思科 Tetration 平台

为多云数据中心提供整体性工作负载保护

应用正在引领数据中心基础设施不断发展。当今的应用采用了虚拟化、容器化、微服务和工作负载移动性等多种技术，动态性极强，而且应用组件之间的通讯模式也在不断变化。现在，76% 的数据中心流量为东-西向流量，与过去的流量模式截然不同。这种技术能够在增大的攻击面上最小化横向移动。网络和安全运营团队难以实施安全的基础设施。对于多云数据中心，这一挑战甚至更加严重。为了有效应对这一挑战，网络和安全运营团队需要更加深入地了解应用和整体工作负载保护策略。

思科 Tetration 平台（图1）使用无监督的机器学习、行为分析和算法方法来满足这些要求。它提供了一个现成的解决方案，用于准确识别数据中心中运行的应用及其依赖关系，以及不同应用层之间的底层策略。该平台还可使用白名单策略和分段来实施零信任模式，监控服务器上运行的进程的行为，并识别与软件相关的漏洞和风险。借助此方法，思科 Tetration 平台可跨多云环境中运行的虚拟化和裸机工作负载提供多维安全方法。

优势

- 使用基于行为的应用洞见，自动执行白名单策略。
- 使用应用分段最大限度地减少横向移动，实现安全的零信任模式。
- 通过进程行为偏差更快地识别异常。
- 通过快速识别常见漏洞和风险，减少数据中心内的受攻击面。
- 从异构环境中收集全面的遥测数据，在几分钟内即可提供切实可行的洞见。
- 支持长期保留数据，实现深度调查、分析和故障排除。

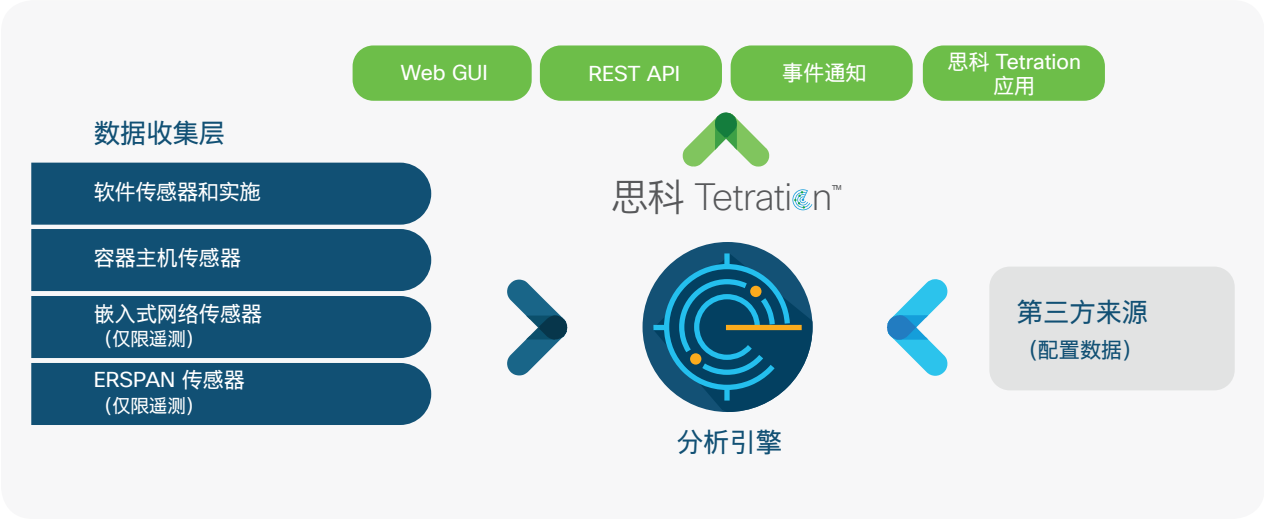
“Cisco Tetration Analytics 为我们提供了前所未有的网络和应用可视性，而且帮助我们从传统的黑名单策略模式迁移到白名单策略模式，这种新模式可以显著增强安全性。”

- 医疗行业客户

通过在数据中心基础设施中使用软件传感器、硬件传感器和封装的远程交换端口分析器 (ERSPAN) 传感器，该平台可以支持现有环境（棕地）和新环境（绿地）部署。软件传感器也可充当应用分段的实施点。

