奇安信Web安全网关

奇安信SWG是奇安信集团为满足企业用户针对互联网边界安全管理需求而研发的一款专业的安全Web代理产品。它通过结合多种检测技术，包括Web过滤、数据丢失防护、防病毒以及高级威胁防护等，来保护企业员工免受来自互联网的安全威胁。 它可以帮助企业信息化管理人员，通过精细的应用控制来保障互联网合规性策略的有效落地。SWG提供包括高性能物理硬件和虚拟设备的部署方式，以满足于小型、中型和大型企业的不同部署场景。

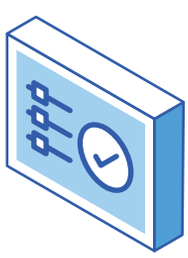
关键能力 KEY CAPABILITIES

- 领先的应用风险库（12000种应用程序）、应用风险和合规性评级
- 影子IT、云服务、应用程序可见性和控制
- 自适应策略执行
- 用户和实体行为分析（UEBA）

自适应访问控制

- 网关杀毒进行实时保护
- 七层保护技术：Web、DNS和应用程序控制、AV、IPS、DLP和内容分析
- 云沙箱和本地设备集成
- 集成领先的TI 威胁情报

高级威胁防护



- 高性能代理，单节点提供超过10Gbps的代理处理能力
- 多机堆叠的可扩展性
- HA高可用性

高性能及高可靠性

- 识别和控制敏感信息
- 与企业 DLP 产品集成
- 内容分类标签
- 水印

数据保护

核心功能 CORE FUNCTIONS

网页过滤

提供全面的Web过滤能力，内置数亿规模的URL数据库，包括130多个类别，以满足精细的Web控制要求。
有效应对包括勒索软件、凭证盗窃、网络钓鱼等其他基于Web的网络攻击威胁。

细粒度应用管控

支持针对SNS、IM、BBS等类型，共计12,000多个互联网应用程序的细粒度识别，可覆盖绝大多数SaaS应用及移动应用。
提供有效的应用程序可见性和影子IT控制。

数据丢失防护

提供针对PII等敏感信息的检测扫描能力，阻止将敏感数据、敏感文件通过未经批准的途径外发，从而防止将受监管的数据或知识产权外泄。
提供与其他企业DLP产品集成的能力，从而进行更为严格、全面的检测。

恶意软件和高级威胁防护

集成本地化基于行为模式的病毒检测引擎。
提供基于云模式的URL、IP、文件哈希动态检测及扫描能力。
集成领先的威胁情报。

未知威胁防护

本地设备与云沙箱进行协同，通过机器学习和基于仿真的沙盒技术实现对未知威胁的实时防护。

加密流量检测

提供针对SSL/TLS 流量的解密、检查和再加密能力，可以基于多种条件对未分类及特定分类的SSL流量进行检测。

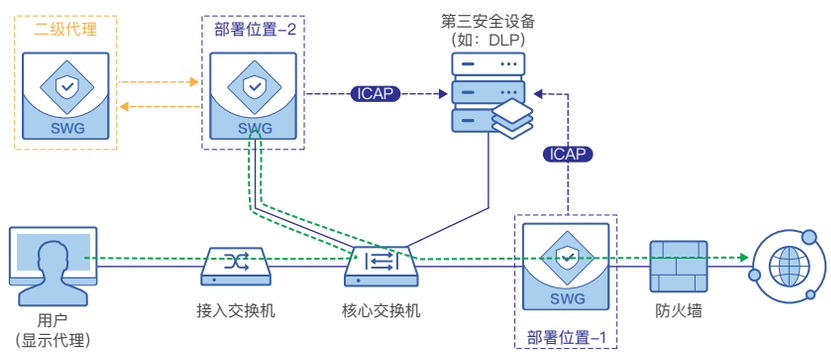
分布式架构

支持多机集群方案，提供性能扩展能力。
配合独立的策略中心，保障分布式管理的策略一致性。

典型应用 CLASSICAL PRACTICE

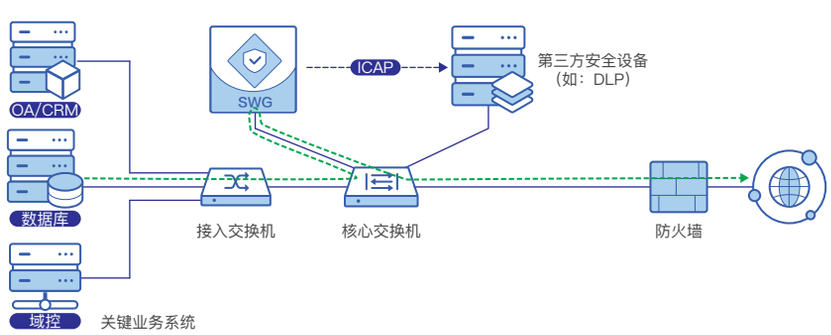
互联网出口管控

- SWG串行部署于互联网出口或旁路部署于内网；所有用户必须通过SWG代理上网
- 从用户发起的Web流量中过滤掉存在风险的流量和恶意软件；有效保护用户免受基于Web的威胁



关键业务系统代理访问互联网

- 关键业务系统配置显式代理，当其进行升级或特征更新时需通过代理访问互联网
- 保护用户免受基于Web的威胁



内部业务系统安全访问

- SWG部署于内部业务系统前，内网用户通过“反向代理”访问业务系统
- 实现对业务系统真实信息的隐藏和保护，及对访问流量的全方位安全检测与控制