# **API安全平台快速用户指南**

# **一．仪表盘**

**APISEC**自动收集已处理流量的指标，并在**仪表盘APISEC**控制台部分。仪表板允许任何用户分析恶意和合法流量趋势，并获取一段时间内的应用程序漏洞状态。

指标显示如下几项:

**-当月的统计数据和遇到请求的速度**

**-正常和恶意流量**

**-攻击类型**

**-API协议**

**-攻击来源**

**-攻击目标**

**-漏洞扫描器**

**当月的统计数据和遇到请求的速度**

小组件显示以下数据:

-订阅计划中指定的每月请求配额

-当月检测到的点击数和被阻止的点击数

-遇到请求和命中的实时速度



**正常和恶意流量**

小部件显示以下数据：

-流量

-请求、命中和事件的数量

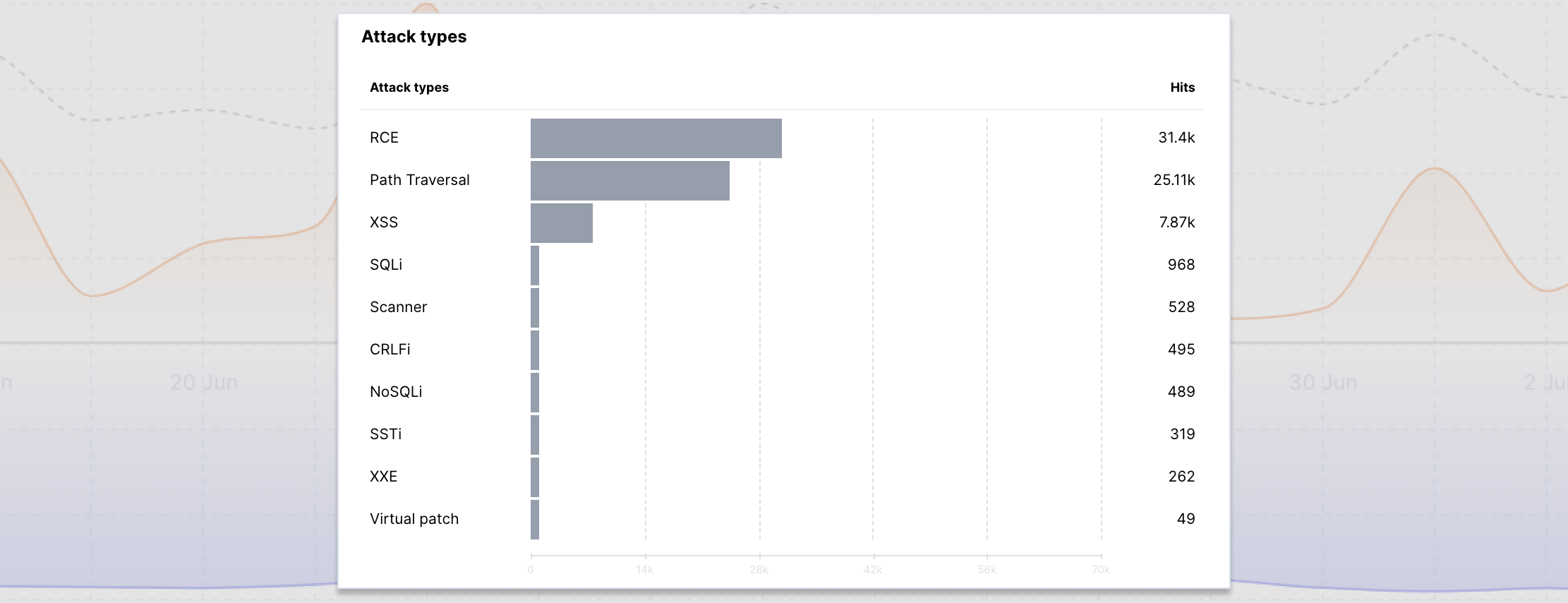
-攻击者的估计攻击成本：该值考虑了IP地址租用的近似成本和攻击持续时间



