Trusted Cloud

世纪互联蓝云安全运营中心

Microsoft Azure 由世纪互联运营

Office 365 由世纪互联运营

Power BI 由世纪互联运营

由世纪互联运营的 Microsoft Azure、Office 365 和 Power BI 是在中国大陆独立运营的公有云服务，由北京世纪互联宽带数据中心有限公司的全资子公司上海蓝云网络科技有限公司（简称为"上海蓝云"）独立运营和销售。世纪互联采用微软服务于全球的 Azure、Office 365 和 Power BI 技术，为中国客户提供全球一致的服务质量保障。

当今世界，网络罪犯遍布在我们的周围。网络攻击的复杂度和频度正在越来越恶化，有组织的犯罪集团设计复杂的金融骗局以谋取利益。面对来自全球的各种威胁，任何个人或组织都无法百分百的确保自身安全。我们今天所面临的各种威胁并非新生事物，但黑客的攻击水平却在不断冲击新的高度。

世纪互联蓝云安全运营中心自 2014 年 3 月投入运营以来，世纪互联确立了多项切实有效的方法和措施，加速了安全解决方案的开发以及安全威胁的识别和解决。世纪互联蓝云安全运营中心汇集了大量安全技术和专家经验，建立起统一、协作的防御体系，以应对不断升级的安全威胁——保护世纪互联蓝云的云计算基础设施、服务、产品和设备，以及公司自身服务客户的资源。

世纪互联蓝云安全运营中心

正在消失的安全边界

以往，保护您的计算环境仅仅意味着建立起严密防守的边界，把敌人拦截在边界之外。但随着连接设备和服务的迅猛发展，包括自带设备（BYOD）和云应用程序的发展，边界已跨越愈发多样化的技术门类。在今天的"物联网"中，透过汽车、能源管控、健康监测、安全系统、智能手机、电视、冰箱以及平板电脑，均可看到这种日益显著增长的连接性。

今天，伴随机构内外的数据爆炸，攻击途径无处不在。"恶意行为者"（即网络恐怖分子和黑客）在应对这个不断进化而又紧密相连的世界时，技术手段越来越先进，组织也越来越严密。

这就对世纪互联如何超越传统的安全边界，对超大规模的云计算基础设施和云计算服务、客户使用的产品和设备、及世纪互联内部的资源进行保护，以及检测入侵、应对危害和攻击提出了新的挑战。

世纪互联蓝云安全运营中心

世纪互联安全运营中心汇集了公司的安全事件响应专家，时刻保护基础设施和服务、随时检测安全威胁并实时做出响应。在由传感器、设备、认证事件和通信构成的云服务中，海量的数据点在不断提供信息。

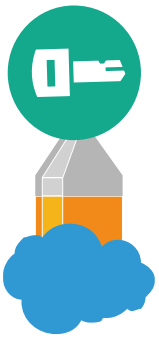
来自世纪互联生态系统的操作数据由安全专家进行分析，可在攻击行为影响我们的云计算服务和客户之前检测到攻击。世纪互联在安全分析方面进行了广泛投资，建立起丰富的行为档案和预测模型，能够连接各节点，识别难以探测的高级威胁，从而发起强力遏制，并展开协调治理。

世纪互联还与客户、合作伙伴和同行分享我们从大规模运营中掌握的安全知识和最佳实践，从而促进云计算生态环境的安全。

世纪互联网络安全态势

数字世界要求云计算服务商致力于不断提升保护、检测、并应对网络安全威胁的能力。这三项策略界定了世纪互联蓝云安全运营中心的网络防御方法，也是我们在战略和战术实现中的实用框架。

保护



世纪互联蓝云遵循全球先进的国际安全标准，权威的国家安全标准，业界领先的行业安全标准，实施了严格的物理、逻辑、流程和管理控制，确保合规性和客户的安全。由世纪互联联运营的 Microsoft Azure、Office 365 和 Power BI 以使用可信赖技术为基本原则。微软许可给世纪互联的 Microsoft Azure、Office 365 和 Power BI 技术从设计上立足于安全性，确保基础设施能够抵御攻击。以假定违反"作为一项安全战略，世纪互联的事件响应团队随时采取措施抵御任何攻击对 Microsoft Azure、Office 365 和 Power BI 服务造成的影响。这些实践基于世纪互联的安全管理流程，用于对抗数字化犯罪，响应 Microsoft Azure、Office 365 和 Power BI 安全事件和漏洞，以及防范恶意软件。

