

亚信安全™

服务器深度安全防护系统即服务

基于 Azure 打造的敏捷安全性服务





目录

1. 产品概要	2
2. 产品主要优势	2
3. 产品主要特点	3
4. 产品主要功能	3
5. 关键业务问题的解决	5
6. 支持平台	5
7. 关于亚信安全	5
8. 服务定价	6
9. 联系我们	6

1 产品概要

越来越多的组织认识到了云计算所带来的巨大经济和运营效益，开始转向业界领先的各种云提供程序，包括Amazon Web服务(AWS)、Microsoft Azure、Google Cloud等。在云环境中，安全性是一种共担责任。云提供程序要对从物理和网络基础架构一直到虚拟机监控程序层的整体安全性负责。但要在云中存储并保护哪些内容—工作负载—包括操作系统、服务配置、应用程序和数据，这由您决定。

亚信安全™服务器深度安全防护系统™即服务基于亚信安全业界领先的混合云安全解决方案构建而成，并由XGen™提供支持，旨在为云工作负载提供全方位的防护，以提高云提供程序的安全性。亚信安全服务器深度安全防护系统提供了一套完整的安全功能，包括入侵检测和防御、防火墙、采用Web信誉的防恶意软件、沙盒分析、完整性监控、日志审查和应用程序控制。

通过亚信安全服务器深度安全防护系统即服务，您将可以获得亚信安全服务器深度安全防护系统经验证的防护功能，可谓一举多得。部署服务后，那些繁琐的工作将由我们来为您完成。我们将为您管理常规产品和内核更新，设置和维护安全数据库，并负责亚信安全服务器深度安全防护系统管理中心的管理工作。

我们基于云的安全服务可以为您的云实例快速设置、自动化运行并简化安全性相关的各种操作。

2 产品主要优势

- **快速**：只需数分钟即可开始保护工作负载
- **经济高效**：采用基于使用量的定价模式，起始价格仅为 0.01 美元/小时
- **全面**：在单个产品中提供多种安全控制
- **省时**：我们负责管理和更新产品，因此您可以专注于自身业务
- **成熟**：为全球数千个客户和数百万台服务器提供防护服务

3 产品主要特点

简化安全管理

- 减少设置和管理所需的资源
- 在单个产品中提供多种安全控制，简化购买和管理流程
- 通过自动执行重复和资源密集型的安全任务，降低管理成本

云安全

- 快速抵御 Shellshock 和 Heartbleed 等漏洞
- 阻止试图避开检测的恶意软件(包括勒索软件)
- 确保云服务器仅与预期系统和安全域进行通信
- 检测可疑或恶意活动并向您发送警报

实现经济高效的合规性

- 一款解决方案即可满足 PCI DSS、HIPAA、NIST、SANS 和 SSAE 16 的主要合规性要求
- 提供详细、可审计的报告，其中记录了已防御攻击和策略合规状态
- 节省审计所需的准备时间和精力

4 产品主要功能

入侵检测和防御

- 通过屏蔽已知漏洞，主动防御各种已知和零时差攻击
- 检查所有传入和传出流量中是否存在协议偏差、策略违规或带攻击迹象的内容
- 虚拟修补帮助确保符合 PCI DSS、HIPAA 等主要法规
- 抵御 SQL 注入、跨站点脚本以及其他 Web 应用程序漏洞
- 对访问网络的应用程序加强监视或控制

防恶意软件

- 确保您的工作负载免受恶意软件攻击
- 隔离恶意软件，保护实例免受复杂攻击(包括勒索软件)
- 把可疑对象提交给亚信安全™深度发现™分析器，以供进行沙盒分析

触手可及的完全控制

- 支持策略驱动型管理
- 借助可自定义的控制台，用户能够轻松一览安全环境的运行状况
- 借助可自定义的策略模板，用户能够根据分配的规则即时启用和禁用安全控制
- 提供可能需要立即引起注意的事件或活动的即时通知(日志记录警报)

应用程序控制

- 更加深入地监视在给定系统上运行的应用程序，检测并阻止未经授权的软件(如勒索软件等恶意攻击)
- 扫描服务器并确定计算机上当前正在运行的应用程序
- 管理员能够锁定服务器，以阻止未列入白名单的新应用程序运行
- 加强运营控制和提高稳定性，让管理员能够确定新应用程序是否可以加入并安全地运行