**攻击类型**

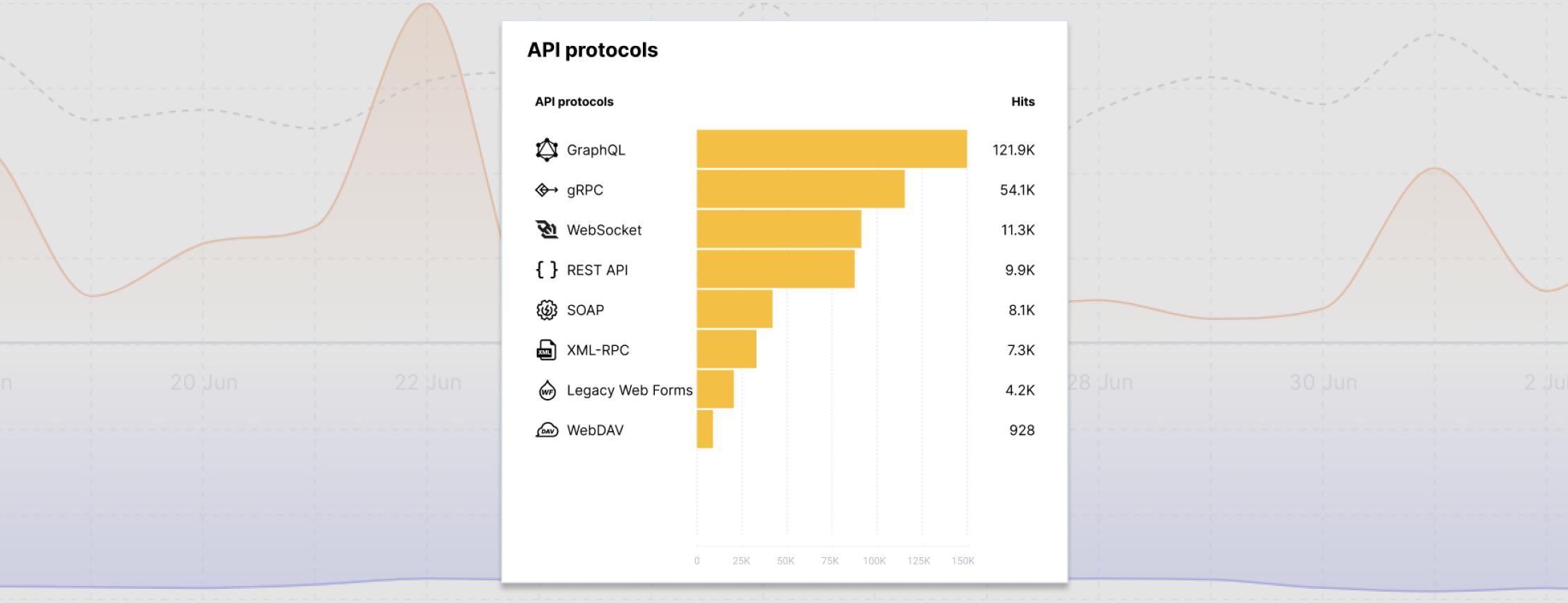
此小部件显示检测到的攻击的顶级类型，有助于分析恶意流量模式和攻击者行为。

使用这些数据，您可以分析服务对不同攻击类型的脆弱性，并采取适当的措施来提高服务安全性。



**API协议**

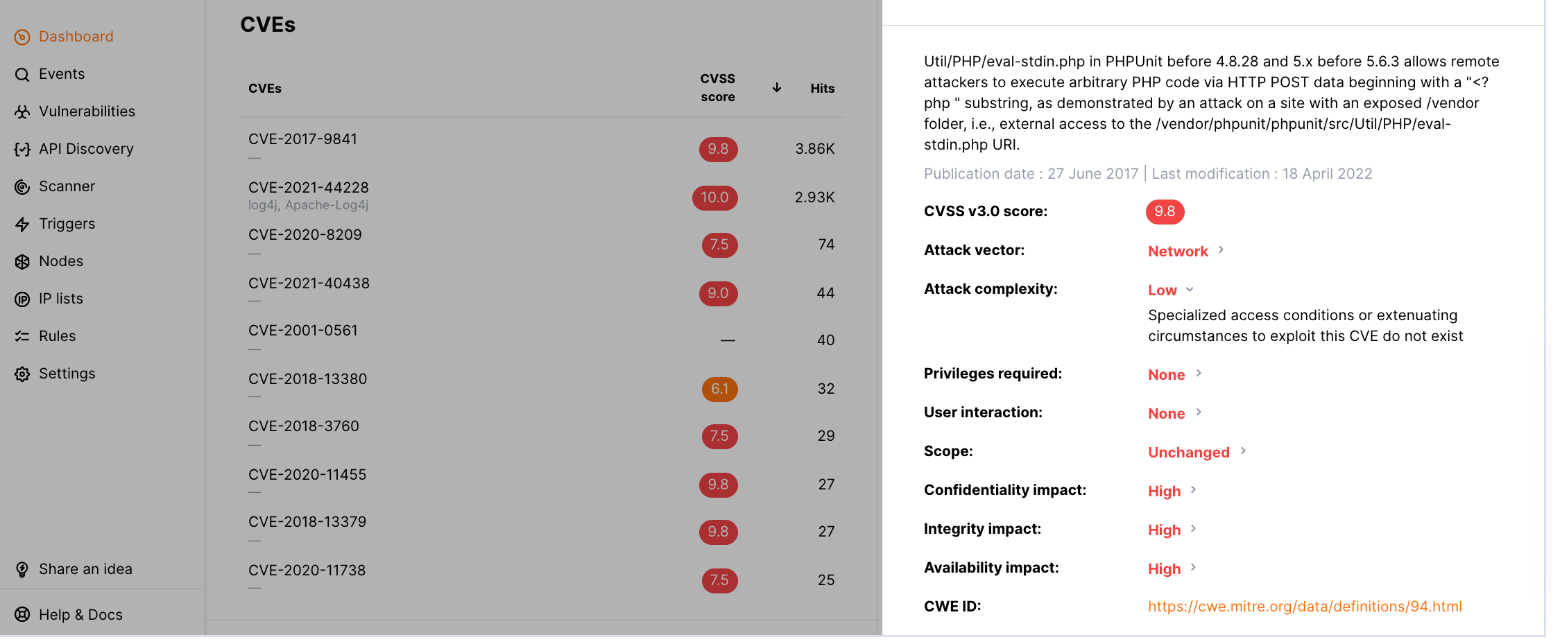
此小部件显示攻击者使用的API协议的统计信息。Wallarm可以识别以下API协议：GraphQL、gRPC、WebSocket、REST API、SOAP、XML-RPC、JSON-RPC、WebDAV



使用该小部件，您可以分析通过特定协议发送的恶意请求，并评估系统对此类请求的脆弱性。

**CVEs**

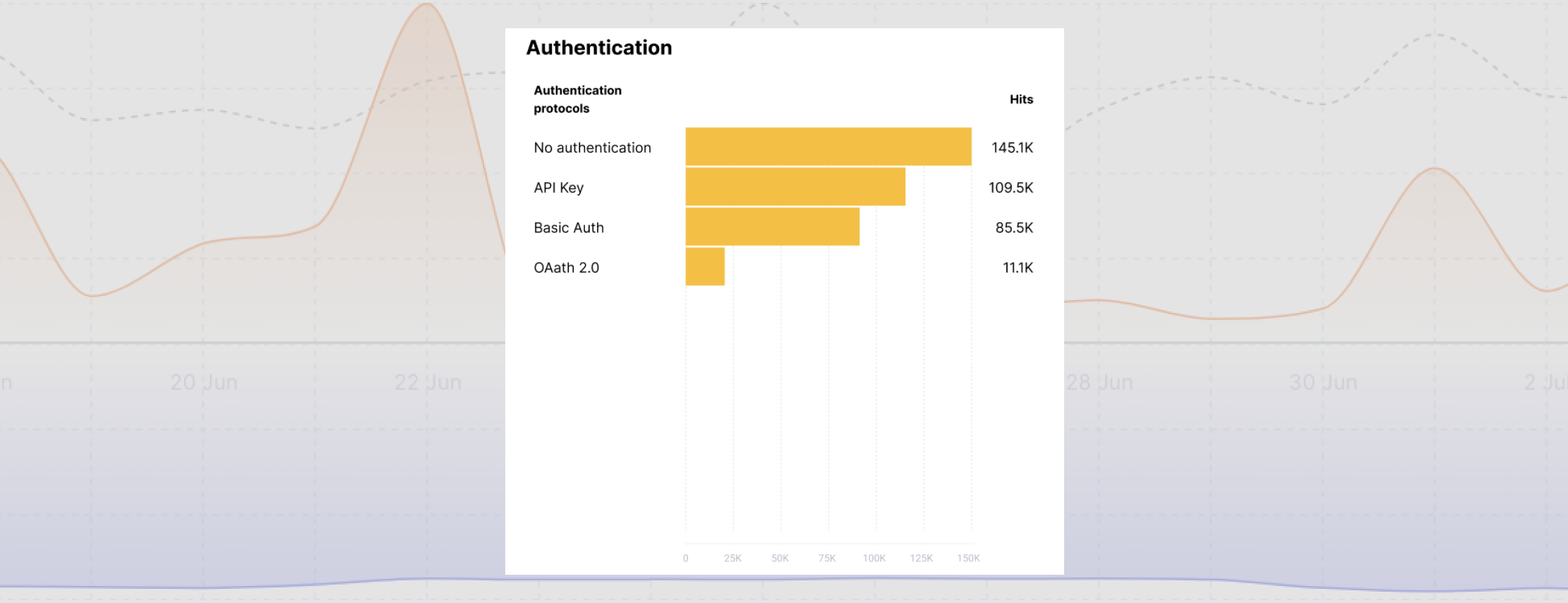
CVEs小部件显示了攻击者在选定时间范围内利用CVE漏洞的TOP排序，通过更改排序类型，您可以了解最新的CVE，可以跟踪受攻击最多的CVE。



