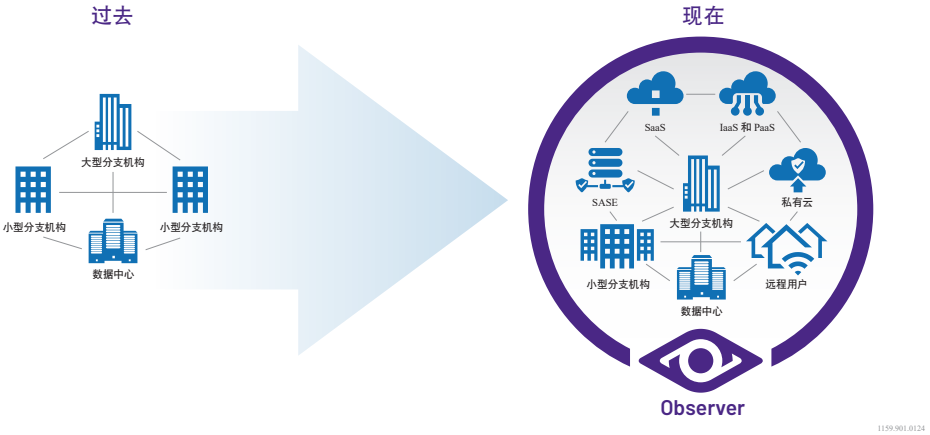
Observer Apex

专为 NetSecOps 打造：查看更多。更快地解决。
通过高级分析提供全面的网络和安全可见性。

网络无处不在

复杂的多层应用程序托管在本地或基于云的资源中，包括 SaaS、IaaS、PaaS 和 SASE。用户随时随地访问应用程序是新的常态。今天的网络没有边界，但每一项 IT 服务仍然依赖于它。

如果网络或服务架构的任何组件出现故障，应用程序交付可能会迅速降级，导致客户满意度下降和业务盈利能力下降。为了避免这种情况，必须具备全面的服务可观察性。



Observer Apex 在您最需要的地方提供可见性，并且是第一个针对每个事务生成最终用户体验 (EUE) 评分的绩效管理解决方案。Apex 通过多个数据源提供适应性和可见性：数据包、元数据和丰富数据流。组织可以选择最适合其预算的来源。

Apex 提供全球 IT 服务健康和状态意识，符合其提供全面可见性的承诺。当出现服务异常或检测到潜在的安全漏洞时，高效的工作流使 NetOps、DevOps 和 SecOps 团队能够发现根本原因并快速修复。

NETSECOPS 指挥中心

- 机器学习支持的自动 EUE 评分将多个关键绩效指标转换为一个易于理解的指标，并结合详细的分数扣除，自动隔离问题领域，提供确定快速补救优先级所需的信息
- 包括数据包、元数据和丰富数据流在内的灵活数据源选项为从网络工程师到业务线所有者的每个利益相关者提供了正确的视图
- 面向全球运营智能的可定制仪表板和高效的工作流可帮助 NetOps、SecOps 和 DevOps 快速识别和解决问题
- 按需应用程序依赖关系映射无需配置即可实现快速、准确的多层应用程序可见性
- 用于快速服务异常和快速网络安全漏洞响应的集成性能管理和取证