Web 信誉

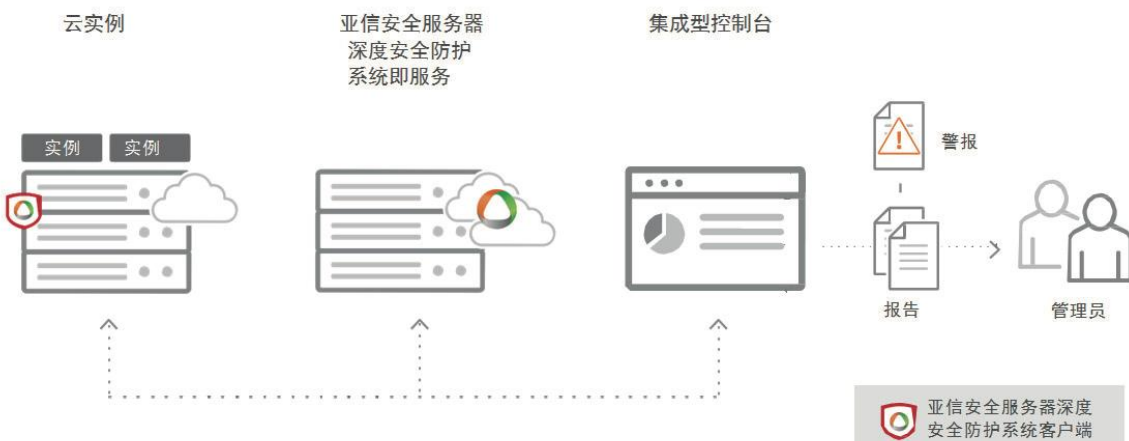
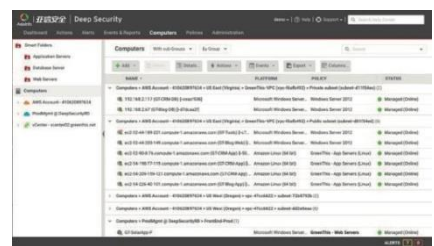
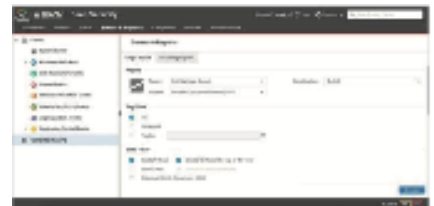
- 与亚信安全™云安全智能防护网络™相集成，可阻止与已知的命令和控制服务器进行通信

双向防火墙

- 通过创建防火墙边界来阻止攻击，可减少攻击面
- 限制为只能通过必要的端口和协议进行通信
- 集中管理服务器防火墙策略，包括用于常见服务器类型的模板

日志审查

- 收集操作系统和应用程序日志，并分析其中的可疑行为、安全事件和管理事件
- 通过识别重要安全事件确保满足合规性要求(PCI DSS)
- 将事件转发到 SIEM 系统或集中的日志记录服务器，以进行关联、报告及归档



5 关键业务问题的解决

虚拟修补

在漏洞被人利用之前就做好严密防护，消除紧急修补、频繁修补周期引发的操作问题，避免出现代价高昂的系统停机

零时差安全性

抵御零时差漏洞，同时最大限度地降低资源效率低下和紧急修补造成的运营影响

合规性

实现并证明符合 PCI DSS、HIPAA、SANS、NIST、SSAE16 等一系列监管要求

集成型安全性

从多个点产品过渡到一个全面的安全服务

6 支持平台

- Microsoft Windows (32 位/64 位)
- Amazon Linux AMI (32 位/64 位)
- Ubuntu (64 位)
- CentOS 5、6、7
- Oracle Linux
- Cloud Linux 5、6
- Red Hat®Enterprise 5、6、7 (32 位/64 位)
- SUSE®Enterprise 10、11 (32 位/64 位)

7 关于亚信安全

亚信安全是亚信集团“领航产业互联网”版图中的重要业务板块，于 2015 年由亚信科技对全球最大的独立网络安全软件提供商趋势科技中国区业务进行收购重组，专注于产业互联网安全服务领域，是中国领先的云与大数据安全技术、产品、方案和服务供应商。亚信安全在中国北京和南京设有独立研发中心，拥有超过 2000 人的专业安全团队，以“护航产业互联网”为使命，以“云与大数据的安全技术领导者”为战略愿景，亚信安全坚持“产品、服务、运营三位一体”的经营模式，助力客户构建“立体化主动防御体系”，为国家提供网络安全与云产业安全保障，推动实施自主可控战略。

8 服务定价

您只需为自己使用亚信安全服务器深度安全防护系统即服务的量付费。

全方位保护您的云工作负载，而起始价格仅为 0.01 美元/小时-无需承诺使用时长，也没有最低费用限制。

定价灵活，满足云需求：亚信安全服务器深度安全防护系统即服务采用基于使用量的定价模式

Microsoft Azure 虚拟机	每小时单价(美元)
1 个核心: A0、A1、D1	0.01 美元
2 个核心: A2、D2、D11、G1	0.03 美元
4+ 个核心: A3-A11、D3-D4、D12-D14、G2-G5、D3、D4	0.06 美元

9 联系我们

中建材信息技术股份有限公司 孙庆波 135-2025-0962 sunqingbo@cnbmtech.com

了解更多，请点击查看[微软爱中小企业官网](#)。

关于中建材信息技术股份有限公司：

中建材信息技术股份有限公司（简称：中建材信息）创立于 2005 年 4 月，注册资金 11025 万元。隶属中国建材集团有限公司，是中建材集团进出口公司的控股子公司。公司为混合经济体制企业。公司始终致力于向行业客户提供安全、可靠、高质量、易扩展的行业解决方案。帮助客户实现信息化管理最佳实践，以满足客户信息化建设不同需求。为合作伙伴提供专业、高效、创新的渠道增值服务，协助合作伙伴巩固核心竞争力，快速开拓市场，积极应对市场变化。



关于 Microsoft Azure：

在中国，由世纪互联运营的 Microsoft Azure 是在中国大陆独立运营的公有云平台，与全球其他地区由微软运营的 Azure 服务在物理上和逻辑上独立，采用微软服务于全球的 Azure 技术，为客户提供全球一致的服务质量保障。所有客户数据、处理这些数据的应用程序，以及承载世纪互联在线服务的数据中心，全部位于中国境内。位于中国东部（上海）和中国北部（北京）的数据中心在距离相隔 1000 公里以上的地理位置提供异地复制，为 Azure 服务提供了业务连续性支持，实现了数据的可靠性。

Microsoft Azure 由世纪互联运营