每个CVE都附有从漏洞数据库收到的CVSS v3.0分数、攻击复杂性、所需权限等详细信息。2015年之前注册的漏洞未提供CVSS v3.0评分。

**身份验证**

此小部件显示攻击者在指定时间内使用的身份验证方法，



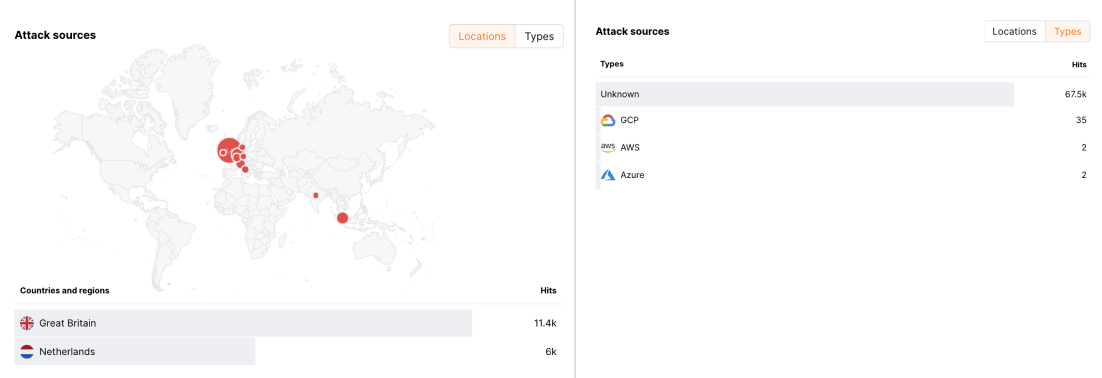
例如：API密钥、基本身份验证、不记名令牌、Cookie Auth等。

**攻击源**

此小部件显示有关攻击源组的统计信息：

位置

类型，例如Tor、Proxy、VPN、AWS、GCP等。



这些数据可以帮助定义滥用攻击源，并通过使用IP地址的灰色或拒绝列表来阻止来自这些攻击源的请求。

您可以在单独的选项卡上查看每个源组的数据。

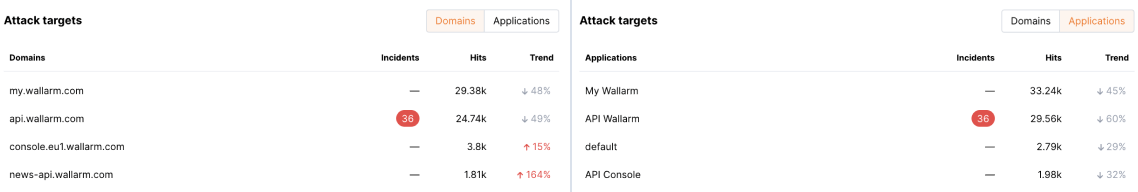
**攻击目标**

此小部件显示受攻击最多的域和应用程序。为每个对象显示以下指标：

-检测到的事件数

-检测到的命中数

-趋势：所选时期和前一时期的点击量变化。例如：如果您检查上个月的统计数据，则趋势将显示上个月和上上个月之间的点击数差异（百分比）



您可以在单独的选项卡上查看域和应用程序的数据。

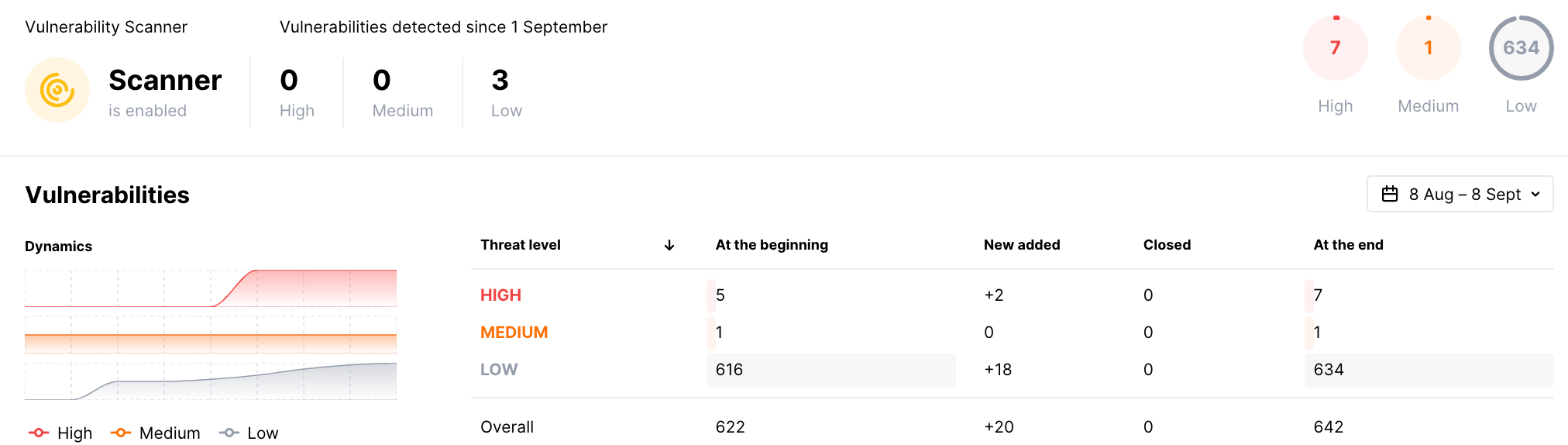
**漏洞扫描器**

Scanner小部件显示在公共资产中检测到的漏洞的统计信息:

-在所选期间检测到的所有风险级别的漏洞数量

-在所选期间结束时，所有风险级别的活动漏洞数量

-选定期间所有风险级别漏洞数量的变化

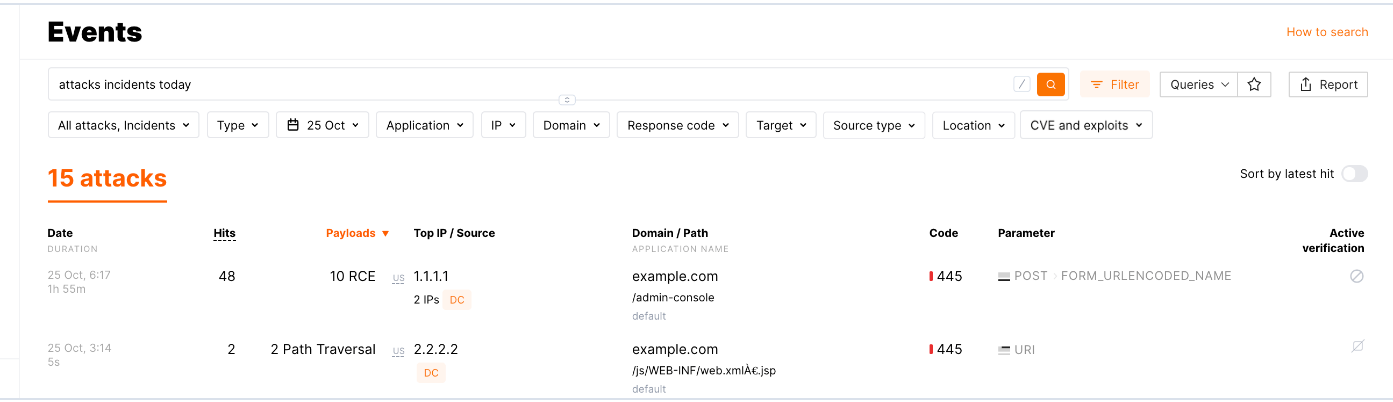


# **二．事件**

**检查事件**

您可以在API安全控制台的事件部分检查检测到的攻击、事件和漏洞。要查找所需的数据，请使用此处描述的搜索字段或手动设置所需的搜索筛选器。

1. **攻击**



**日期：**恶意请求的日期和时间。

-如果在短时间内检测到多个相同类型的请求，则攻击持续时间将显示在日期下。持续时间是在指定的时间段内，某一类型的第一个请求和同一类型的最后一个请求之间的时间段。

-如果攻击发生在当前时刻，则会显示相应的标签。

**请求(点击次数)：**在指定的时间范围内，攻击中的请求数（命中数）。

**有效载荷：**攻击类型和唯一恶意有效载荷的数量。

**Top IP/Source**：发起恶意请求的IP地址。当恶意请求来自多个IP地址时，界面显示负责大多数请求的IP地址。还显示了IP地址的以下数据：

-在指定时间段内发起同一攻击的请求的IP地址总数。

-注册IP地址的国家/地区（如果在IP2Location等数据库中找到）

-源类型，如公共代理、Web代理、Tor或IP注册的云平台等（如果在IP2Location等数据库中找到）

**域/路径：**请求目标的域、路径和应用程序ID。

**颜色指示器显示攻击阻止的状态：**

-橙色指示器，如果攻击的所有命中都被记录，但由于过滤节点在监控模式下运行，因此过滤节点未阻止。如果您的应用程序阻止了攻击（例如，应用程序返回403禁止），则指示器仍为橙色，代码列将显示应用程序返回的代码。