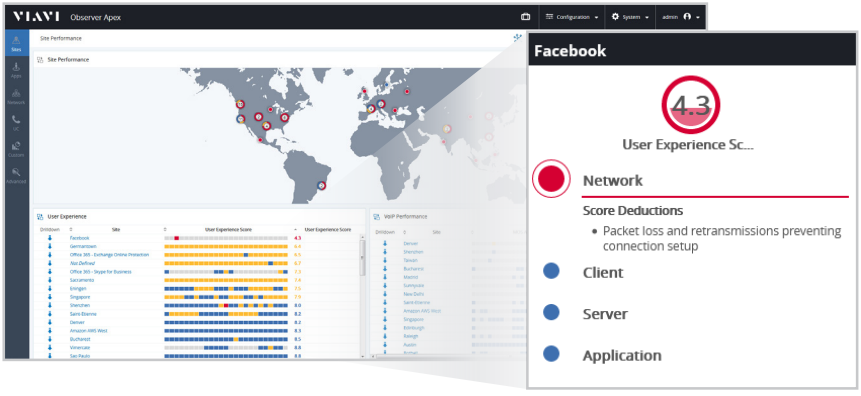
- 深度数据包检测(DPI)功能解决了了解网络流量构成并确定非关键流量是否对关键业务服务和最终用户产生负面影响的难题
- 由 CrowdStrike® 提供威胁情报的 Observer 威胁取证将数据包级洞察与嵌入式对手上下文相结合，以丰富调查，支持更快的分类、高置信度验证和跨混合环境的可操作威胁可见性
- 数字证书分析，识别已过期或即将过期的证书，并突出显示过时的协议，帮助确保用户的合规性和不间断服务
- 统一通信工作流指导统一通信专家从全球摘要和特定于站点的视图到交互式呼叫详细信息。数据包和流数据无缝集成，以可视化网络基础设施中单一点对点或复杂多点呼叫的路径
- 云流量日志接收和分析提供所需的云流量可见性，有助于云环境（如 Amazon Web Services (AWS)和 Microsoft Azure）的安全威胁检测、异常识别和合规性遵守
- 从专门为数据中心构建的设备到虚拟机映像，灵活的部署选项可实现简单高效的云部署

性能管理

最终用户体验分数

Apex 通过机器学习提供的专利分析来准确分析和评估所有对话，从而消除了评估用户满意度的猜测。使用颜色编码和分级从用户的角度表示性能，并考虑独特的环境和应用程序行为以消除误报，每种方法的得分都在 0 到 10 之间。

分数提供了对单个用户体验的可见性，也可以扩展到站点、服务或全球企业视图。Apex 更进一步，通过简单易懂的问题描述将问题隔离到网络、客户端、服务器或应用程序域。



自定义业务级别仪表板

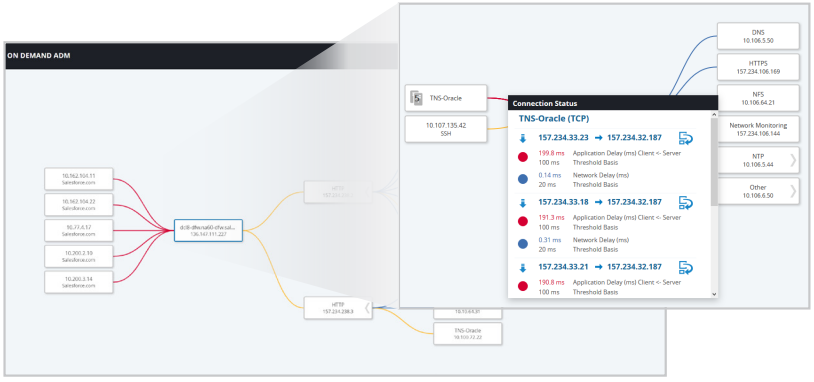
基于地理位置、用户定义的仪表板支持将企业范围的情况感知集成到服务交付状况中。

故障排查工作流

站点和服务驱动的工作流与最终用户体验评分相集成，这意味着 IT 团队可以即时了解所有资源的全球情况，然后快速深入到单个用户，以快速解决问题。

按需多层应用程序智能

按需应用程序依赖关系映射提供多层服务感知、应用程序相互依赖关系的快速发现，以及清晰可视化这些复杂关系的地图临时渲染。只需单击鼠标，Apex 就会生成整个地图，并自动定位和突出显示最差的连接，因此用户可以快速分配故障排查优先级。