世纪互联蓝云合规性

由世纪互联运营的 Microsoft Azure、Office 365 和 Power BI 满足国际、国家和行业特定的合规性标准，拥有 ISO/IEC 20000 和 ISO/IEC 27001 认证，同时也符合公安部制定的信息系统安全等级保护定级标准，GB 18030 信息技术中文编码字符国家标准以及可信云服务认证（TCS）。

此外，基于风险管理的"信息安全管理系统"为我们的操作提供了指导，其中包括符合行业标准的 800 多个控制。基于风险的信息安全和隐私控制，以及广泛的合规框架，确保我们的基础设施能够履行我们的承诺，同时帮助客户简化其复杂的合规需求。对于使用我们云服务的客户而言，这些措施定期经过第三方审计的安全认证，确保满足客户所在行业的安全、隐私和合规规定。

世纪互联在数据中心运维和支持各种规模的商业、企业、和政府客户方面拥有丰富经验。我们了解商业运行软件的关键需求，包括认证、数据主权性、安全性和隐私性的要求。采用世纪互联云计算服务来处理您的业务，可以进一步满足您业务的合规需求。

世纪互联蓝云运营

世纪互联首先承诺保护我们客户和员工所在的计算环境，确保云计算基础设施和服务、产品、设备及公司内部资源具备韧性。

我们还确保配置变更管理政策得以建立并受到密切监控，在整个环境中对控制和组件实施主动维护，并迅速部署更新。

世纪互联蓝云纵深防御策略

纵深防御作为整个行业的最佳实践，是我们用来保护客户和企业资产的关键措施。在多个层面实施控制涉及采用冗余的保障措施和风险缓解策略，这将确保跨平台之间的保护更具韧性。

世纪互联的保护策略包括：

- 对世纪互联数据中心的物理环境实施广泛的监测和控制，包括针对物理访问的摄像、人员筛查、防护墙和障碍物、以及多重身份验证。
- **软件定义网络保护**我们的云基础设施免受入侵和分布式拒绝服务（DDoS）攻击。这些网络包括高级防火墙和网络入侵检测系统。
- **多重身份验证**被用于我们的基础设施，旨在控制身份验证和访问管理。它确保关键资源和数据受到以下至少两项认证的保护：您所知的（密码或 PIN）、您是谁（生物测定）和 / 或您所拥有的（智能手机）。
- **非持久性管理**对管理我们基础设施和服务的工程技术人员赋予 JIT 和 JEA 特权，从而为预先指定期限终止后自动过期的权限提升访问提供唯一凭证。此外，"密钥管理"措施和"密码库使用"消除了在共享列表中保留密码的需要，并降低了"Pass-the-Hash 渗透"等横向移动技术的有效性。严格控制和管理对这些资源的访问，有助于防止未经授权的入侵。
- 通过运行最新的反恶意软件和实施严格的补丁和配置管理，保持**适当的安全环境**。我们通过采用微软的先进技术，借助微软在全球网络（由传感器、设备、全球数亿服务器和设备接收的认证事件和通信构成）中的数万亿个数据点，使得世纪互联在与恶意软件的战斗中处于独树一帜的领先地位。
- **借助微软恶意软件防护中心**的研究团队识别、反向设计、并开发恶意软件代码技术，世纪互联将其部署于基础设施中，进行高级检测和防御。这些代码通过系统的更新和通知被分发到响应器，达到保护设备的目的。
- **安全开发生命周期**用于强化所有应用程序、在线服务和产品，并通过渗透测试和漏洞扫描定期验证其有效性。
- **威胁建模和攻击面分析**确保潜在的威胁和公开的服务得到评估，并通过限制服务和删除不必要功能减小攻击面。
- 根据数据的敏感性（即业务影响的高、中、低程度）**对数据进行分类**，采取相应的数据保护措施，包括对传输中和存储后的数据加密，并通过强制执行最小特权访问原则提供额外保护。

实施充分的控制并采取纵深防御策略，可确保任一个区域发生故障时，我们都能在其他区域进行补救控制，从而维护客户、云计算服务以及世纪互联基础设施环境的安全和隐私。

然而，没有任何环境是安全无虞的，因为人会犯错，而对手会不断寻找方法来触发和利用这些错误。我们会继续对保护层和基线分析进行重大投资，以便在出现异常活动时实现快速检测。

检测

世纪互联在假设入侵的态势下运营。这意味着尽管所有保护措施都已到位，但我们仍然假设系统会出现故障或人员会犯错误，导致对手渗入我们的基础设施和服务。这种态度使我们处于"随时待命"的状态，可快速检测危害行为，并采取适当的行动。

