Forcepoint

解决方案简介

Forcepoint ONE: 云平台简化混合劳动力的安全性

用例

- 查看并控制混合员工 (即采用混合办公模式的 员工) 与 Web、云和私有应用程序中数据的 交互。
- 防止滥用托管或非托管设备访问的敏感 数据。
- 控制对高风险网络内容 和不同类型 GenAI 站点的访问。
- 实现对业务资源与私有应用程序的快速安全远程访问, 省却 VPN 的繁琐。

解决方案

- 单一、统一的平台允许管理 所有业务应用程序的一致 安全策略。
- 一体化云服务, 结合安全 Web 网关 (SWG) 、云访问安全代理 (CASB) 和零信任网络访问 (ZTNA) 保护访问及数据。
- 将高级威胁防护与数据安全集成, 以此阻止攻 击者并保护敏感数据。
- RBI、用于扫描公有云风险配置的 CSPM、用 于下载文件消毒的 CDR 等其他功能。
- 用于数据标记的 Forcepoint 分类。

成果

- 简化 — 将网络、云和专用应用程序的安全性整合到一个统一的平台中 (支持无代理) 。
- 现代 – 将零信任原则与 SASE 架构以及高级安全管理 (例如, 远端浏览器隔离和下载文件消 毒) 相结合。
- 无处不在 – 提供 300 多个入网点 (PoP), 实现 全球访问。
- 可靠 – 自 2015 年以来, 经验证正常运行时间 达 99.99%。
- 快速 – 采用分散式执行和自动扩展, 以消除阻塞点。

Data-first Security

安全问题日益复杂化, 但我们有更优解。用户如今可以在任何地方工作, 他们的数据分布在网站、云应用和私人应用中。

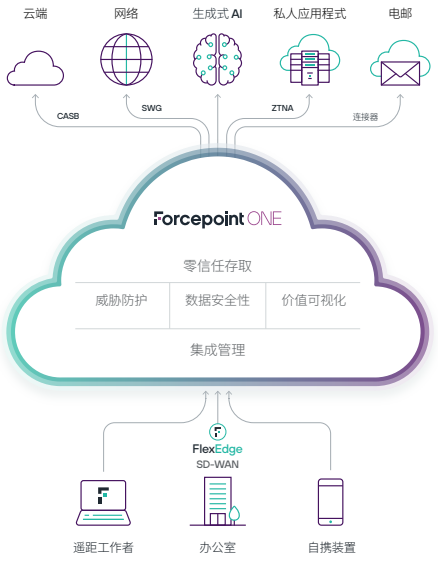
为了支持回归办公室 (RTO) 计划和混合型劳动力, 安全团队需要一个将数据置于中心位置的融合安全平台。安全控制需要能够跨越网络、云和私有应用访问, 具有一致的可见性和控制, 以便组织能够在损失发生之前采取行动, 阻止数据丢失。

通过数据优先的解决方案, 在任何地点工作的人员的业务数据可无时无刻得到保护。

Forcepoint ONE 简化安全管理

Forcepoint ONE 是一个集成的云平台, 可让安全变得简单。您可以快速采用零信任和安全服务边缘 (SSE, 即 SASE 的安全组件), 因为我们汇集了 SWG、CASB 和 ZTNA 等关键的安全服务 。

通过安全地采用 GenAI 等新技术来释放生产力控制对不同类型 GenAI 站点的访问, 并持续执行防护措施来保护敏感数据并防止恶意软件风险。



在任何地方保护数据，为任何地方工作的人们服务

Forcepoint ONE 的云原生与零信任功能包括：

- → **适用于云和私有应用程序的无代理 DLP 安全性。**从个人设备安全使用私人企业 Web 应用程序，同时保证敏感数据的安全。
- → **集成高级威胁防护和数据安全。**防止数据丢失或泄露，并通过各处的一致控制阻止黑客入侵。
- → **统一网关用于云、网络和私有应用访问。**为 SWG、CASB 和 ZTNA，将基于身份的业务应用程序访问控制集中管理于一处。
- → **动态扩展，实现全局访问** – 无论员工的工作场所如何，300 个建立在 AWS 上的入网点能确保快速且低延迟的连接并保障 99.99% 的正常运行时间

Web、云和私有应用程序的统一安全管理

- → **云：**CASB 将在任何设备上执行对企业 SaaS 应用程序和数据的细粒度访问。CASB 能实时阻止敏感数据下载以及恶意软件上传。它将扫描热门 SaaS 和 IaaS 中的静态数据，以查找恶意软件和敏感数据，并根据需要提供修正。CASB 将检测影子 IT 应用程序并控制任何托管设备的访问。
- → **Web：**SWG 根据风险和类别监控与任何网站的互动，阻止下载恶意软件或将敏感数据上传到个人文件共享和电子邮件账户。我们的-设备网络安全可在任何地点的托管设备上执行可接受的使用策略。
- → **私有应用程序：**ZTNA 将保护并简化对私有应用程序的访问，避免与 VPN 相关的复杂性或风险。

将高级威胁防护与数据安全集成

- **数据泄漏防护 (DLP)：**上传或下载文件或文本时将 扫描敏感数据，并根据需要阻断上传或下载、跟 踪、加密或 改写。
- **恶意软件扫描：**上传和下载文件时将扫描恶意软 件，如果发现有恶意软件，将立即停止上传或下 载。

集成可见度和控制

- **集成管理套件** 用于跨 SSE 通道 进行配置、监控和报告。
- **登录策略** 可根据用户位置、设备类型、设备状态、用户行为和用户组控制 对网络、云或专用应用程序的访问。这些参数有助于防止账户被盗
- **易于使用的 DLP 策略** 可用于控制托管 SaaS 应用程序、专用应用程序和网站的 敏感数据和恶意软件，以及托管 SaaS 和 IaaS 中存储数据的下载和上传。
- **设备代理** 适用于 Windows 和 MacOS 系统，支持 SWG、CASB 或 ZTNA，用于非浏览器客户端应用程序和影子 IT 控制。
- **统一的分析与数据可视化**，针对单一云端安全平台的安全风险、总体使用情 况以及相关影响迅速提供洞察报告。

按需提供其他功能

- **云安全态势管理 (CSPM)：**描 AWS、Azure 和 GCP 中的风险配置，并提供手动和自动修正。
- **SaaS 安全态势管理 (SSPM)：**描 Salesforce、ServiceNow 和 Office 365 中的风险配置，并提供手 动和自动修正。
- **远端浏览器隔离 (RBI)：**在云托管的 VM 中运行浏 览器，保护用户的本地设备免受 Web 恶意软件的攻 击。
- **Forcepoint Classification**：利用人工智能提供的建议进行数据分类标记，以提高标记准确度。
- **AMDP:** 在受控恶意软件沙箱中分析文件行为以识别隐藏和恶意内容。

即刻订阅，简化战略尽在你手

可按用户进行年度订阅：

- **一体化版**，用于 Web、云和私有应用程序。
- **网络安全版** 包括网络网关 及内联 CASB，用于无限云应用程序，而 RBI 基础版用于未分类和新注册的站点，以添加对云应用程序的 API 支持，并在以后支持专用应用程序。
- **ZTNA 版**本保护无限数量的私人应用程序。
- **CASB 版**本可内联保护无限数量的云应用程序，并包括 3 个应用程序的 API，并且能够添加其他应用程序包或专用 API 轮询节点。
- **所有订阅** 都包括集中式云管理，数据丢失预防策略，通过端点代理的自动访问，以及全面报告。

forcepoint.com/contact

[FP-Forcepoint ONE-Solution-Brief-SCH] 03Jul2024