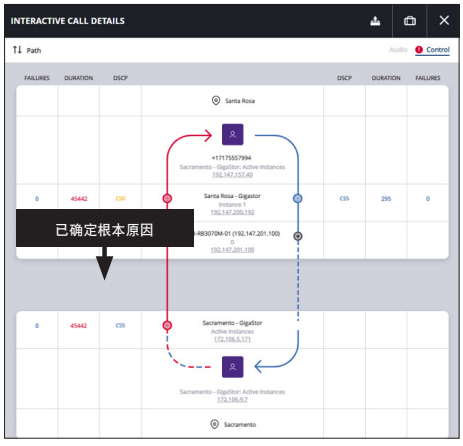
具有集成终端用户体验评分的自动化应用程序依赖关系图

统一通信 (UC)

Apex 统一通信仪表板和工作流可有效指导 VoIP 和统一通信专家从全局摘要和特定站点视图到独特的交互式呼叫详细信息可视化。只有 Observer 将分组和流数据无缝地结合在一起，以可视化单个点对点或复杂的多点呼叫通过网络基础设施的路径，找出质量下降的根源，同时在需要时提供对相关分组数据的一键访问。

主要优势包括：

- **可视化旅程映射：**将数据包和流量数据转换为直观的可视化形式，以方便通话
- **快速解决问题：**通过轻松确定统一通信性能问题的根本原因，显著降低 MTTR
- **用户友好界面：**易于使用和理解的界面，使您能够为非专家提供复杂的多点和点对点 UC 呼叫的简化描述

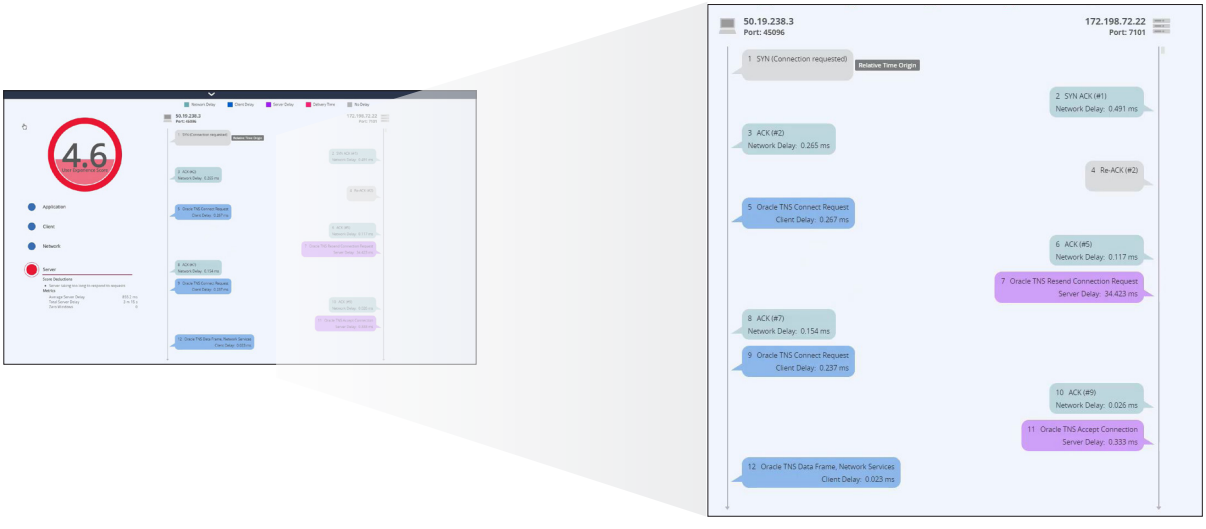


交互式通话详情确定质量下降的根本原因。

网络和安全取证

Observer 网络取证集成了两个互补的数据源；数据包和丰富流，以及将这些数据保留更长时间的能力。虚拟机映像部署选项支持收集和分析云托管应用的丰富流量和数据包。找到许多性能问题和大多数网络安全漏洞的根本原因始于元数据和直观的仪表板，但往往止于逻辑工作流，导致对底层数据的可见性，有时是在事件发生几天后。这就是为什么 Observer 会在更长的时间内保留支持详细信息的原因。