我们拥有由传感器、设备、认证事件和通信构成独特的、超大规模的网络，依靠世纪互联云计算服务的规模和智能、借助机器学习和行为分析，我们能够深入了解网络威胁的态势，并快速检测出异常活动。这类信号还得到语境元数据和行为模型的加强，其来源包括"活动目录"、资产和配置管理及事件日志。

定期进行漏洞扫描，以测试并改进保护措施的有效性。世纪互联对我们的安全生态系统的大量投资和世纪互联蓝云安全运营中心团队监测信号的多样性，使其比大多数服务提供商能够提供更全面的威胁视角。

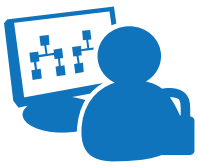
140 多天

攻击者在被检测到之前，在受害者的网络中停留的平均时间为 140 多天。取决于攻击类型，世纪互联云服务和安全软件工具能够将这一平均值降低到几天、甚至是几分钟。

世纪互联的检测策略包括：

- 为潜在的网络安全事件提供全天候（24x7x365）**监控网络和物理环境**。行为建模的基础是掌握使用模式和了解针对我们服务的独特威胁。
- 进行**身份验证和行为分析**，寻找异常活动。
- **机器学习**软件和技术被固定用于发现和标记不规则现象。
- **高级分析工具和流程**被用于进一步识别异常活动和创新关联能力，使我们能够基于接近实时的大量数据实现高度语境化的检测。
- **基于软件的自动化流程**能够不断进行审计和进化，提升效力。

当我们检测到系统出现异常时，安全响应团队就会立即行动。



响应

我们的第三项承诺是做出迅速、精确的响应。在我们的自动响应系统中，软件检测系统会不断发出通知。这些系统采用基于风险的算法来标记需要我们团队进行干预的事件。"平均缓解时间"至关重要，因此我们的自动系统将为响应器提供相关的行动信息，以加速分类、缓解和恢复活动。

为管理超大规模的安全事件，我们部署了一个多层次系统，以高效将响应任务分配给正确的资源，并促进开发合理的升级途径。我们的网络安全人员在众多领域均拥有高级认证资格，包括事件响应、取证和入侵分析。

网络威胁

受损的凭据

由于社会工程行动与出于好意的员工之间会发生冲突，获得凭据变得异常容易，这往往导致网络安全形成薄弱环节。超过 90% 的持续性高级威胁攻击始于钓鱼邮件。网络罪犯利用人类的情感——善意、恐惧、疑惑和专注——引诱用户在不知情的情况下分享其登录信息。钓鱼软件是首次入侵某个选定机构的首选武器。过去很容易识别钓鱼邮件——糟糕的语言、不规范的标识——但现在网络罪犯在引诱经历丰富的用户这方面更加游刃有余。他们一旦入侵您的网络，接下来能否在网络中成功进行横向移动，取决于受害者事先部署的额外保护措施。

分布式拒绝服务（DDoS）攻击防御

- 虽然 DDoS 攻击已存在多年，但这些攻击的规模仍然令人难以防范威胁。每秒超过 100 兆的攻击在一年前还属罕见，但这种程度的攻击变得越来越普遍，现在此类攻击每秒超过 600 兆。
- 互联网和物联网的发展创造了更多的连接设备，其中很多设备是不安全的，并且会引发更大规模的 DDoS 攻击。由世纪互联运营的 Microsoft Azure 提供一项自动 DDoS 检测和响应功能，可在 90 秒内检测并响应攻击，无需人工干预。针对 DDoS 攻击的检测和威胁缓解的速率得到大幅提升。

假定入侵策略

- 网络攻击者热衷于制造事端，因此所有网络使用者需要联合起来遏制他们。最近的研究显示，超过 82% 的公司将在未来一年内面临网络安全事件。
- "假定入侵"模型是我们遵循的关键安全原则。这仅表示，尽管我们对所实施的防护措施有强烈的信心，但我们仍然假定对手可能找到渗透安全边界的途径。在这种"假定入侵"策略下，我们将从攻击者的角度看待防御，并开展测试以发现和修复漏洞。

为世纪互联客户提供全方位的网络防御

云计算服务的用户应采用什么工具和流程来保护其网络环境，以及世纪互联如何帮助实施保护，这一直是我们的客户关心的问题。世纪互联已将我们在世纪互联蓝云安全运营中心使用的众多网络防御产品和服务整合到最佳实践和云计算服务中，并且与微软和我们安全生态系统中的其他服务商合作，提供最合适的解决方案，满足客户的特定需求。

请扫描信任中心
（www.trustcenter.cn）了解更多 Trusted Cloud 相关信息