ManageEngine
Log360

# SIEM 如何帮助企业遵守

## 支付卡行业
## 数据安全标准（PCI DSS）


https://www.manageengine.cn/log-management/

支付卡行业数据安全标准 (PCI DSS) 框架对于处理信用卡交易的组织至关重要。支付卡行业安全标准委员会（包括美国运通、Discover、JCB International、万事达卡和 Visa 等主要支付品牌）制定了 PCI DSS，为保护支付卡数据建立了基准。

自 2004 年首次发布以来，该标准已不断发展，以应对新出现的威胁和技术进步。最新版本的 PCI DSS五v4.0 于 2022 年 3 月推出，有来自 200 多个组织的反馈，并采纳了 6,000 多条建议，目的是在复杂且快速变化的支付安全环境中保持相关性。

4.0 版引入了新的要求，并完善了现有要求，扩大了数据安全覆盖范围。这些变化增强了安全控制，明确了指导方针，并在实施和验证安全措施方面提供了更大的灵活性。这一演变标志着向自适应、持续的安全方法的转变，解决了网络威胁的动态性质，并强调了支付卡行业需要最新的、强大的防御措施。

遵守 PCI DSS 需要满足12项关键要求，这些要求通过定期评估、修复和报告来实现持续改进。本指南将深入探讨安全信息和事件管理（SIEM）解决方案的高级功能如何与 PCI DSS 的更新要求保持一致并支持合规性。

## SIEM 在 PCI DSS 合规性中的作用

对于处理持卡人数据的组织而言，实现并保持对 PCI DSS v4.0 的遵守至关重要。SIEM 解决方案可以克服保护敏感信息方面日益增加的挑战。这些解决方案提供了多方面的方法来满足各种 PCI DSS 要求，对于中型和大型组织尤其重要。

例如，SIEM 解决方案擅长监控、警报和记录网络安全控制所需的事件（PCI DSS 要求 1.2、1.3），这使得监控和限制持卡人数据环境的网络访问、监控关键网络配置的更改变得更加容易。这项功能对于防止未经授权的访问至关重要。管理受信任网络与不受信任网络之间的连接（要求 1.4）也是 SIEM 提供重要支持的领域。SIEM 通过及时检测和响应潜在的安全威胁来实现这一目标，能够识别恶意流量。

关于反恶意软件和反网络钓鱼机制（5.2、5.3、5.4），SIEM 解决方案通过与反恶意软件工具和威胁源集成来提高安全性。这种集成增强了组织检测、警报和跟踪的能力。并能够应对恶意软件和网络钓鱼攻击。

SIEM 解决方案的突出特点是其全面的审计日志记录能力 (10.2)。它们在各种系统和应用程序中实施广泛的日志记录，支持异常检测和可疑活动监控。这有助于进行取证分析，并确保网络内的所有操作都是可追溯的，符合 PCI DSS 的基本要求。审计日志也受到保护，以防止未经授权的修改 (10.3)，并配置警报以识别可疑活动 (10.4)。这种警惕性对于保护组织免受可能随时从任何媒介出现的威胁至关重要。

此外，SIEM 解决方案支持检测的并响应网络入侵和意外文件更改（11.5），通过文件完整性监控提供额外的安全保障。

因此，SIEM 解决方案对于满足 PCI DSS 的要求至关重要v4.0。其全面的功能（包括日志记录、实时监控和网安全）完全符合这PCI DSS。在快速发展的网络威胁形势下，SIEM 是任何致力于保护其持卡人数据环境的组织的核心组件。

## 卓豪 Log360 如何满足 PCI DSS v4.0要求

| PCI DSS 编号 | 明确方法要求 | Log360 如何提供帮助 |
|---|---|---|
| **1.2 配置并维护网络安全控制（NSC）。** | | |
| 1.2.2 | 对网络连接和 NSC 配置的所有变更均按照要求 6.5.1 中定义的变更控制流程进行批准和管理。 | Log360 监控和审计所有网络活动和配置更改。配置更改监控确保所有更改都被记录，为变更控制过程中的审查和批准提供审计追踪。 |
| 1.2.8 | NSC 的配置文件具有以下特点：防止未经授权的访问，并与活动网络配置保持一致。 | Log360 的文件完整性监控 (FIM) 插件可保护 NSC 配置文件免遭未经授权的访问。它会跟踪这些文件的更改，确保它们与活动配置保持一致。 |
| **1.3 对持卡人数据环境的网络访问受到限制。** | | |
| 1.3.1 | 到 CDE 的入站流量受到如下限制：仅限必要的流量，所有其他流量被明确拒绝。 | Log360 的实时监控有助于确保允许必要的流量。可以立即标记和调查不必要或可疑的入站网络流量。 |
| 1.3.2 | CDE 的出站流量受到如下限制：仅限必要的流量，所有其他流量均被明确拒绝。 | 与入站流量监控类似，Log360 可以跟踪来自 CDE 的出站流量，仅允许必要的通信并标记任何未经授权或意外的流量模式以供调查。 |

