FORCEPOINT

产品资料

FORCEPOINT UEBA

信息安全

保护IP、检测被破解帐户、降低内部风险

Forcepoint用户和实体行为分析（UEBA）使安全团队能够主动监控企业内部的高风险行为。我们的安全分析平台通过融合结构化和非结构化数据来识别和破坏恶意、被盗用和疏忽的用户，从而提供无与伦比的环境。我们能发现诸如被破解账户、企业间谍、知识产权盗窃和欺诈等关键问题。

为什么要强调UEBA的安全

客户依靠我们提供关于企业内部人为行为环境。只有Forcepoint UEBA才能提供可配置的分析功能，以帮助安全分析人员解决对业务最为重要的问题。我们在帮助安全团队的同时，可以扩展规模：

- 减少检测内部攻击的时间
- 当安全团队淹没在噪声中时，需要提供相关警报
- 详细了解内部活动，超越SIEM和其他工具
- 提高事件响应和事后取证的调查效率

平台支柱

Forcepoint　UEBA提供对高风险行为和个人的洞察力，而不仅仅是异常警报。通过评估人员、数据、设备和应用程序之间细微的相互作用，Forcepoint　UEBA优先考虑安全团队的时间安排。我们的软件建立在四大支柱上：

丰富的背景 > 将不同的数据源融合为一个单独的记录文件，将通信内容与SIEM、端点和员工资源提要一起解密。

行为分析 > 应用针对变化、模式和异常检测的多种严格行为和基于内容的分析，以更好地检测复杂的攻击。

搜索和发现 > 通过背景丰富的用户界面公开强大的取证搜索和发现工具，以进行持续监控和深入调查。

直观的工作流程 > 提供与人员工作和现有客户信息架构高度集成的主动报告，以提高运营效率。

主要使用案例

- 先导活动
- 内容感知DLP
- 被破解账户的检测
- 数据侦察
- 特权用户滥用
- 安全分析

重新确定安全分析

环境驱动的可见性 > Forcepoint UEBA通过将非结构化的、多背景的数据流与结构数据集成，独特地提供对员工活动、行为和关系的可视性。我们的分析模型允许通过所有数据流中的多个镜头对实体和事件进行评分和优先级排序 – 以前，安全团队无法使用这些功能。我们还整合了活动目录、SIEM、EDR和关键数据来源，以提供真实的情境意识，以及一个从根本上加强内部调查的强大取证平台。

可配置的分析 > 传统的黑盒UBA工具通常仅限于结构化数据源，在不同的系统中进行分析，具有固定的分析配置。相比之下，Forcepoint UEBA提供了强大的分析功能，使安全团队能够处理不断变化的安全使用案例，并执行实时临时分析，包括跨所有数据集的高级搜索。我们的分析可以在无需额外编程的情况下进行调整，从而更灵活地应对安全威胁。

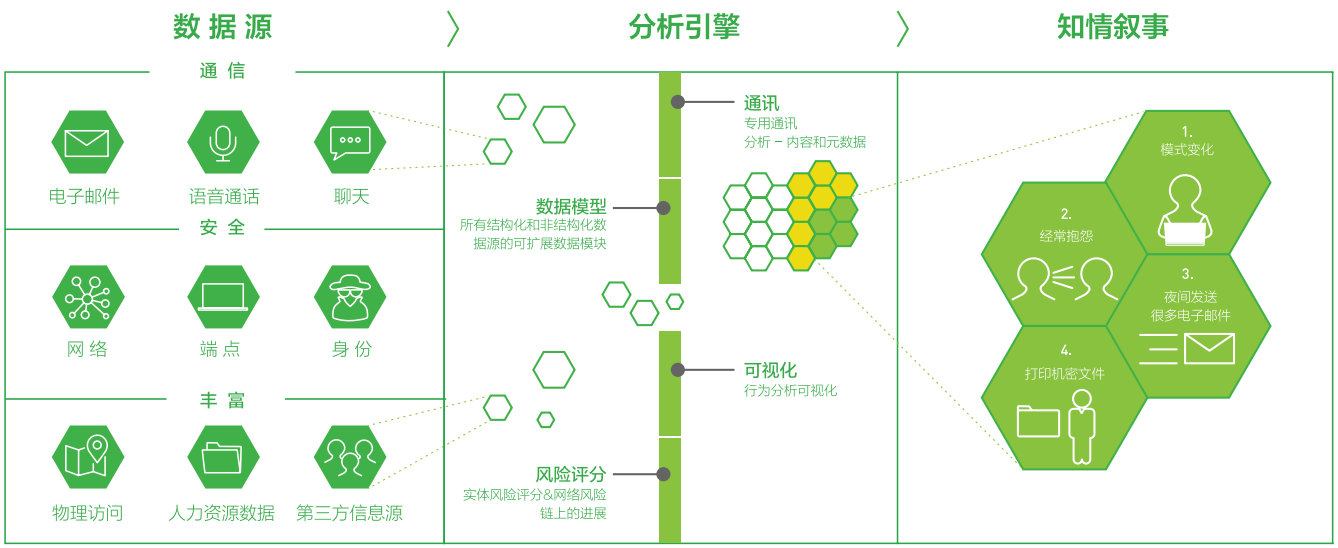
规模 > 我们基本上按比例建设。只有Forcepoint UEBA使用ElasticSearch来支持即时访问海量数据。我们的平台无缝存储结构化数据和非结构化数据，并与客户进行横向扩展。Forcepoint UEBA还提供不同水平的访问和管理控制，所以你可以在任何类型的部署中依靠我们的技术来协助您的工作。

功能

- **基于角色的仪表板和工作流程** 通过直观的用户界面快速审查不合规活动，以便分析师和管理员可以快速调查、审查、升级和采取行动。
- **强大的数据权利** 完全支持内部控制和外部驱动数据的隐私问题所需的复杂数据权利。
- **可扩展平台** 可配置的分析、仪表板和工作流程支持开箱即用的安全用例，具有可扩展到任何风险使用案例的全面功能。提供先进的数据科学模型，而无需沉重的专业服务承诺。
- **灵活的部署选项** 在虚拟私有云，甚至在使用Forcepoint UEBA设备的情况下，快捷预配Forcepoint UEBA。

高级分析

- **行为分析** 通过情绪和内容分析来识别员工行为的变化，这些行为可能暗示当前或潜在的非法、不需要或不符合要求的活动的
- **智能分级** 根据内容和元数据模式的分析来确定感兴趣事件和警报的优先级。
- **自然语言处理（NLP）** 通过智能的、自然语言处理、任何语言的复杂词汇和文字识别技术的实际应用，可识别来自受威胁的电子邮件的免责声明和引用文本的，从而显著减少误报。
- **可视化效果** 专门量身定制的可视化效果，以开启分析师自己的推理能力，提供相关活动的最充分的情况。快速了解是谁、在做什么、什么时候做、怎样做等员工行为的细节信息。
- **内容分类** 使用Forcepoint UEBA的内容分类引擎识别并过滤掉不相关的通信像群发邮件、第三方邮件等加强DLP部署。



联系方式：
www.forcepoint.com/contact