FIREEYE™

数据表

FireEye Helix

重新控制您的安全运营

亮点

- **检测高级威胁：**集成 300 多种 FireEye 和非 FireEye 安全工具，而且覆盖上下文威胁情报和行为分析，可提供出众的态势感知。
- **最大限度地减少事故的影响：**通过前线经验配合安全协调和自动化的工作流程，加快响应速度。
- **获得可见性：**无论在内部还是在云端，都可以通过下一代 SIEM 集中安全数据和基础架构，全面了解威胁和漏洞。

简介

网络安全的挑战性不断增加。几乎每天，新的威胁都会暴露公司的漏洞，迫使他们购买更多的产品并雇用更多的人才。这种反应式方法导致复杂性升级，而这又是攻击者可以利用的另外一个漏洞。安全运营无论大小，都需要全面、基础性的方法。FireEye Helix 可帮助组织构建这样的基础。

FireEye Helix 为云托管的安全运营平台，企业可通过该平台控制事故的警报到修复流程。FireEye Helix 可与任何 FireEye 解决方案共同使用，集成您的安全工具，将其与下一代 SIEM、协调流程和威胁情报功能相结合，以捕获未开发的安全投资潜力。该产品由安全专家设计，对于安全专家而言，它使安全团队能够高效地执行警报管理、搜索、分析、调查和报告等主要功能。

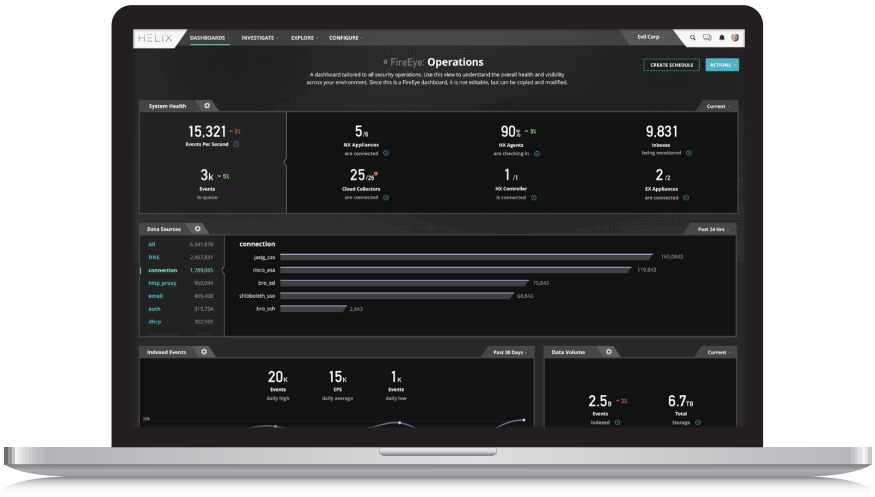

图 1. 可用于获取即时态势感知的操作界面。

FireEye Helix 的作用

通过修正多个工具的数据，检测安全事故

通过情境威胁情报作出明智、有效的决定

集中安全数据和基础架构

威胁情报
检测、丰富、探索和了解最新情报威胁。

下一代 SIEM
通过高级用户行为分析，改进威胁和漏洞检测功能。

安全协调
通过前线工作人员创建的预制手册自动响应。

调查工作台
索引、归档和搜索整个基础架构中所有来源的警报和事件数据，以支持灵活的旋转和快速搜索。

工作流程管理
通过自动和人工工作流在调查过程中组织、分配、协作和采取行动。

合规报告
使用和自定义仪表板和小部件来实现直观聚合，呈现和进一步了解最重要的信息。

如何获取 FireEye Helix 平台

购买 FireEye 基于订阅的解决方案即可随附 FireEye Helix。其适用于所有 FireEye 技术，并集成您安装的非 FireEye 安全产品。随着组织的发展和变化，FireEye 解决方案可以在不中断组织运营的情况下进行重新配置、添加或升级。

若要了解更多关于 FireEye 的信息，请访问：**www.FireEye.com**

FireEye
中国上海市黄浦区淮海路东段淮海中路99号大上海时代广场26楼
China@FireEye.com | www.FireEye.com

H-EXT-DS-US-EN-000050-05

关于 FireEye, Inc.
FireEye 是一家情报主导型安全企业。FireEye 为客户提供无缝式、可扩展的讯息安全解决方案，提供一个将创新型安全技术、国家级威胁情报以及闻名于世的 Mandiant® 咨询集成于一体的平台。通过这种方式，FireEye 为殚精竭虑防备、阻止和应对网络攻击的组织，消除了网络安全的复杂性和负担。