| | | |
|---|---|---|
| **1.4 可信网络与不可信网络之间的网络连接受到控制。** | | |
| 1.4.4 | 存储持卡人数据的系统组件不能从不受信任的网络直接访问。 | 虽然 Log360 不控制访问，但它可以监控和审核网络连接，以确保存储持卡人数据的系统不会被不受信任的网络访问。 |
| 1.4.5 | 内部 IP 地址和路由信息的披露仅限于授权方。 | Log360 的审计功能包括检测并警告内部 IP 地址和路由信息未经授权的披露。 |
| **1.5 能够同时连接到不受信任的网络和 CDE 的计算设备并给CDE 造成的风险得到缓解。** | | |
| 1.5.1 | 安全控制在任何计算设备（包括公司和员工拥有的设备）上实施，这些设备连接到不受信任的网络和 CDE，如下所示：特定配置设置、主动运行的安全控制、用户无法更改的安全控制。 | Log360 可以监控和报告设备的安全态势，确保遵守所需的安全控制。 |
| **2.2 系统组件的安全配置和管理。** | | |
| 2.2.2 | 供应商默认账户的管理如下：如果使用，则根据要求 8.3.6 更改默认密码，如果不使用，则删除或禁用该帐户。 | Log360 可以跟踪和报告用户帐户变化，包括供应商默认帐户，确保遵守密码和帐户管理政策。 |
| **2.3 无线环境的安全配置和管理。** | | |
| 2.3.1 | 对于连接到 CDE 或传输帐户数据的无线环境，所有无线供应商默认值都会在安装时更改或确认是安全的，包括但不限于：默认无线加密密钥、无线接入点上的密码、SNMP 默认值。 | Log360 可以审核无线网络配置的变化，确保所有默认设置都是安全的并且符合 PCI DSS 要求。 |
| 2.3.2 | 对于连接到 CDE 或传输帐户数据的无线环境，无线加密密钥会根据需要更改。 | Log360 可以监控并报告无线加密密钥的变化，确保它们符合 PCI DSS 要求进行更新。 |
| **3.4 对完整 PAN（主账号）显示的访问和复制 PAN 的能力受到限制。** | | |
| 3.4.2 | 使用远程访问技术时，技术控制可防止所有人员复制和/或重新定位 PAN，但拥有记录在案的明确授权和合法、明确的业务需求的人员除外。 | Log360 不直接控制对 PAN 数据的访问，但可以监控和警告未经授权的访问或复制 PAN 的行为，尤其是通过远程访问技术。 |