如上所述，许多性能异常可以通过最终用户体验评分快速隔离。然而，当需要更高保真度的细节时，支持数据立即可用。



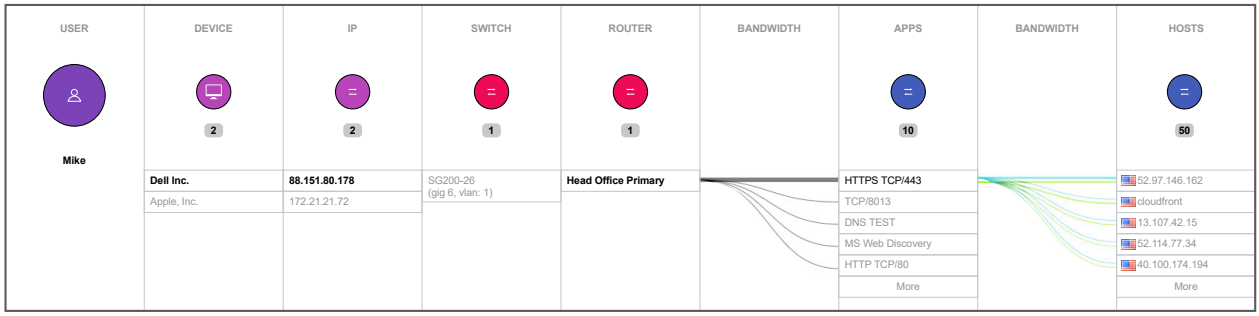
最终用户体验分数及关联连接动态对话突破

对话取证

利用 Observer 捕获的数据包数据，每个事务（从头到尾）都可以用于审查和调查活动。高效的工作流程只需几步，即可随时根据需要将用户从全球仪表板引导至各个数据包。

借助 DPI 驱动的应用识别提供的额外可见性，Observer 提供了高级网络流量洞察。该功能允许网络工程师轻松识别非标准端口上运行的流量，量化非关键流量，并深入研究 HTTP 和 HTTPS 等协议。Observer 的 DPI 功能使您能够识别 4300 多种应用程序，一目了然地确定对话是商业交易还是其他。

丰富数据流取证



Observer GigaFlow IP Viewer 可直观显示网络基础设施中每次对话的用户活动

通过将第 2 层到第 3 层的洞察汇集到一个丰富数据流记录中，Observer 可以生成独特的交互式可视化效果，展示用户、IP 地址、MAC 地址和应用程序在整个网络中的使用情况之间的关系。用户只需输入名称/用户 ID 或 IP 地址，就能立即找到与之相关的所有设备、接口和应用程序。找出您网络中的互联设备和通信者从未如此简单。

数字证书管理

Observer 在分析您的网络流量时监控 SSL/TLS 握手，识别已过期或即将过期的数字证书并提供主动通知。它可以识别发布不安全会话的服务器，突出显示过时的协议，验证合规性，并帮助确保为用户提供不间断的服务。

对于网络工程师和管理员来说，确保正常运行时间和客户满意度对于提供基于 Web 的服务至关重要。从手动报告方法（如电子表格）过渡到主动证书分析方法简化了流程，保护您的公司免受与证书相关的潜在停机影响。

证书分析仪表板提供 TLS 版本、证书到期状态和密码套件分发。

主要优势包括：

主动监控：实时分析、报告和通知让您提前了解证书到期情况

增强的安全洞察力：获得运行中的 SSL 或 TLS 版本的清晰视图，从而快速淘汰过时或不安全的协议

不间断服务：通过识别和补救与证书相关的问题，避免了潜在的运行中断，确保了无缝的用户体验

就网络安全而言，防范威胁的最佳方案需要预防、检测和响应三管齐下的策略。

预防		检测	响应
• 防火墙 • DDoS 预防 • 数据丢失预防 • 入侵预防 • 防病毒和恶意软件	• 加密 • 反垃圾邮件/网络钓鱼 • 访问控制 • 端点安全性	• 入侵检测 • 安全事件管理 (SIEM) • 端点发现	• 网络取证 • 安全事件管理 (SIEM)

