WHITE PAPER

云世界的安全保障

越来越多的各类组织采用云计算，速度之快前所未有，这已经从根本上改变了企业和政府的计算基础设施。IT 市场研究公司 IDC 预测，到 2016 年，美国 IT 云服务的收入将达 432 亿美元，高于 2011 年估计的 185 亿美元。虽然云计算无疑能为各类组织显著节省成本，提高运营效率，同时也会带来新的风险和不确定性。部署公共、私有或混合云基础设施的组织——如今几乎所有组织都是如此——必须减轻内在的安全风险，同时也确保符合行业和政府的规定。

幸运的是，在信息安全性和合规性管理技术中的进步授予云计算用户降低风险、提高威胁响应并大幅减少合规性管理所需工作量的权力。而 NetIQ 公司走在这方面的最前沿。本文包含转移到云计算时保持可见性和控制权的三个简单步骤，并解释 NetIQ 公司如何提供相应的帮助。

NetIQ

NetIQ | WHITE PAPER

目录

云计算的优势 3

云计算的安全挑战 3

降低安全风险 3

检测安全漏洞 3

保持合规性 4

获得可见性和控制权的三个简单步骤 4

步骤 1：降低风险 5

步骤 2：增强威胁响应 5

步骤 3：减少合规性工作量 6

NetIQ 能提供什么帮助 7

NetIQ® Change Guardian™ 7

NetIQ Secure Configuration Manager™ 7

NetIQ Privileged User Manager 8

NetIQ Directory and Resource Administrator™ 8

NetIQ Sentinel™ 8

总结 9

关于 NetIQ 10

云计算的优势

云计算已经彻底改变了 IT 行业向其用户递送应用程序和服务的方式。采用云计算的组织不断增多，其增加的速度要比采用传统软件的速度快[1]五到十一倍，越来越多的组织将相当一部分的 IT 预算转移到云。

各类组织已经体验到几十个实实在在的云计算优势，尤其是降低运营成本、增强可伸缩性和提高业务灵活性。

云计算的安全挑战

尽管云计算能带来实实在在的好处，但转移到一个公共、私有或混合云体系结构当然也面临着一定的挑战，由于涉及到安全性和合规性，就更是如此。IT 部门依然有责任和职责确保安全性和合规性，在监管业务的同时，继续在适当的时间和地点向合适的用户递送业务服务。

降低安全风险

关于应用程序和服务迁移到云基础设施常常存在一种误解，即迁移能减少网络安全风险是由于云服务提供商能提供（貌似）精密的网络安全保护。这是一个危险的假设，因为您始终需要保护您敏感数据的保密性、完整性和可用性并且证明符合行业和政府规定，说到底这仍是您的责任。依赖云服务提供商提供的保护可能是一个灾难性的决定，这从 2011 年 Expedia 云计算漏洞和 2012 年 Apple 的 iCloud 漏洞可见一斑。

虽然云服务提供商不断地部署同类最佳的防火墙和入侵防御系统 (IPS) 以抵御已知的网络威胁，但这些设备不会降低与系统配置错误以及错位（和管理不善的）管理特权相关的风险。物理网络上存在的安全隐患在云中托管的系统内依然存在。对于系统，我们永远不应眼不见为净。

检测安全漏洞

入侵防御系统设备、下一代防火墙 (NGFW) 以及其他基于签名的防御可以有效地检测已知威胁。有些产品甚至可以针对已知的操作系统和应用程序漏洞，检测未知的威胁。然而，当今最复杂和危险的网络威胁包含前所未见的定制恶意软件，专门利用操作系统和应用程序内未知的零日漏洞，作为高级持续威胁（或称 APT）的一部分。

监控托管在云中的系统的安全漏洞可能远比监控物理计算机网络更具挑战性。大多数云服务提供商不会向客户提供访问其网络安全设备管理控制台或日志的权限，因为提供商利用上述控制台或日志来监控多租户虚拟化环境中的入侵，这些入侵会影响许多客户。由于缺乏可见性，客户很难甚至无法主动检测并应对针对其敏感数据的威胁。