| | | |
|---|---|---|
| **5.2 预防、检测并处理恶意软件（malware）。** | | |
| 5.2.1 | 所有系统组件上都部署了反恶意软件解决方案，但根据要求 5.2.3 的定期评估确定的系统组件除外，这些系统组件不存在恶意软件威胁。 | Log360 通过持续监控和日志分析帮助识别哪些系统组件面临恶意软件的威胁，支持本条款要求的定期评估。 |
| 5.2.2 | 部署的反恶意软件解决方案可检测所有已知类型的恶意软件，并删除、阻止或包含所有已知类型的恶意软件。 | Log360 通过提供与恶意软件相关的任何活动的详细日志和警报来帮助检测过程，从而提高部署的反恶意软件解决方案的有效性。 |
| **5.3 反恶意软件机制和流程处于活跃状态、维护并受到监控。** | | |
| 5.3.1 | 反恶意软件解决方案通过自动更新保持最新。 | 虽然 Log360 不会直接更新反恶意软件解决方案，但它可以监控和记录这些解决方案的更新状态，确保它们是最新且有效的。 |
| 5.3.2 | 反恶意软件解决方案执行定期扫描和主动或实时扫描，或者对系统或进程执行持续的行为分析。 | Log360 通过其日志管理功能支持监控反恶意软件活动，包括定期和实时扫描。 |
| 5.3.3 | 对于可移动电子媒体，反恶意软件解决方案会在插入、连接或逻辑安装时执行自动扫描或持续行为分析。 | Log360 可以跟踪和记录与可移动媒体相关的活动，有助于执行反恶意软件扫描。 |
| 5.3.4 | 反恶意软件解决方案的审计日志已按照要求 10.5.1 启用并保留。 | Log360 可以收集、保留和管理来自各种反恶意软件解决方案的审计日志，确保符合要求 10.5.1。 |
| 5.3.5 | 反恶意软件机制不能被用户禁用或更改，除非有专门记录，并在有限的时间内由管理层逐案授权。 | 如果反恶意软件解决方案被更改或禁用，Log360 的警报系统可以通知管理员，从而 有助于执行此要求。 |
| **5.4 反网络钓鱼机制保护用户免受网络钓鱼攻击。** | | |
| 5.4.1 | 我们已经制定了流程和自动化机制来检测并保护人员免受网络钓鱼攻击。 | Log360 具有针对 Microsoft 365 和 Exchange Server 的审计功能，可确保有效识别和阻止网络钓鱼企图。它通过分析入站和出站电子邮件流量来监控、分析和警告恶意附件。 |

| | | |
|---|---|---|
| **6.3 识别并解决安全漏洞。** | | |
| 6.3.1 | 使用业界认可的来源来识别和管理安全漏洞，分配风险等级，涵盖定制和第三方软件的漏洞。 | Log360 通过与漏洞扫描程序的集成，可以帮助识别和管理安全漏洞，并提供合规日志和报告。 |
| **6.4 面向公众的网络应用程序受到保护，免受攻击。** | | |
| 6.4.1 | 对于面向公众的网络应用程序，会持续解决新的威胁和漏洞，并通过审查或自动化技术解决方案防范已知攻击。 | Log360 可以监控和记录 Web 服务器和应用程序活动，帮助检测面向公众的 Web 应用程序的威胁和漏洞。 |
| 6.4.2 | 对于面向公众的 Web 应用程序，部署了一种自动化技术解决方案，可以持续检测和防止基于 Web 的攻击，生成审计日志并配置为阻止攻击或生成警报以供调查。 | Log360 的实时监控和警报功能可以帮助检测针对面向公众的应用程序的基于网络的攻击。 |
| **7.2 对系统组件和数据的访问权限得到适当的定义和分配。** | | |
| 7.2.4 | 所有用户帐户和相关访问权限（包括第三方/供应商帐户）都会定期审查，以确保其仍然合适，并解决任何不适当的访问权限。 | Log360 可以定期审查和报告用户帐户权限并确保其保持按配置配置。 |
| 7.2.5.1 | 所有应用程序和系统帐户的访问以及相关的访问权限都会定期审查，并处理任何不适当的访问，并且管理层确认访问仍然是适当的。 | Log360 还可以审查和报告应用程序和系统帐户访问，帮助确保遵守此要求。 |
| 7.2.6 | 用户对存储的持卡人数据的查询存储库的访问受到限制，禁止直接进行未过滤的查询访问，除非由授权管理员执行。 | Log360 可以监控和审计数据库查询，确保对存储的持卡人数据的访问受到限制。 |
| **8.2 在账户的整个生命周期内，对用户和管理员的用户身份和相关账户进行严格的管理。** | | |
| 8.2.5 | 已终止的用户的访问权限将被立即撤销。 | Log360 监控并报告用户帐户状态，以确保及时撤销终止用户的访问权限。 |
| 8.2.6 | 不活跃的用户帐户将在 90 天内被删除或禁用。 | Log360 可以识别并报告不活动的用户帐户，帮助及时删除或禁用这些帐户。 |