对于许多组织来说，重点通常是预防和检测，直到确认入侵并且紧急作战室场景开始对威胁做出响应。在这一点上，随时访问并从当前回溯所有网络活动对于限制损害和自信地发出“解除警报”是至关重要的。

这就是网络取证无价的地方。Observer 结合了流量和丰富的流量取证功能，通过回答每个网络安全漏洞涉及的方式/人员/内容/位置，让您的业务恢复正常运行。

交通流量取证

设备是如何连接的?

谁在进行通信?

丰富数据流取证

传输了什么内容?

有问题的行动延伸到了什么程度?

通过回答这些问题，IT 团队可以快速确定“攻击媒介”（不法分子如何绕过预防和检测措施以获得进入权），以及哪些 IT 服务、设备或敏感的客户/业务数据遭到了破坏。一旦完成这项工作，就有可能进行控制，并最终完成损害评估。

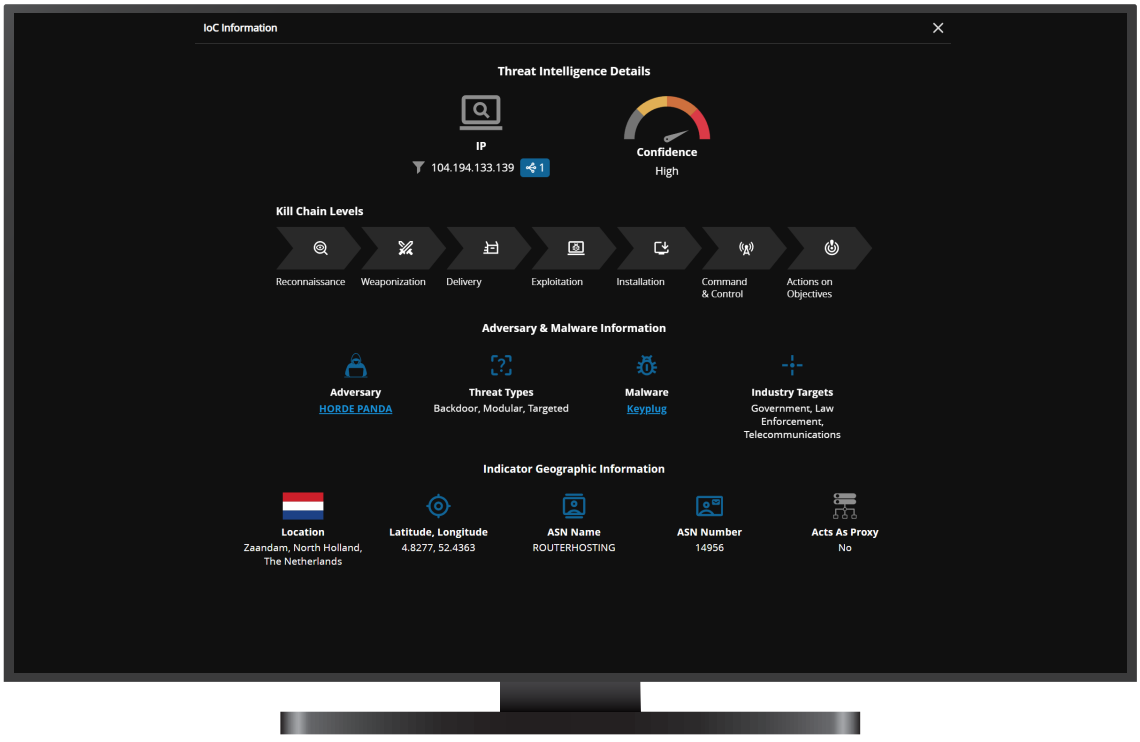
OBSERVER 威胁取证

可操作的威胁可见性，实现自信的响应

Observer 威胁取证系统为网络取证增添了新维度，通过 CrowdStrike® 提供的持续更新的威胁情报，将增强的流数据和数据包层证据融入其中。这使安全团队能够实时将对手行为与可疑流量模式和性能下降相关联。

