重新思考 IT 安全性指南

应对不断变化的 IT 形势带来的安全挑战

vmware®

定义数字化转型时代

如果我们看一看近年崛起的那些生来就实现了数字化的企业（比如 Uber 和 Airbnb），我们就会发现技术是如何助力这些企业形成竞争优势的。例如，Uber 在不拥有一辆车的情况下成了全球最大的网约车服务提供商；Airbnb 在不拥有任何不动产的情况下成了全球最大的酒店业务提供商。

重塑传统企业

与此同时，我们还可以看到技术在如何转变更为成熟的传统企业。例如，制造公司发现，有必要采用软件方式来提高运维效率和生产效率。General Electric 的董事长兼首席执行官 Jeff Immelt 简明扼要地指出：“我们认识到，工业企业可能会在一夜之间成为软件企业。”GE 和其他企业了解的情况是：当今业务环境中的竞争已转变为数字化业务之争。

安全挑战评估

伴随着数字化转型趋势的高涨，使用数字设备的终端用户数以及必须接受管理的应用和数据量也呈现持续的爆炸式增长。这一现象致使 IT 组织面临一场安全威胁的“完美风暴”。曾经安全地部署在本地的数据中心已发展为高度动态的、由公有云和私有云混合而成的多种云环境。曾经通过企业桌面工作的用户时常在工作场所之外移动办公，希望通过自己的设备，甚至通过物联网 (IoT) 来访问公司网络。

风险不断升高

由于这些因素的存在，风险也在不断增大。老练的攻击者纷纷试图利用这些数据中心漏洞。在近期对全球企业 IT 安全性进行评估的一项问卷调查中，75% 的受访者认为他们在 2016 年可能会遭受网络攻击。[1] IT 组织还要面对不断增长的法规遵从性需求。实际上，IT 员工需要将高达 20% 的时间用于处理合规性职责。[2]

在这种不断变化的 IT 形势下，我们可以清楚地看到安全挑战是什么（尽管解决它们并非易事）：如何保护用户、应用和数据之间的交互?

造成的影响不断加剧

- 2016 年，数据中心故障所造成的平均损失上升至 740,357 美元。[3]
- 包括知识产权遭窃、全球网络间谍活动造成的损失在内，企业每年的损失高达 1 万亿美元。[4]
- 2016 年，数据泄漏所造成的平均损失上升至 4 百万美元，或者每条丢失或被盗的记录造成的损失为 158 美元。[5]

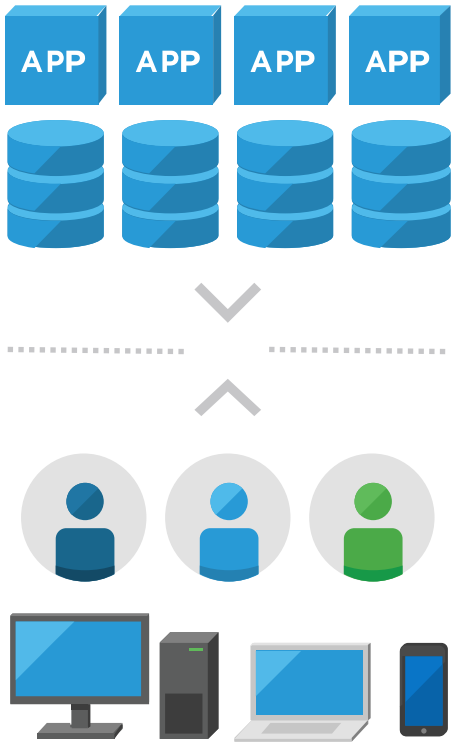


图 1. “数字化转型影响 IT 和安全性”

[1] State of Cybersecurity: Implications for 2016，ISACA，2016 年。
[2] Cost of Data Center Outages，Ponemon Institute，2016 年 1 月。http://datacenterfrontier.com/white-paper/cost-data-center-outages/。
[3] Cost of Data Center Outages，Ponemon Institute，2016 年 1 月。
[4] Https://www.sdxcentral.com/articles/analysis/securing-cloud-sdn/2016/05/。
[5] 2016 Cost of Data Breach Study: Global Analysis，Ponemon Institute，2016 年 6 月。