云安全联盟 (CSA) 等组织所定义的标准将支持云安全性和审计数据的联合，让客户更好地了解其敏感数据。然而，让供应商现在就采用这些标准，实在为时过早。在托管在云中的敏感数据具有更好的可见性之前，IT 团队必须对其组织内建立的信息类型进行分类，并根据其灵敏度和价值，指派相关的风险等级。对此有所了解后，IT 团队可以更好地确定哪些类型的信息（如有）适合外部主机同时确定用于管理访问的策略和程序。

IT 团队可能决定在组织内保管高度敏感信息，无论是在应用程序内或私有云内，均可以通过集中控制和监控拥有访问权限的人员来防御漏洞或窃取。

[1] “Gartner’s Magic Quadrant 排名前三的云股票”，*Motley Fool，2013 年 3 月 7 日*。

保持合规性

将应用程序和其他 IT 服务迁移到云计算从未减少证明其符合行业规定（如 PCI 和 NERC）和政府规定（例如 HIPAA、FISMA、GLBA、SOX）的需求。然而，在云环境中向外部审计员证明合规性可能更具挑战性，因为许多用以确保云计算基础设施安全的安全系统是由云服务提供商提供和监控，而非您的组织。

组织必须确保，托管在云服务中的敏感数据，包括私有云或基础设施即服务 (IaaS)，其保护和管理的方式与企业信息管理策略和行业规定保持一致。他们还需要监控和验证服务级别，确保服务提供商能够始终如一地递送他们承诺的服务级别和客户体验。

获得可见性和控制权的三个简单步骤

组织不能只是依赖于外部云服务提供商的安全防御。实施云计算技术之前，组织必须主动在其内部系统持续地实施同类最佳的安全控制，实现“云就绪”状态。

云就绪安全计划可以帮助团队管理云计算引来的复杂性和风险。在使用云计算技术之前，通过在企业内部加强安全控制、制度和策略，团队可以更好地管理不断增多的用户、设备、应用程序和信息交换。云就绪安全计划将在整个传统组件和云组件（例如来自 IaaS 提供商的组件）组成的混合环境中有效地扩展。云就绪安全计划以数据为中心，专注于降低风险，帮助团队保持持续安全性和合规性状态。云就绪安全计划的组件包括：

- **更改监控**—更改监控解决方案不断监控、识别和报告意想不到的关键文件、平台、应用程序和系统更改。这些意想不到（往往未经授权）的更改可能是无意的或是恶意的，但仍会危及整个组织的安全性和合规性状况。例如，文件完整性监控 (FIM) 是一种特定类型的更改监控技术，通过比较其当前状态与已知良好的基线，监控关键文件的完整性。文件完整性监控提醒 IT 团队可能存在恶意代码嵌入操作系统和应用程序的情况，帮助检测可能绕过传统安全防御的高级威胁。

- **安全配置管理**—安全配置管理解决方案根据法规要求、安全最佳实践和企业 IT 策略评估关键 IT 系统的安全配置设置（例如口令合规性、启用服务、修补的漏洞和开放端口），证明合规性并管理信息安全风险。如果其中一项解决方案发现违反安全配置管理策略的安全设置，该解决方案会提醒 IT 团队（如有必要）评估并修复该设置。如今的配置管理解决方案有助于组织“强化”其关键 IT 系统，在满足合规性需求的同时保持稳固的安全状况。

- **特权账户管理**—特权账户管理解决方案能够使 IT 团队通过精细的权限委托和管理活动监控来控制和审计特权用户凭证（通常是 Active Directory）的使用。这些产品保护组织避免未经授权的特权升级，并有助于发现特权帐户的滥用。