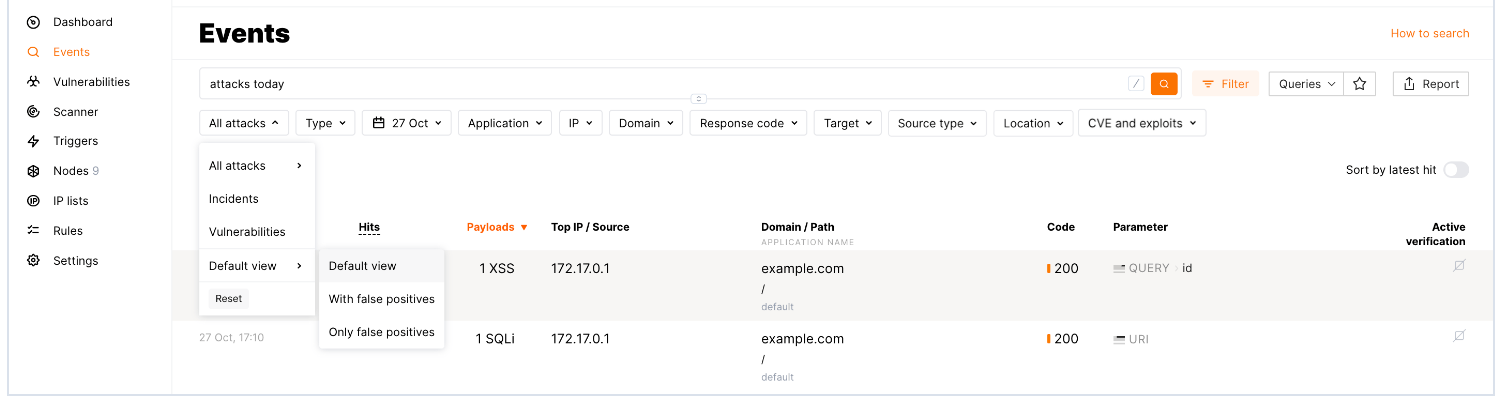
-红色指示器，如果攻击的所有命中都被过滤节点阻止。

-如果攻击的某些命中被阻止，而其他命中仅被记录（某些命中的过滤模式设置为监控），则红色带白色指示灯。

**代码：**服务器对请求的响应状态代码。当有多个响应状态代码时，将显示最频繁的代码和返回的代码总数。如果过滤节点阻止了请求，则代码将为403或其他自定义值。

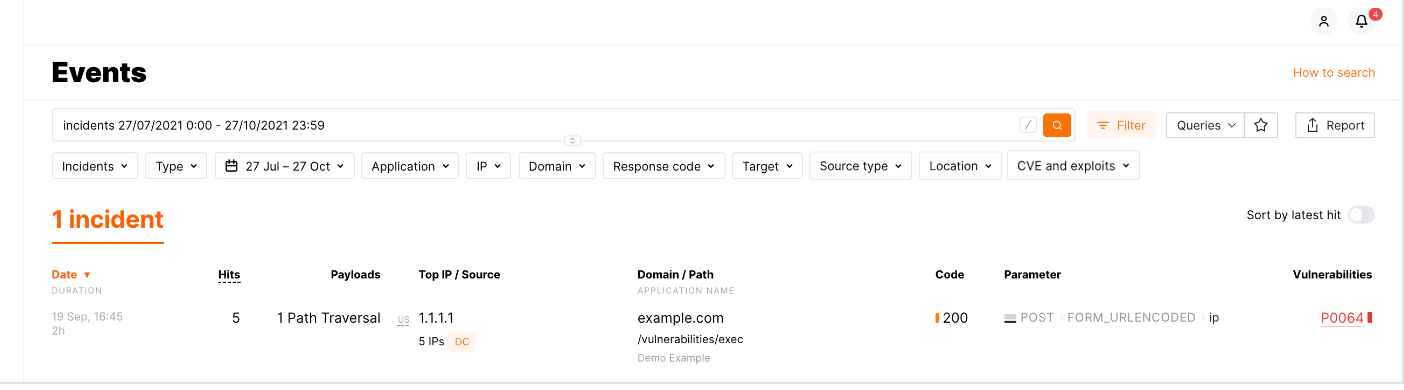
**参数：**恶意请求的参数和应用于该请求的解析器标签

**主动验证：**攻击验证状态。如果攻击被勾选为假阳性，则相应的标记将显示在此列（FP）中，并且不会再次验证攻击。要通过假阳性操作查找攻击，请使用下面的搜索过滤器:



要按上次请求的时间对攻击进行排序，可以使用“按最新命中排序”开关。

1. **事件**

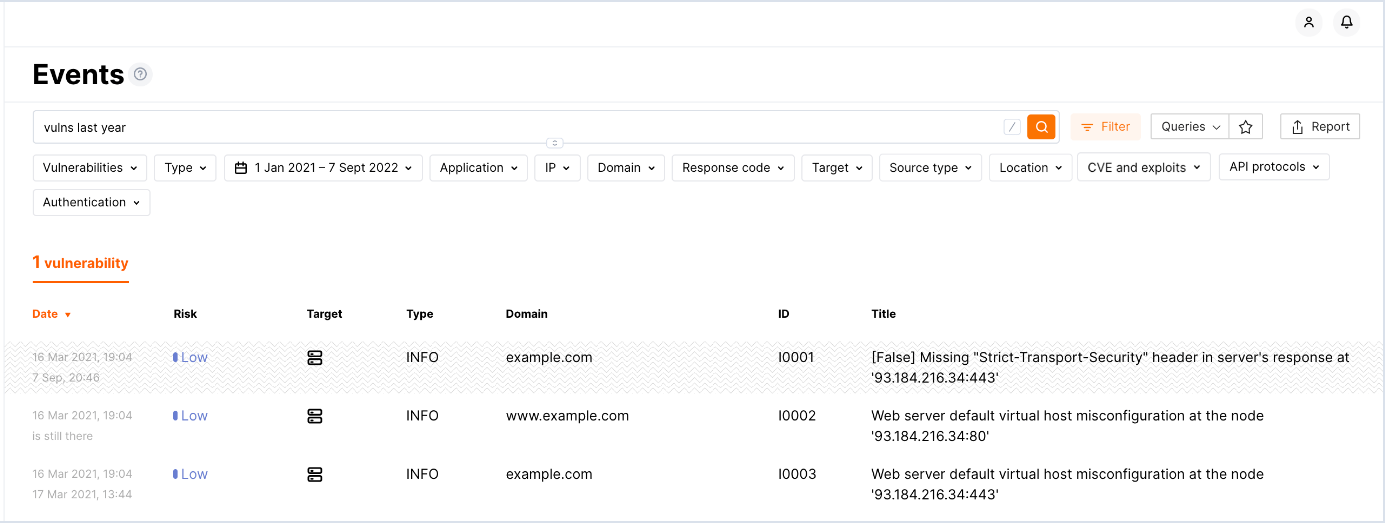


事件与攻击具有相同的参数，除了一列：漏洞列取代了攻击的验证列。“漏洞”列显示相应事件利用的漏洞。

单击该漏洞将显示其详细描述以及如何修复该漏洞的说明。

要按上次请求的时间对事件进行排序，可以使用“按最新命中排序”开关。

1. **漏洞**



日期：漏洞发现的日期和时间。

风险：脆弱性的危险程度。

目标：在漏洞利用的情况下成为受害者的一方（客户端、服务器）。

类型：利用漏洞的攻击类型。

域：发现漏洞的域。

ID：API安全系统中漏洞的唯一标识符。

标题：漏洞的标题。

1. **当前正在发生的事件**

您可以实时查看事件。如果您的公司资源正在接收恶意请求，控制台中将显示以下数据：

-过去5分钟内发生的事件数，将显示在“事件”部分名称旁边和部分内部。

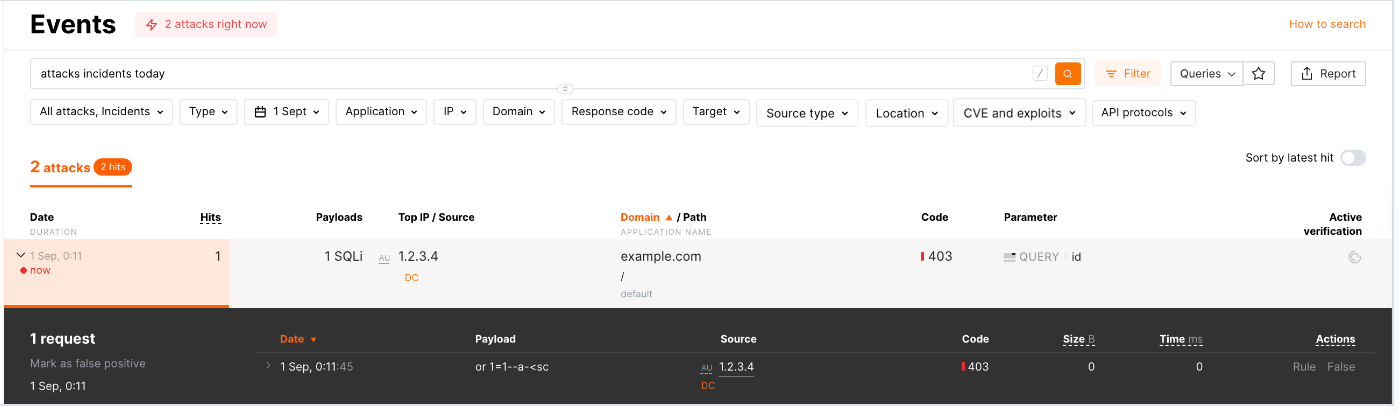
-特殊标签，显示在攻击或事件表中的事件日期下。