从五个方面重新思考 IT 安全性

如我们所见，即使 IT 安全性开销仅在 2016 年一年就超过了 800 亿美元[6]，但实现 IT 安全性的旧方法不足以阻止不断上升的威胁水平。考虑到这一点，不妨从以下五个方面重新思考用于实现 IT 安全性的方法：

1. **更改安全模式**
   传统的 IT 安全系统使用附加的点式解决方案、独立的硬件或软件产品，导致系统纷繁复杂且难以协调。我们需要的是全面构建的模式，能够既便捷又高效地提供安全性。
2. **实施遍布式软件层**
   借助跨应用基础架构和端点的遍布式软件层，可以将基础架构抽离在其上运行的应用。这样，您就可以在整个数据中心内轻松高效地应用安全性。
3. **最大程度地提供可见性和情境信息**
   通过将基础架构抽离应用，可深入了解用户、应用和数据之间交互的应用数据流和完整的端到端情境信息。
4. **根据应用调整安全控制和策略**
   借助最大程度获得的可见性和情境信息带来的好处，您可以开始针对要尝试保护的应用来调整安全控制和策略。
5. **注入额外的第三方安全服务**
   根据应用调整安全控制和策略后，您可以开始注入额外的第三方安全服务，以提供额外一层的智能保护。

网络安全性的新规则

旧有的网络安全基本规则已不再适用，IT 团队需要紧跟以下形势：

- **不断变化的基础架构：** 基础架构正在从本地部署环境演变为支持云环境和分布式应用。
- **与日俱增的移动化：** IT 部门需要扩展其安全策略，以支持纷繁复杂的新设备和型号。
- **日益严苛的合规性要求：** 组织面临法规遵从性的新要求。

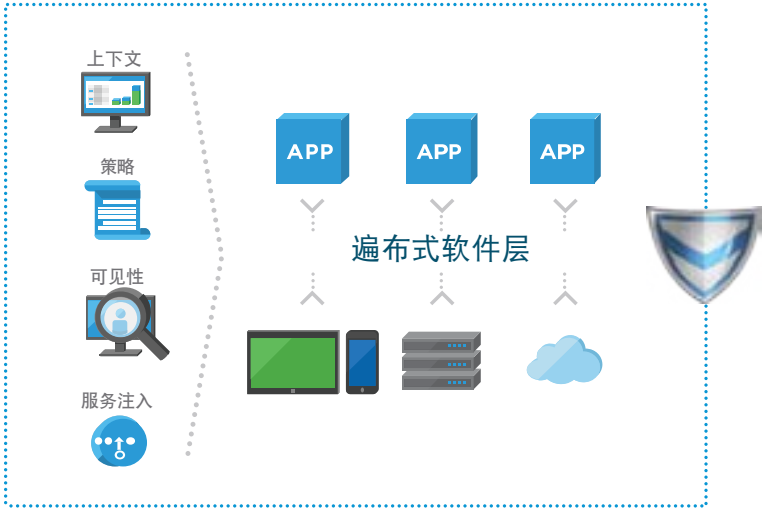


图 2. 遍布式软件层意味着安全防护无处不在

[6] “Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016”，Gartner Inc.，2016 年 8 月。

