全功能：

曾经，您的IT部门可能需要花费几周的时间才能完成Wi-Fi认证。现在，您可自动完成该认证，为您和您的团队加速提供安全的连接环境。



持续的警示和支持：

将多年的操作系统安全更新和硬件提升与故障排除、漏洞评估和内部安全协作相结合。



可根据您的需要定制：

更想自己设定安全级别？Zebra提供了可配置解决方案，可根据您的公司或部门的需要调整安全级别，从而使您轻松实现这个目标。



遵循出色实践：

请放心，Zebra遵循了世界安全专家（包括ISO、国家标准与技术研究所（NIST）和互联网安全基准控制中心）制定的出色实践和指南。我们的产品和解决方案用于帮助组织遵守HIPAA、PCI-DSS和GDPR等的应用程序之中。



更简单的维护和服务：

相信我们的安全设置、软件和硬件已经开发和测试，以实现更少维护和更长的正常运行时间。另外，如果您需要，我们还有24小时服务响应团队。



在安全企业技术领域表现出色：

为企业强化了 Google Android 操作系统，并提供长达十年的安全操作系统支持。从我们强化的企业移动数据终端到我们安全的打印机和有远的技术，您会发现提升生产力和安全性是我们工作的核心。

Zebra产品、解决方案和服务支持NIST网络安全框架的不同阶段

识别	风险管理监控 打印机安全评估向导 专业服务	供应链风险管理 安全委员会
保护	LifeGuard™ for Android 用于Android打印机保护模式 设备管理	PrintSecure更新 自动Wi-Fi证书管理风险管理框架 风险管理框架
检测	Printer Profile Manager Enterprise 安全监控	实时检测
回应	设备管理 威胁探测对策	事件响应 客户警报
恢复	专业服务 增强	恢复到已知状态





保护您的性能优势

安全性对您的业务和工作流非常重要。这就是为什么Zebra通过将多层保护集成到我们的解决方案中,主动防范安全漏洞的原因所在。Zebra设备、技术和服务的设计都考虑到了安全性,并保持您的工作效率。你会发现您的一线员工可轻松部署并利用我们的安全措施。通过我们的智能可配置技术,您可以在现实世界中实时平衡操作目标 and 安全性。依靠Zebra提供的安全服务,帮助您在边缘实施业务和技术战略。



了解我们的安全措施如何提升您的安全防护

请访问 <http://www.zebra.com/product-security>

来源:

1. Juniper Research, 2018 2. Carbon Black Incident Response Threat Report, Nov. 2018 3. Ponemon Institute, 2018 and 2019 Cost of Data Breach 4. Black Report, Nuix 2017 5. Shape Credential Spill Report 2018 6. Verizon 2019 Data Breach Investigations Report

ZEBRA 和其标志性的斑马头像是 Zebra Technologies Corporation 的注册商标,已在全球多个司法管辖区注册。所有其他商标均为其各自所有者的财产。©2023 Zebra Technologies Corporation 和/或其关联机构版权所有。保留所有权利。