您也可以在搜索字段中添加now关键字，以仅显示当前发生的事件：

-立即攻击以显示当前发生的攻击。

-事件立即显示当前正在发生的事件。

-立即攻击事件以显示当前发生的攻击和事件。



1. **获取攻击、事件和漏洞的API调用**

要获取攻击、事件和漏洞详细信息，除了使用Wallarm控制台UI外，还可以直接调用WallarmAPI。下面是相应API调用的一些示例。

获取过去24小时内检测到的前50次攻击

在过去24小时内确认前50起事件

在过去24小时内获得状态为“活动”的前50个漏洞

# **漏洞**

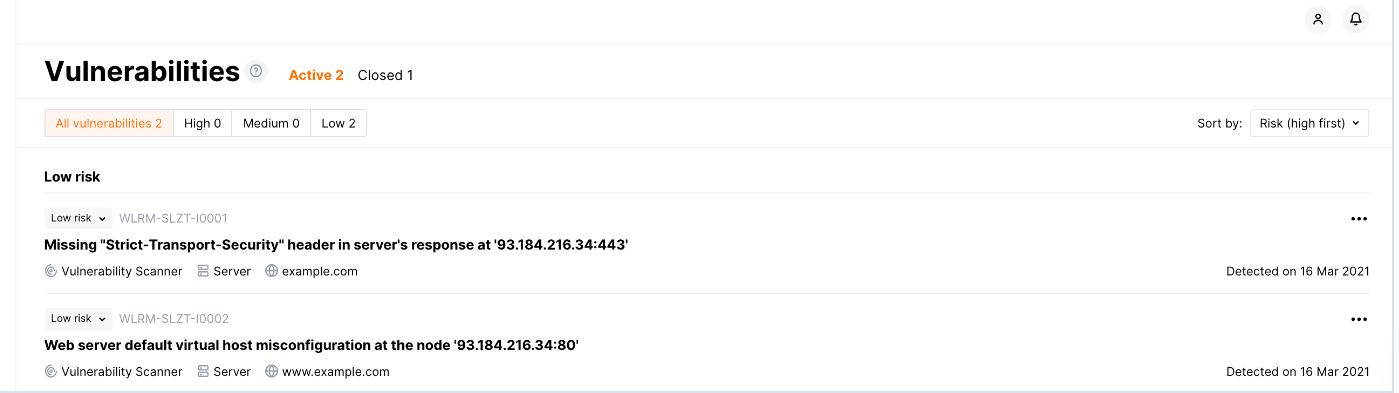
**检测漏洞**

在控制台的“漏洞”部分，您可以检查应用程序中平台检测到的漏洞。

默认情况下，所有漏洞都按风险级别进行分组。组内的列表按漏洞发现日期排序。

平台存储所有发现的漏洞的历史记录，并定期对其进行检查，包括打开的和关闭的漏洞。如果检查后打开了已关闭的漏洞，您将收到相应的通知。

单击漏洞将显示其更改日志。



**按风险或日期对漏洞进行排序**

您可以根据以下标准对漏洞进行排序：

风险：高优先级、低优先级

日期：从最新、从最早

您可以按以下按钮之一，按风险级别筛选漏洞：

-全部-显示所有风险级别组的漏洞

-高风险-显示高风险漏洞

-中等风险-显示中等风险漏洞

-低风险-显示低风险漏洞

**筛选活动和已关闭漏洞**

单击“活动”查看活动漏洞。

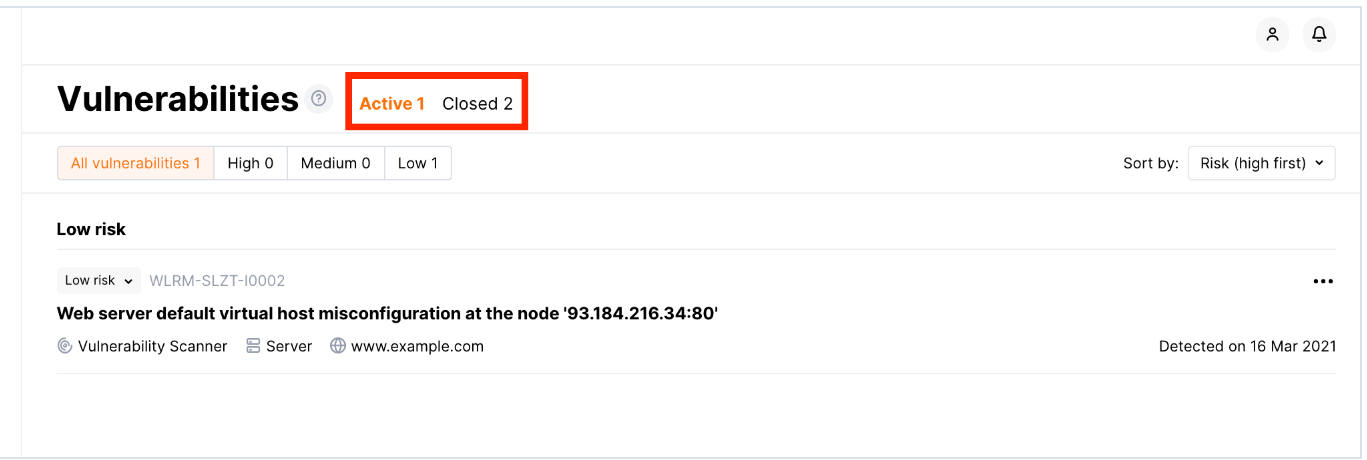
单击关闭以查看已关闭的漏洞。

您可以通过单击以下选择器来筛选已关闭的漏洞：

-all：已关闭和错误漏洞列表。

-fixed：该列表仅修复了漏洞。

-false：仅列出错误漏洞。



# **API发现**

本节介绍如何使用API发现模块构建的API结构。

构建的API结构在API发现部分中介绍。该部分仅适用于以下角色的用户：

-管理员和分析员可以查看和管理API发现模块发现的数据。