采用三管齐下的方法实现 IT 安全性

实现环境的安全转型以满足当今严峻的安全挑战，需要一种三管齐下的战略。

保护数据中心：重新思考数据中心的管理和安全性

您需要用有效的方式来更好地“隔离”敏感资源，以便更好地调整围绕这些资源的安全控制以及获得更多可见性和控制力，从而帮助您检测和应对威胁。

端点保护：重新思考用户基础架构的管理和安全性

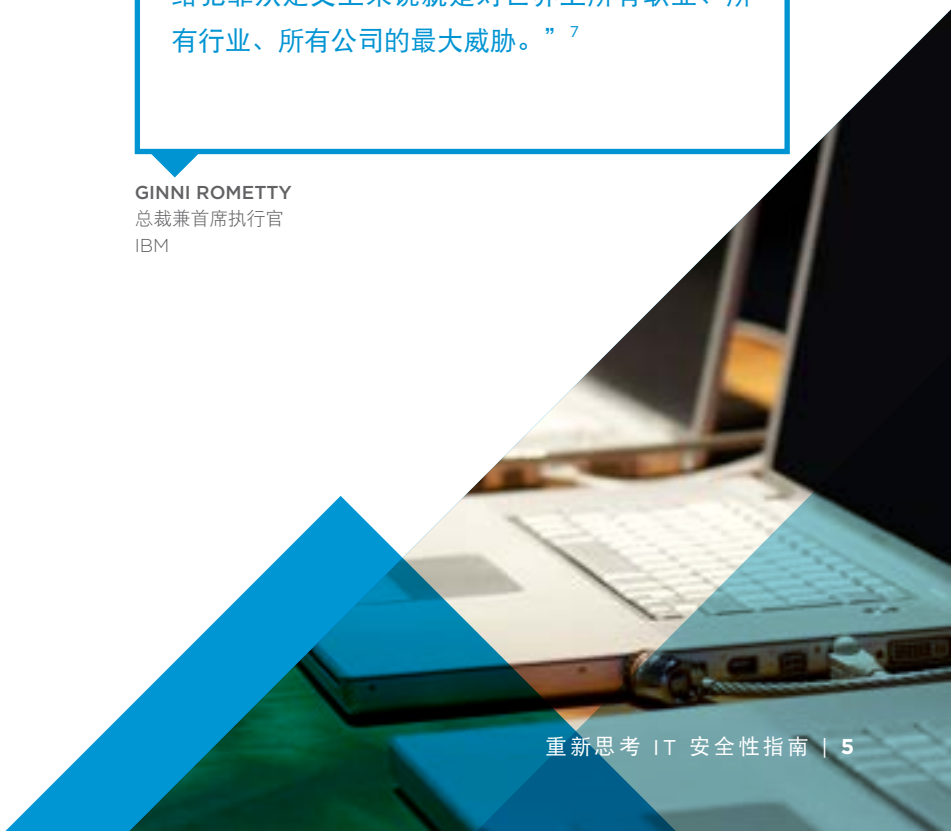
由于移动设备和操作系统的激增，用户基础架构没有统一的结构。这是一个巨大的异构世界。无论是从基础架构的角度，还是从以应用为中心的角度看，您都需要更好的可见性和控制力，同时不会损害用户期望获得的体验。

保护用户：重新思考用户/访问控制

用户访问权限对于增强员工能力至关重要。您需要找到一种方法，帮助您减少受攻击面、深入了解用户交互、高效应对无法避免的安全威胁。

> “我们认为，数据是我们这个时代特有的现象。它是世界上新的自然资源， 也是竞争优势的全新基础，并且正在改变着每一个职业和行业。如果所有这些说法都成立，或者说必然发生，那么网络犯罪从定义上来说就是对世界上所有职业、所有行业、所有公司的最大威胁。”[7]

GINNI ROMETTY
总裁兼首席执行官
IBM



[7] “IBM’s CEO on Hackers: ‘Cyber Crime is the Greatest Threat to Every Company in the World’”，福布斯，2015 年 11 月 24 日。

总结

数字化转型为您的业务提供了巨大机会。但该机会蕴藏着风险和严峻的挑战，即保护用户、应用和数据之间不断增加的交互。

通过重新思考用于实现 IT 安全性的方法，您可以应对这种新型的安全挑战。建立跨应用基础架构和端点的遍布式软件层是实现企业安全转型的起点。通过部署此软件层，您可深入了解想要保护的这些交互，获得有助于理解其意义的情境信息。

立即开始行动

获取重新思考 IT 安全方法的帮助

了解更多 >

在线加入我们：



关注 VMware中国

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
威睿信息技术（中国）有限公司
中国北京海淀区科学院南路 2 号融科资讯中心 C 座南楼 1 层 邮编：100190 电话：+86-10-5993-4200
中国上海办公室 上海市淮海中路 333 号瑞安大厦 804-809 室 邮编：200021 电话：+86-21-8024-9200
中国广州办公室 广州市天河路 385 号太古汇一座 3502 室 邮编：510610 电话：+86-20-87146110
中国香港公司 香港港岛东太古城太古湾道 12 号太古城中心 4 期 4 楼 电话：852-3696 6100 传真 852-3696 610 www.vmware.com/cn