| | | |
|---|---|---|
| 8.2.7 | 第三方用于通过远程访问来访问、支持或维护系统组件的帐户管理如下：仅在需要的时间段内启用，不使用时禁用，监控使用情况以防意外活动。 | Log360 可以监控和管理第三方账户的使用情况，确保仅在需要时启用这些账户，否则禁用。 |
| **8.3 建立并管理针对用户和管理员的强身份验证。** | | |
| 8.3.4 | 无效身份验证尝试的限制如下：尝试次数不超过 10 次后锁定用户 ID，将锁定时间设置为最短 30 分钟或直到确认用户身份。 | Log360 跟踪并报告失败的登录尝试。当失败尝试次数超过阈值时，它可以向管理员发出警报，从而帮助遵守用户 ID 锁定策略。 |
| 8.3.5 | 如果使用密码/密码短语作为身份验证因素，则会为每个用户设置和重置密码，如下所示：首次使用时设置为唯一值，重置后强制在首次使用后立即更改。 | 虽然 Log360 不直接管理密码重置，但它会监控并报告 Active Directory 环境中的密码重置活动和策略变化。 |
| 8.3.6 | 如果使用密码/密码短语作为身份验证因素，则它们需要满足以下最低复杂程度：最小长度为 12 个字符（如果系统不支持 12 个字符，则为 8 个字符），包含数字和字母字符。 | Log360 不直接强制执行密码复杂性，但可以报告 Active Directory 中的密码策略变化，帮助确保符合复杂性要求。 |
| **10.2 审计日志用于支持异常和可疑活动的检测以及事件的取证分析。** | | |
| 10.2.1 | 所有系统组件和持卡人数据的审计日志均已启用并处于活动状态。 | Log360 收集并存储来自各种来源的审计日志，确保审计日志持续活跃并可用于所有系统组件和持卡人数据。 |
| 10.2.1.1 | 审计日志捕获所有个人用户对持卡人数据的访问。 | Log360 通过帮助满足监控和捕获个人用户活动的要求，捕获包括用户访问持卡人数据在内的详细日志。 |
| 10.2.1.2 | 审计日志记录任何具有管理权限的个人采取的所有操作，包括应用程序或系统帐户的任何交互式使用。 | Log360 专门监控和记录所有管理活动，包括系统更改和数据访问，确保全面记录所有关键操作。 |
| 10.2.1.3 | 审计日志捕获对审计日志的所有访问。 | Log360 确保对其自身审计日志的所有访问都受到监控和记录，符合记录审计日志访问的要求。 |

| | | |
|---|---|---|
| 10.2.1.4 | 审计日志捕获所有无效的逻辑访问尝试。 | Log360 记录所有无效访问尝试，为安全分析提供此类事件的详细见解。 |
| 10.2.1.5 | 审计日志记录所有身份和身份验证凭据的更改，包括：创建新帐户、提升权限、更改帐户<br><br>管理访问权限。 | Log360 可以记录并警告身份识别和身份验证凭证的更改，包括帐户创建和权限提升。 |
| 10.2.1.6 | 审计日志捕获：所有新审计日志的初始化，所有现有审计日志的启动、停止或暂停。 | Log360 确保捕获并报告审计日志的初始化或修改等事件。 |
| 10.2.1.7 | 审计日志捕获系统级对象的所有创建和删除。 | Log360 跟踪并记录系统级对象的创建和删除，提供合规性必要的审计跟踪。 |
| 10.2.2 | 审计日志记录每个可审计事件的详细信息：用户身份、事件类型、日期和时间、成功和失败指示、事件的起源、受影响数据的身份或名称、系统组件、资源或服务。 | Log360 捕获可审计事件的全面详细信息，包括用户身份、事件类型、日期和时间以及成功和失败指示。 |
| **10.3 审计日志受到保护，不得破坏和未经授权的修改。** | | |
| 10.3.1 | 只有具有工作相关需要的人员才有权读取审计日志文件。 | Log360 通过基于角色的访问控制来限制对审计日志的访问，确保只有授权人员才能查看日志，符合与工作相关的要求。 |
| 10.3.2 | 审计日志文件受到保护，以防止个人修改。 | Log360 的安全存储和受限访问可防止未经授权修改审计日志文件。它还可保留对日志的任何访问或更改的清晰审计跟踪。 |
| 10.3.3 | 审计日志文件（包括面向外部的技术的日志文件）会及时备份到安全的、中央的、内部的日志服务器或其他难以修改的媒体。 | Log360 有助于将日志文件及时备份到安全的集中式服务器。这可确保来自各种来源（包括面向外部的技术）的日志得到安全存档和保护。 |
| 10.3.4 | 审计日志使用文件完整性监控或变化检测机制，以确保现有日志数据不会被更改，除非生成警报。 | Log360 采用文件完整性监控和变化检测机制，对日志文件的任何未经授权的更改向管理员发出警报，确保日志数据的完整性。 |