思科 Tetration 平台可借助大数据技术支持数据中心扩展。它可以近乎实时地处理传感器接收的全面遥测信息（每秒多达 200 万个遥测事件）。该平台可以在上万台服务器运行的数以千计的应用中实施一致的策略。该平台专用于满足长期数据保留需求，能够从其数据湖中搜索数百亿条遥测记录，并在不到一秒内返回切实可行的洞见。

图 1. 思科 Tetration 平台架构



“过去，我们最长需要一个月的时间才能映射一个复杂的应用，而利用思科 Tetration，我们可以在几天或更短的时间内完成这项工作。这将帮助我们在更短的时间内完成重大的 IT 计划，并显著降低成本影响。”

– 亨廷顿国家银行

使用行为分析作出明智的安全和运营决策

思科 Tetration 平台使用无人监督的机器学习和基于行为的算法方法，提供现成的解决方案：

- **应用洞见：**该平台可使用机器学习技术提供对应用依赖关系和行为基准的洞见。它还能利用通信模式和进程信息来自动识别应用组件集群（例如数据库集群），并对其进行分组。利用此实时遥测数据，它可以自动生成应用分段所需的白名单策略。
- **应用的基于行为的白名单策略：**通过使用高级算法，该平台自动生成用于分段的精细白名单策略。它还能够将业务策略要求与基于应用洞见生成的策略进行合并。此策略的规范化和分层合并有助于确保权限范围较小的管理员无法覆盖更高级别的业务策略意图。该平台支持“先试后用”模式，即在将白名单策略应用于生产网络之前，可以先进行模拟和影响分析。
- **自动化的策略实施：**该平台通过跨公共云和私有云以及本地部署的软件传感器实现一致的策略实施。由于策略针对工作负载本身实施，因此该平台支持虚拟化和裸机环境。此方法还可确保策略随工作负载移动，即使应用组件从裸机服务器迁移到虚拟环境，也是如此。
- **进程行为偏差识别：**通过为服务器上运行的进程建立基准并确定与这些基准的任何偏差，可以确定服务器的行为。在思科 Tetration 中，算法可以将这些偏差与恶意软件执行模式相匹配，从而更快地检测异常。这些行为模式映射包括诸如“Specter”（幽灵）和“Meltdown”（熔断）等影响较大的威胁。
- **检测与软件包相关的漏洞：**思科 Tetration 平台还对已安装的软件包、软件包版本、补丁级别等进行了基线化。该平台包括 19 年的漏洞和风险信息。使用此数据，Tetration 平台可检查是否有任何软件包存在常见漏洞和风险 (CVE) 数据库中列出的已知信息安全漏洞。当检测到漏洞时，您可以找到完整的详细信息，包括严重性和影响评分，并找到安装了相同版本软件包的所有服务器。您还可以预定义当服务器安装了有某些漏洞的软件包时进行特定操作（例如隔离主机）的策略。
- **合规性和审计：**该平台可监控应用组件的策略合规性。利用行为分析技术，它可以在数分钟内检测到任何合规性偏差，并触发通知。此外，实施策略还会自动更新，以适应某些应用行为更改。

“对我们来说，使用思科 Tetation 带来了巨大的投资回报，我们无需再次执行应用映射；通过动态映射，我们不必针对未来的计划再次进行此操作。”

- 亨廷顿国家银行

- **网络性能：**该平台扩展了机器学习功能，可提供运营团队之前无法获取的一些关键网络性能信息。它提供每数据流路径视图、TCP 性能指标、网络数据平面性能指标等。所有这些信息都在时间序列视图中提供，用户可以及时返回并搜索详细信息。
- **通过搜索引擎实现对整个数据中心的可视性、故障排除和调查分析：**该平台可以收集并存储全面的流量数据。除了对服务器的可视性之外，您现在还可以在虚拟桌面基础设施 (VDI) 计算机上部署软件传感器，获得对 VDI 环境的可视性。这样一来，通过查询这些数据即可获得对整个数据中心的可视性，并实现对整个数据中心的调查分析。不仅如此，这些数据还能用于网络和应用问题的故障排除。

思科 Tetration 平台不同于业内任何其他平台。它是一个具有高级管理功能的就绪型平台，只需进行极少的配置，部署十分快捷。通过使用机器学习功能，该平台极大地减少了获取通信模式信息所需的手动工作量。利用该平台的整体工作负载功能，您可以为应用构建更安全的基础设施，并显著降低暴露风险。

更多详细信息

有关思科 Tetration 平台的更多详细信息，请访问 http://www.cisco.com/go/tetration。

C45-737257-05 2018/02