- **安全信息和事件管理 (SIEM)**—安全信息和事件管理解决方案全面审视组织的 IT 安全系统及其相关的安全事件。安全信息和事件管理平台集合日志以及防火墙、防病毒 (AV) 平台、入侵防御系统设备、应用软件等其他安全相关的数据，然后关联不同的数据，努力发现隐藏的威胁。

这四个安全和风险管理解决方案协同工作，帮助组织提高基础设施安全性，降低风险。除非组织首先利用这些技术来确保其内部系统的安全——协调努力以实现云就绪状态——否则组织将任何服务迁移到云计算时面临的风险会增加。

以下三步流程——包括更改监控、安全配置管理、特权帐户管理以及安全信息和事件管理技术的方方面面——提供了一个确保内部系统安全的合理框架。

步骤 1：降低风险

在云计算中获得系统可见性和控制权的第一步是降低风险。通过减少基础设施的攻击面、监控系统配置的完整性和优化特权用户访问即可做到这一点。

减少攻击面。简单地说，基础设施的攻击面是攻击者可以未经授权地访问系统，未经授权进行更改并获得敏感数据的一切手段集合。为了减少攻击面，IT 团队必须配置用户只能访问被视为业务所需的应用程序、服务、端口和协议，以此来强化系统。此后，IT 团队必须不断监控和评估上述系统，以确保其根据最佳实践进行配置。

各类企业 IT 安全软件可用于管理、监控和实施直接连接到您网络的系统配置最佳实践。如果计划转移到云计算，必须逐一审查这些软件，以确定这些软件是否仍然会在云计算中有效，因为云服务提供商可能不支持直接以您在原来环境中使用的相同方式进行低级别访问。

利用 IT 安全框架。为了帮助组织实现 IT 安全最佳实践——并最终降低网络安全风险——一些组织已经构建 IT 安全框架（其中有许多在行业和政府的 IT 安全规定中有所参照，例如 PCI 和 FISMA），这类框架结合了强化防火墙、路由器、交换机、服务器、台式机、便携式计算机和移动设备安全配置指南。一些比较常见的 IT 安全框架包括：

- SANS 20 项关键安全控制
- NIST SP 800-53
- ISO 27001
- COBIT

领先的安全配置管理解决方案结合了四个框架的策略模板。用户可以利用仪表板和报告，识别不兼容的主机并审查修复主机返回兼容状态的指示。

优化特权访问。说到授予 IT 人员管理特权，多数专家认为，组织应遵循“最小特权原则”。最小特权规定，应向授予用户其可以拥有的最低级别权限，同时确保能够做好本职工作。不幸的是，并非所有的平台都支持需要授予最小特权的精细特权，许多平台令这类特权的配置和管理变得十分困难。此外，最小特权本身并不会减少来自负担过重或居心不良的 IT 人员的风险。凭借领先的特权帐户管理技术（内部系统以及基于云的平台和服务均有安装），IT 组织可以根据精细定义的角色授予 IT 人员权限，每个角色指派一个或多个权利（权限）。为了防止未经授权的用户特权升级，更好的特权帐户管理解决方案采用双密钥的安全性，即需要两个 IT 管理员确认特权帐户升级。

步骤 2：增强威胁响应

在内部系统及第三方提供商（例如 IaaS 提供商）安全配置经过强化，特权用户帐户经过优化之后，在云计算中维持安全性和合规性的的第二个步骤即增强您的威胁响应。通过检测来自混合基础设施威胁、关联针对其他安全防御所生成智能的威胁并监控潜在违规访问的特权用户，即可做到这一点。

检测内部威胁。当涉及到检测针对基于云的主机网络威胁，您的云服务提供商的防火墙和入侵防御系统是您的第一道防线。但如今最具破坏性的威胁将目标锁定在零日漏洞，不能仅仅依靠云服务供应商的传统外围防御。