-具有多租户功能的帐户中的全局管理员和全局分析师具有相同的权限。

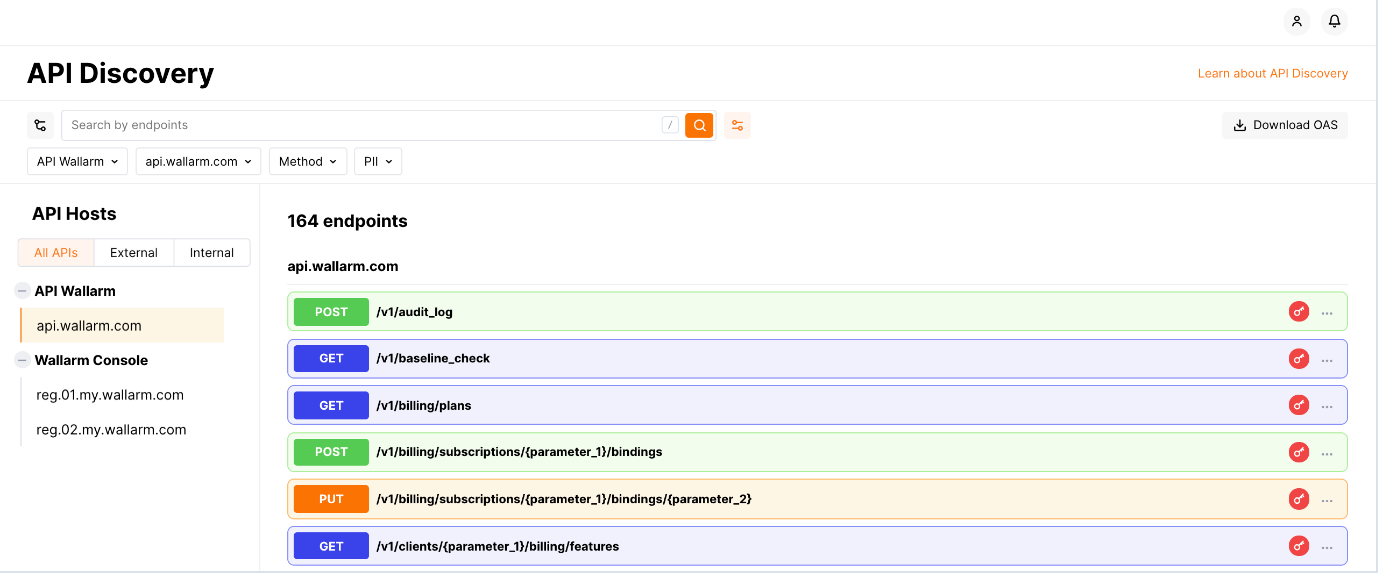
-API开发人员可以查看和下载API发现模块发现的数据。该角色允许区分任务仅需要使用平台获取公司API实际数据的用户。这些用户无权访问除API发现和设置之外的任何控制台部分→ 配置

为了向用户提供熟悉的API表示格式，平台在类似Swagger的界面中提供了已发现的API列表及其详细信息。

API结构包括以下元素：

-发现API主机的客户应用程序。

-发现按API主机分组的终结点。对于每个端点，将显示HTTP方法。



# **使用搜索和筛选器**

平台提供了搜索检测到的攻击、事件和漏洞的便捷方法。在Wallarm控制台的事件部分，有以下搜索方法可用：

-筛选以选择筛选条件

-用于输入具有类似于人类语言的属性和修饰符的搜索查询的搜索字段

过滤器中设置的值在搜索字段中自动复制，反之亦然。

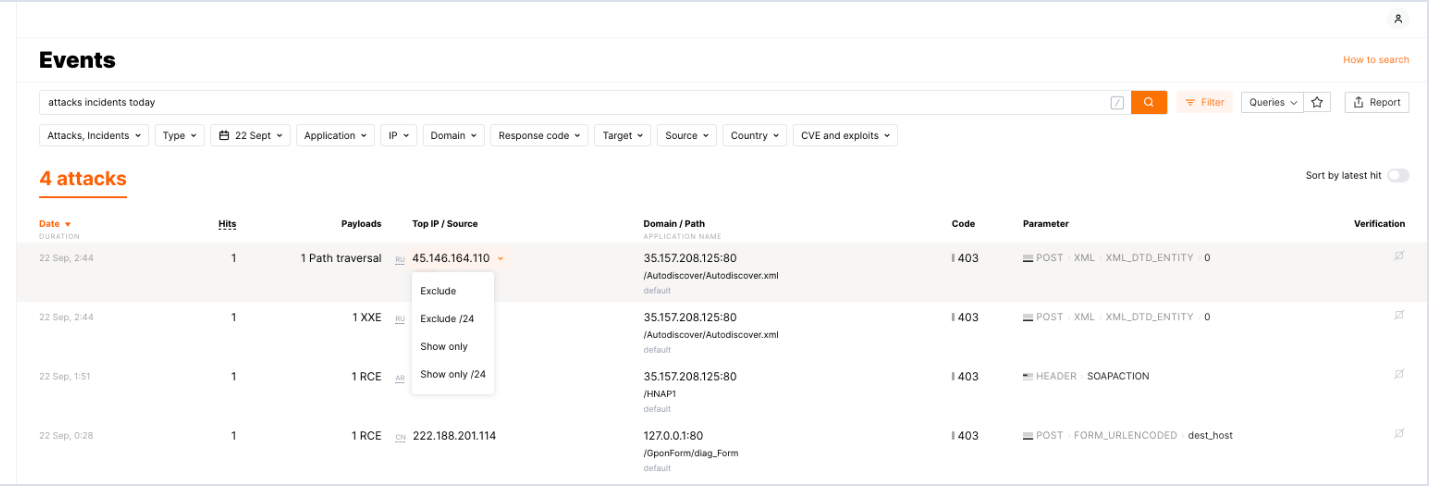
单击“保存查询”可以保存任何搜索查询或过滤器组合。

**过滤器**

API安全平台控制台中以多种形式显示了可用的过滤器：

-使用“过滤器”按钮展开和折叠的“过滤器”面板

-用于排除或仅显示具有特定参数值的事件的快速过滤器



# **扫描仪**

扫描仪执行以下任务：

-网络范围扫描

-搜索典型漏洞和安全问题

-主动威胁验证

-更新以前检测到的漏洞的状态

**网络范围扫描**

网络范围是公司连接到公共网络的公共资源（域和IP地址）。

它定义了一个要扫描典型漏洞的区域，是安全过程的基石。

随着项目的发展，范围内的资源数量稳步增加，对它们的控制不可避免地减少。

这些资源可能不仅位于公司的数据中心，还位于共享主机上-例如，您的营销人员将创建新的登录页面并开始新的营销活动。这些资源被放置在主项目的子域上，可能危及项目的安全。