| | | |
|---|---|---|
| **10.4 审查审计日志以识别异常或可疑活动。** | | |
| 10.4.1 | 以下审计日志每天至少审查一次：所有安全事件、存储、处理或传输 CHD 和/或 SAD 的所有系统组件的日志、所有关键系统组件的日志、执行安全功能的所有服务器和系统组件的日志。 | Log360 的自动日志收集和分析功能有助于每日审查所有必要的审计日志。它可以根据特定标准（例如安全事件和关键组件的操作）生成报告和告警。 |
| 10.4.1.1 | 使用自动化机制来执行审计日志审查。 | Log360 利用其先进的分析和报告功能自动化审计日志审查流程，确保持续监控并及时检测任何安全事件或违反政策的行为。 |
| 10.4.2 | 所有其他系统组件的日志都会定期审查。 | Log360 的自动日志报告允许定期和系统地检查来自各个系统组件的日志，以满足定期审查要求。 |
| 10.4.2.1 | 所有其他系统组件的定期日志审查频率在实体的目标风险分析中定义。 | Log360 允许定制日志报告计划，使组织能够根据其风险分析和合规性要求定义频率。 |
| 10.4.3 | 解决审查过程中发现的例外和异常。 | Log360 的高级分析和警报机制有助于在日志审查期间识别和解决异常和异常，确保及时响应潜在问题。 |
| **10.5 审计日志历史记录保留并可供分析。** | | |
| 10.5.1 | 保留审计日志历史记录至少 12 个月，其中至少最近三个月的历史记录可立即用于分析。 | Log360 的日志保留设置可以配置为保留 12 个月或更长时间的日志，并可以立即访问最近三个月的日志，有助于高效分析和合规。 |
| **10.6 时间同步机制支持所有系统的一致时间设置。** | | |
| 10.6.1 | 采用时间同步技术实现系统时钟和时间的同步。 | Log360 依赖于底层系统的时间同步，但确保所有日志数据都根据系统时间一致地加盖时间戳，以便进行准确的事件跟踪。 |
| 10.6.3 | 时间同步设置和数据受到如下保护：只有有业务需要的人员才能访问时间数据，对关键系统上时间设置的任何更改都会被记录、监控和审查。 | Log360 可以监控并记录系统时间设置的任何更改，确保时间同步数据和设置的安全且可审计。 |

| | | |
|---|---|---|
| **10.7 及时发现、报告和应对关键安全控制系统的故障。** | | |
| 10.7.1 | 关键安全控制系统的故障会被及时检测、警告和处理，包括但不限于以下关键安全控制系统的故障：网络安全控制、IDS/IPS、FIM、反恶意软件解决方案、物理访问控制、逻辑访问控制、审计日志机制、分段控制（如果使用）。 | Log360 可以配置为监控和警告各种安全控制故障，确保快速检测和响应这些系统的任何问题。 |
| 10.7.2 | 关键安全控制系统的故障会被及时检测、警告和处理，包括但不限于以下关键安全控制系统的故障：网络安全控制、IDS/IPS、变更检测机制、反恶意软件解决方案、物理访问控制、逻辑访问控制、审计日志机制、分段控制（如果使用）、审计日志审查机制、自动安全测试工具（如果使用）。 | 通过 Log360，管理员可以立即收到关键安全控制故障的警报，从而能够迅速采取行动解决和降低风险。 |
| 10.7.3 | 任何关键安全控制系统的故障都会得到迅速响应，包括但不限于：恢复安全功能、识别和记录安全故障的持续时间、识别和记录故障原因和所需的补救措施、确定是否需要采取进一步的措施来应对安全故障、实施控制以防止故障原因再次发生、恢复对安全控制的监控。 | Log360 通过其警报和报告功能支持快速响应机制，有助于快速解决安全控制故障。 |
| **11.2 识别和监控无线接入点，并处理未经授权的无线接入点。** | | |
| 11.2.1 | 授权和未授权的无线接入点的管理如下：测试无线（Wi-Fi）接入点的存在，检测和识别所有授权和未授权的无线接入点，每三个月至少进行一次测试、检测和识别。 | 通过与网络监控工具集成，Log360 可以帮助检测和记录授权和未授权的无线接入点。 |