通过在检测时嵌入危害指标 (IOC)、攻击者 TTP 和其他对手详细信息，Observer 可以实现即时、高置信度的威胁验证，而无需人工拼接或延迟的丰富过程。

无论是已知威胁触发，还是网络流量模式中的异常行为触发，每条告警都包含可直接调用的原始数据包数据和增强型流元数据访问权限，为分析人员提供评估影响、调查范围、确定根本原因并在混合环境中采取果断行动所需的证据。



与通常从第一天开始的传统解决方案不同，Observer 威胁取证支持真正的回顾性分析，允许安全团队将威胁追溯到第零天。通过长期保留的高保真数据，分析人员能够重建完整的攻击时间线，甚至在初始检测之前，就能在单一可信源中追溯根本原因、入侵入口点及横向移动路径。

主要优势包括：

- 网络流量和威胁情报之间的**实时关联**减少了平均解决时间(MTTR)或猜测
- **回顾性分析**提供了零日可见性，为安全分析师提供了在初步检测之前调查威胁活动所需的取证证据
- **嵌入式攻击者上下文**和 TTP 支持可靠的优先级判定和调查
- **数据包证据的直接链接**支持快速深入了解范围和影响评估
- **共享可见性**推动跨 NetOps 和 SecOps 工作流的协作

Observer 威胁取证通过共享的高保真视图将性能和威胁活动关联起来，有助于统一网络和安全运营，从而增强调查并提高跨工作流的信心。集成的丰富流量和元数据提供了实时分类和违规后取证所需的粒度和保留，消除了猜测并加快了问题的解决。

OBSERVER 概述

VIAVI Observer 平台是一个全面的性能和安全管理解决方案，能够为网络、运营和安全团队提供跨混合环境的可操作洞察。Observer Apex 从多个数据源收集事务元数据，用于计算 EUE 分数。它集成了法证级威胁检测和调查，为 NetOps 和 SecOps 团队提供共享可见性和单一事实来源。

作为集成的仪表板和报告资源，Apex 是全球可见性的集中点和快速故障排除的启动点，其优化的工作流可使用数据包、元数据和丰富增强的流来帮助确定根本原因。借助嵌入式威胁环境和对取证数据的直接访问，安全团队可以验证事件、评估影响并快速隔离根本原因。

Observer 以三种基本方式帮助 IT 团队：

- **服务地点** – Observer 提供了对每个托管环境的可观察性，无论是私有云、远程用户，还是分支机构或数据中心的本地部署。无论在哪里，VIAVI Observer 都会为您提供全方位的服务。
- **数据源** - Observer 使用数据包、丰富的流量和元数据提供灵活的可见性选项。这种多层方法支持性能故障排查和违规后取证。借助基于角色的工作流和内容丰富的警报，团队可以在正确的时间使用正确的数据，自信地调查从服务异常到安全威胁的各种问题。
- **部署规模** - 从小规模开始，随着运营和安全需求的发展而扩展。VIAVI 提供灵活的部署模式和分层订阅定价，以满足您的运营支出或资本支出需求，从而实现可扩展的可见性和 NetSecOps 聚合，而无需过度扩展预算或资源。

欲了解更多信息，请访问
viavisolutions.cn/apex

viavisolutions.cn

北京　　电话：+8610 6539 1166
上海　　电话：+8621 6859 5260
上海　　电话：+8621 2028 3588
（仅限 TeraVM 及 TM-500 产品查询）
深圳　　电话：+86 755 8869 6800
网站：　www.viavisolutions.cn

apex-br-ec-zh-cn
30193636 914 1025