与其集中保护现已远远超出传统边界的外围，安全小组更加需要针对数据本身（无论其驻留位置如何）实施安全控制。以数据为中心的方法来防御威胁是保护关键数据和合规性目标最有效的方式，经典的例子是进行加密和标记化。安全小组应该将以数据为中心的方法扩展到定期访问关键数据并与之互动的敏感系统和用户。关注敏感系统和用户的以数据为中心的安全解决方案示例包括，监控特权用户活动是否有不寻常的行为或未经授权访问敏感文件，或者实时监控安全事件和变更，以检测敏感文件和系统出现的意外或恶意更改。

通过采用以数据为中心的方法，安全小组可以更有效和积极地检测敏感数据和系统潜在的威胁并降低风险。这种方法使小组团队能够可靠地实现安全性、合规性和业务目标—甚至当 IT 环境由于采用突破性技术（例如云计算）而日趋复杂时也能如此。

集成安全防御。十年来，企业对于安全信息和事件管理技术的采用迅猛发展。不同于只是集合日志的基本日志监控解决方案，安全信息和事件管理解决方案集成和关联所有安全防御的智能（内部系统和云中），为 IT 团队提供一个单一的控制面板，响应日常安全事件，发现利用其他方式无法检测的高级攻击。领先的安全信息和事件管理平台还紧密集成更改监控解决方案，提供更丰富的安全智能，以实现更快的响应。

监控特权访问违规。领先的特权用户管理产品，不仅使 IT 团队能够根据不同的角色划分特权用户群体，也能在一个安全、只读存档中记录特权用户活动，从而提供了一个详细的所有特权用户操作审计跟踪，其中包括试图访问未经授权的系统——无论此系统是本地或物理安装在公司内部或是托管于第三方提供商（例如 IaaS 提供商）的云中——均可能是 APT 或其他有针对性的攻击过程中特权帐户受到损害的迹象。

步骤 3：减少合规性工作量

获得云计算基础设施可见性和控制权的第三个，也是最后一个步骤是减少实现和保持遵守行业和政府规定（例如 PCI 、HIPAA、FISMA、SOX、NERC 等）的工作量。遵守相关的 IT 安全框架，利用您的安全配置管理解决方案中的策略库和自动生成合规性报告和警报，即可做到这一点。

遵守 IT 安全框架。正如在步骤 1 中所述，许多行业和政府要求的 IT 安全规定参照 IT 安全框架中常见的最佳实践。通过利用同类最佳的文件完整性监控和安全配置管理解决方案——无论是物理网络还是云中——您的组织能够遵守相关的 IT 安全框架，反过来又可以降低实现和保持合规性的工作量。下面是包含相关参照的 IT 安全架构和 IT 安全法规示例：

- PCI 参照的 SANS 20 项关键安全控制
- FISMA 参照的 NIST SP 800-53
- SOX 参照的 COBIT

利用安全配置管理策略模板。安全配置管理策略包括描述特定主机配置设置预期状态的单个“测试”（和多组测试）。更好的产品包含了对应所有主要行业和政府规定的策略库（集合预先配置的测试），包括本文档已经参照的策略。

通过将安全配置管理监管策略模板映射到受 IT 安全法规影响的内部和基于云的主机（例如处理信用卡交易的主机），IT 团队可以显著减少实现和保持合规性的工作量。

自动生成合规性报告。最新的领先信息安全产品——尤其是那些在实现合规性中具有特定作用的产品——提供固定报告，有助于证明其遵守行业和政府的规定。更好的安全解决方案自动化生成合规性报告功能，导致合规性报告自动递送给内部审计师和 IT 管理人员。

NetIQ 能提供什么帮助

如今，网络威胁形势不断发展变化，企业和联邦机构面临的行业和政府规定也是如此。如果没有合适的工具，在云中（或者在物理网络中）实现和保持安全性和合规性会是一项很艰巨的任务。值得庆幸的是，NetIQ 可以提供帮助。

我们认为，仅依靠传统方法来降低数据安全及合规性的风险不再有效，您需要一个全面的解决方案。我们的身份、访问和安全管理解决方案套件经过无缝集成，有助于您控制云服务和数据访问，减少您混合环境中数据漏洞的风险，并有助于遵守行业规定以及云中的安全策略。