| | | |
|---|---|---|
| **11.5 检测并应对网络入侵和意外文件更改。** | | |
| 11.5.1 | 入侵检测和/或入侵预防技术用于检测和/或预防网络入侵，如下所示：在 CDE 的周边监控所有流量，在 CDE 的关键点监控所有流量，对疑似入侵行为发出警报，所有入侵检测和预防引擎、基线和签名均保持最新。 | Log360 利用先进的入侵检测/预防技术来监控 CDE 周边和关键点的流量，并向相关人员发出可疑入侵警报。它还可确保检测引擎和签名得到更新。 |
| 11.5.1.1 | 入侵检测和/或入侵预防技术可以检测、警告/预防并解决隐蔽的恶意软件通信渠道。 | Log360 的入侵检测功能可以识别并警告隐蔽的恶意软件通信渠道，增强网络安全性以抵御复杂威胁。 |
| 11.5.2 | 变更检测机制的部署如下：提醒人员注意关键文件的未经授权的修改，每周至少执行一次关键文件比较。 | Log360 的变化检测机制会向人员发出警报，告知关键文件的未经授权的修改，并至少每周进行一次文件比较，以帮助遵守此要求。 |
| **A1.2 多租户服务提供商为所有客户提供日志记录和事件响应便利。** | | |
| A1.2.2 | 一旦发生任何客户疑似或确认的安全事件，我们将实施流程或机制来支持和/或促进及时进行法医调查。 | Log360 通过其全面的事件管理模块促进法医调查。这有助于及时调查任何客户的安全事件。 |
| A1.2.3 | 实施用于报告和处理疑似或确认的安全事件和漏洞的流程或机制，包括：客户可以安全地向提供商报告安全事件和漏洞，提供商根据要求 6.3.1 处理和补救疑似或确认的安全事件和漏洞。 | Log360 支持报告和解决安全事件和漏洞的机制，包括为客户提供安全的报告渠道和符合要求 6.3.1 的及时补救措施。 |
| **A3.5 识别可疑事件并作出反应。** | | |
| A3.5.1 | 实施一种方法来快速识别系统中的攻击模式和不良行为，包括：识别发生的异常或可疑活动，在检测到可疑活动或异常时向负责人员发出及时警报，根据记录的响应程序对警报做出响应。PCI DSS 参考：要求 10、12 | Log360 实施了实时识别异常或可疑活动、发出及时警报以及促进符合 PCI DSS 的记录响应程序的方法要求。 |

将 PCI DSS 合规性纳入更广泛的 IT 安全范围是至关重要的。此过程需要对当前安全协议进行详细评估，并实施强有力的策略来解决任何安全漏洞。Log360 可以通过将持续、自动化和智能的安全实践嵌入到组织 IT 基础设施的核心中来重新定义组织的合规性态势。

Log360 凭借其在实时日志管理和 IT 合规方面的高级功能引领了这一转型。它通过推广主动应对网络威胁的方法，为集中日志记录、实时监控和威胁检测提供了一种用户友好、全方位的解决方案。Log360 通过自动生成 PCI DSS 报告简化了合规过程。与威胁情报源的集成尤其有益，因为它允许实时更新新出现的安全威胁。此功能可确保组织的安全协议和合规工作始终与最新的威胁形势保持一致，从而降低维护 PCI DSS 合规性所需的复杂性和工作量。

您可以直接下载并试用 Log360 的产品功能，我们支持30 天免费的试用。

## 我们的产品

AD360| ADAudit Plus| EventLog Analyzer |DataSecurity Plus
Exchange Reporter Plus | M365 Manager Plus

ManageEngine
Log360

Log360 是一款集成 DLP 和 CASB 功能的统一 SIEM 解决方案，可检测、确定优先级、调查和应对安全威胁。该解决方案的 TDIR 模块 Vigil IQ 结合了威胁情报、基于 ML 的异常检测和基于规则的攻击检测技术来检测复杂的攻击，并提供事件管理控制台来有效补救检测到的威胁。Log360 凭借其直观和先进的安全分析和监控功能，在本地、云和混合网络中提供全面的安全可见性。有关 Log360 的更多信息，请访问 https://www.manageengine.cn/log-management/。

获取报价 下载