让我们回顾一下五大关键 NetIQ 产品，了解每一种产品如何协助上述三个步骤在您的企业中实现和保持安全性和合规性，以便于您准备迎接云计算的到来。

NetIQ® Change Guardian™

NetIQ Change Guardian 为特权用户提供活动和更改监控，帮助 IT 专家实时检测和响应潜在威胁。该解决方案提醒您在整个分布式环境中发生的更改，详细洞察 Active Directory、文件、目录、文件共享、注册表项（Windows 主机上）系统进程等。这些警报也指明操作是否获得了授权，同时包含更改前后的细节。NetIQ Change Guardian 提供了丰富的安全信息，包括识别威胁和记录更改必要的细节，相比单靠本机日志事件，可以提供更高的保真度和清晰度。

NetIQ Change Guardian 通过以下功能协助组织保护其混合基础设施，保持合规性：

- **特权用户监控**。记录特权用户（例如网络架构师和管理员）的活动，以减少内部攻击的风险。
- **实时更改监控**。实时监控关键文件、平台、应用程序和系统的更改，以防止违规行为，确保策略合规性（包括文件完整性监控）。
- **未经授权更改警报**。一旦检测到可能与 APT 或其他针对性攻击相关的未经授权更改，即可提供智能警报。警报提供识别威胁和记录更改必要的细节——比如指明执行操作的*人员*、执行了*什么样*的操作、执行操作的*时间*和*地点*。
- **合规性报告**。自动递送报告，以证明您监控关键文件和数据访问，并且遵守行业和政府合规性要求的能力。

NetIQ Secure Configuration Manager™

NetIQ Secure Configuration Manager 定期评估和报告系统配置的更改，并使配置与法规要求和最佳实践政策相匹配，帮助确保遵守 SOX、PCI、HIPAA、FISMA、NERC 及其他规定。其用户权利报告可评估用户权限，为您提供关于哪些人能访问关键信息及他们能访问哪些级别的关键信息方面的信息，帮助降低内部威胁。

NetIQ Secure Configuration Manager 通过下列功能，在保护混合基础设施及证明遵守 IT 安全强制规定中起发挥着至关重要的作用：

- **配置评估**。提供与许多 IT 框架及法规标准一致的可定制策略模板，并持续对照已知良好的基线，检查当前系统配置。帮助减少您网络的攻击面，及证明合规性。
- **用户权利报告**。评估用户访问关键系统的权限，帮助审计员了解哪些人能访问哪些级别的关键信息。
- **业务异常管理**。帮助抑制特定系统必须合理偏离获准配置标准的实例中的配置警报，及记录该种除外情况的理由。
- **安全性与合规性仪表板**。通过可定制仪表板，迅速直观地传达系统的安全性与合规性状态，满足众多股东的需求。

NetIQ Privileged User Manager

NetIQ Privileged User Manager 通过提供特权用户管理及跟踪整个 Windows、UNIX 和 Linux 环境，限制未经授权的事务及对敏感数据的访问。它通过允许管理员集中定义特权用户能在平台上执行的命令，确保仅经授权用户才能执行特定管理任务。

NetIQ Privileged User Manager 旨在通过以下功能，保护敏感资产，及证明符合行业规定：

- **简化的策略管理。**允许您通过基于 Web 的控制台集中创建安全规则，然后在所有受管理的 UNIX、Linux 及 Windows 系统上实施它们。
- **主动风险管理。**利用强大的风险分析工具记录和回放用户活动——具体到击键级别。
- **持续合规性。**提供永久性审计记录和自动数据过滤证明合规性。自动将更改添加到永久性审计记录中，并过滤数据，保证高风险事件立即可见。

NetIQ Directory and Resource Administrator™

NetIQ Directory and Resource Administrator 是一个功能完备的特权帐户管理解决方案，协调对 Microsoft Active Directory 的访问，限制用户只能针对整体目录的特定视图进行特定操作。它还支持用户供应及其他自动化任务，同时帮助实施安全策略和职责划分。

NetIQ Directory and Resource Administrator 通过以下功能，帮助保护资产并证明合规性：

- **精细的访问控制**。帮助您通过 60 多个角色和 300 多项权力，精细地将 Active Directory 权限指派给 IT 用户。
- **特权升级控制**。利用双密钥的安全性，即要求两位 Active Directory 管理员确认对用户权限的更改，防止出现未经授权的特权升级。
- **受控制的自助任务**。通过允许最终用户更新他们的个人目录信息及重设置他们自己的口令，降低成本。
- **集中化的活动日志和报告**。通过集中记录所有管理操作及灵活的综合报告，证明合规性。

NetIQ Sentinel™

NetIQ Sentinel 是一个功能完备的 SIEM 解决方案，其简化了 SIEM 技术的部署、管理和日常使用。NetIQ Sentinel 可轻松适应动态企业环境，及提供安全专家所需的切实可行的智能，帮助迅速了解它们的威胁状况，并按轻重缓急处理（内部系统和云中的）响应。

NetIQ Sentinel 使安全分析师能在监控系统完整性的同时，为审计员提供持续证明合规性所需的综合报告。主要功能包括：

- **安全智能集合**。集合您整个 IT 环境的日志数据及其他安全和网络智能，包括防火墙、AV、IPS 设备、安全电子邮件和 Web 网关、数据丢失预防 (DLP) 系统、应用程序、数据库等。
- **异常检测**。通过供应商提供及客户创建的强大的关联规则，自动识别您的组织的物理、虚拟和云环境中的不一致之处。让您根据基线保持“正常”网络通信，及检测潜在指向威胁的异常。
- **身份增强**。通过与 NetIQ Identity Manager 集成，将具体活动和安全事件与整个企业的用户绑定。
- **简化的合规性报告**。自动化繁琐的合规性报告功能，满足内部和外部合规性审计员的需求。

总结

云计算正在改变企业和政府机构向其服务的用户递送 IT 服务的方式。然而，尽管云计算能降低成本、提高可伸缩性及改善业务灵活性，但它也会加剧保护关键系统及证明符合行业和政府的规定所面临的挑战。越来越多人使用云和其他促进业务的技术，将本就十分复杂的 IT 环境推向极限，使得与第三方提供商之间的互相依赖性和集成达到前所未有的高度。

组织如要安全地享受云计算基础设施带来的好处，首先要在它们自己的内部环境中实施上述三步流程。一旦做到这点，根据需要将权限控制和流程扩展到云中会变得更加非常简单明了。通过遵循此流程，组织可以重新获得所需的可见性和控制权，从而有效地保护混合环境（由现场和第三方提供商系统组成）中的敏感数据。它们还能保持它们付出大量努力实现的合规性。

NetIQ 屡获殊荣的安全和合规性解决方案相互配合——加上您现有的 IT 安全基础设施——帮助您的组织即使是在云世界中也能实现和保持安全性及合规性。

关于 NetIQ

NetIQ 是一家全球企业软件公司，提供识别和访问管理、安全和数据中心管理的解决方案，满足混合型 IT 的需求。借助我们的解决方案，客户和合作伙伴可把握当今复杂多变的 IT 局势中的机遇。通过实现技术与服务递送方法的一致，我们的客户能更好地以商业速度提供战略价值。

要了解有关我们屡获殊荣的软件解决方案的更多信息，请访问：www.netiq.com。

562-CN1014-001

全球总部
1233 West Loop South，Suite 810
Houston，Texas 77027 USA
全球：+713 548 1700
美国 /加拿大免费电话：888.323.6768
info@netiq.com
www.netiq.com

http://community.netiq.com

要获取我们在北美洲、欧洲、中东、亚太地区和拉丁美洲办事处的完整列表，请访问：
www.netiq.com/contacts。