黑客总是在公司范围内选择受保护程度最低的资源，并试图首先破坏这些资源。

平台集成了白帽黑客在评估公司安全性和运行渗透测试时使用的所有范围发现机制。

作用域发现不仅结束于域和IP地址映射，还发现可以从Internet访问的网络资源。为此，平台首先扫描端口，然后检测这些端口上的网络资源。

在收集和更新范围数据的连续过程中使用了各种方法：

自动模式

DNS区域传输（AXFR）

NS和MX记录接收

SPF记录数据接收

子域词典搜索

SSL证书解析

通过web界面或平台API手动输入数据。

这导致了一张公司资源的地图，其质量与白帽黑客在进行渗透测试时所做的相同。

**搜索典型漏洞和安全问题**

收集网络范围后，扫描程序会检查其中的所有IP地址和域是否存在任何典型漏洞。

**主动威胁验证**

扫描仪将自动从流量中再现每次攻击。该机制允许检测在攻击期间可能被利用的漏洞。

出于安全原因，当从请求中再现攻击时，身份验证数据（cookie、基本身份验证、viewstate）将被删除。此功能的正确操作可能需要应用程序端的额外配置。

**更新以前检测到的漏洞的状态**

扫描器定期检查漏洞的状态，并自动将其标记为已修复，或者相反，重新打开新复制的漏洞。

当前漏洞和不到一个月前修复的漏洞每天检查一次。

一个多月前修复的漏洞每周检查一次。

未检查标记为false的漏洞。

# **节点**

**赞腾节点**

赞腾控制台UI的节点部分允许您管理赞腾节点和CDN节点类型的节点。本文是关于赞腾节点的。

赞腾节点模块应部署到客户的环境中，以减轻恶意流量。赞腾节点通过减轻恶意请求并将合法请求转发到受保护的资源来充当代理。

赞腾节点UI管理选项：

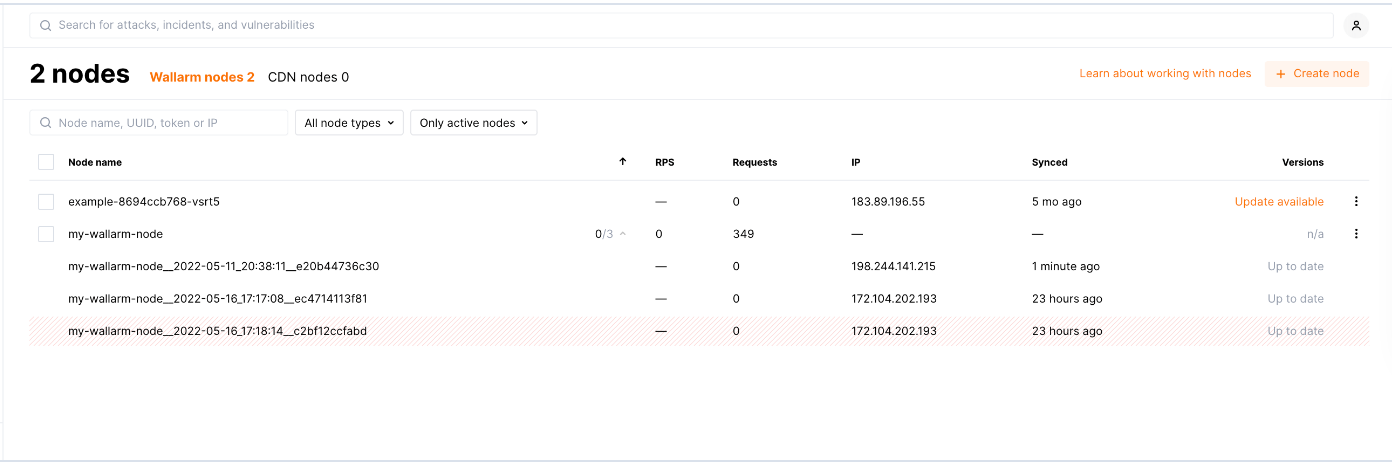
创建新节点

查看已安装节点的属性和度量

重新生成节点令牌

重命名节点

删除节点



**CDN过滤节点**

CDN节点作为受保护服务器的反向代理运行。它分析传入的流量，减轻恶意请求，并将合法请求转发到受保护的服务器。

CDN节点运营方案

至于CDN节点的其他特性：

由第三方云提供商托管，因此部署CDN节点不需要基础架构中的资源。

将请求数据上载到第三方云提供商

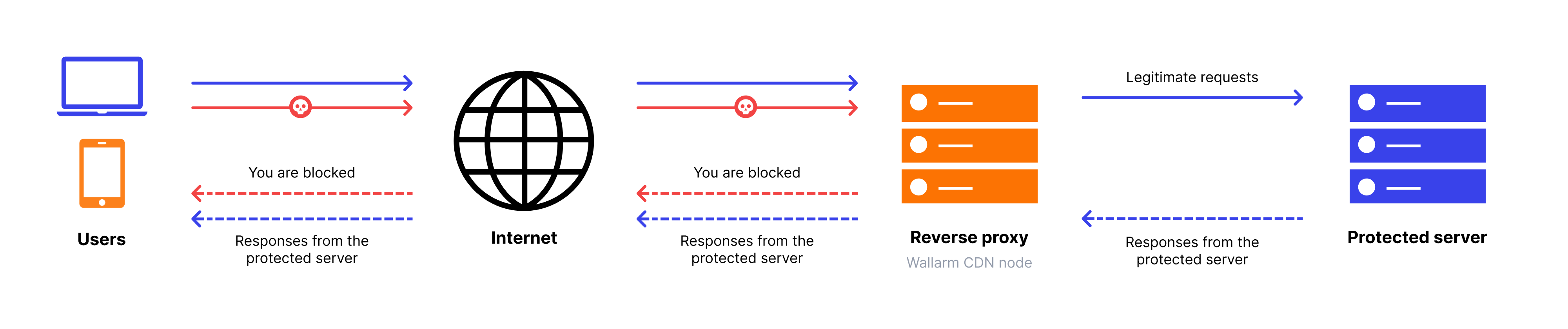
已处理请求的一些数据被上传到Lumen服务。

将一些请求数据上载到赞腾 Cloud。了解有关上传数据和剪切敏感数据的更多信息。

在安全阻止模式下运行，依靠IP灰名单内容来识别可疑流量并阻止它。

要更改模式，请使用相应的规则。

CDN节点通过赞腾控制台UI完全配置。唯一需要以另一种方式更改的设置是将赞腾CNAME记录添加到受保护资源的DNS记录中。



# **规则**

**应用程序配置文件规则**

在“规则”选项卡上，您可以查看和更改为当前应用程序配置文件启用的处理请求的规则。

应用程序配置文件是关于受保护应用程序的已知信息的集合。它用于在请求分析过程中微调系统的行为，并在后分析模块和云中对其进行进一步处理。

为了更好地理解如何应用流量处理规则，建议学习过滤器节点如何分析请求。

对规则进行更改的一个重要问题是，这些更改不会立即生效。编译规则并将其下载到过滤器节点可能需要一些时间。

# **触发器**

**使用触发器**

触发器是用于设置自定义通知和事件反应的工具。使用触发器，您可以：

通过日常工作流程中使用的工具接收重大事件警报，例如通过公司信使或事件管理系统。

阻止从中发送一定数量请求或攻击向量的IP地址。

通过发送到特定API端点的请求数量识别行为攻击。

通过将来自同一IP地址的点击分组为一次攻击来优化事件列表

您可以配置所有触发器组件：

条件：要通知的系统事件。例如：获得一定数量的攻击、拒绝列出的IP地址以及添加到帐户的新用户。

过滤器：条件详细信息。例如：攻击类型。

反应：如果满足指定条件和过滤器，应执行的操作。例如：向Slack或另一个配置为集成的系统发送通知，阻止IP地址，或将请求标记为暴力攻击。

触发器在Wallarm控制台的触发器部分中配置。该部分仅适用于具有管理员角色的用户。



# **IP列表**

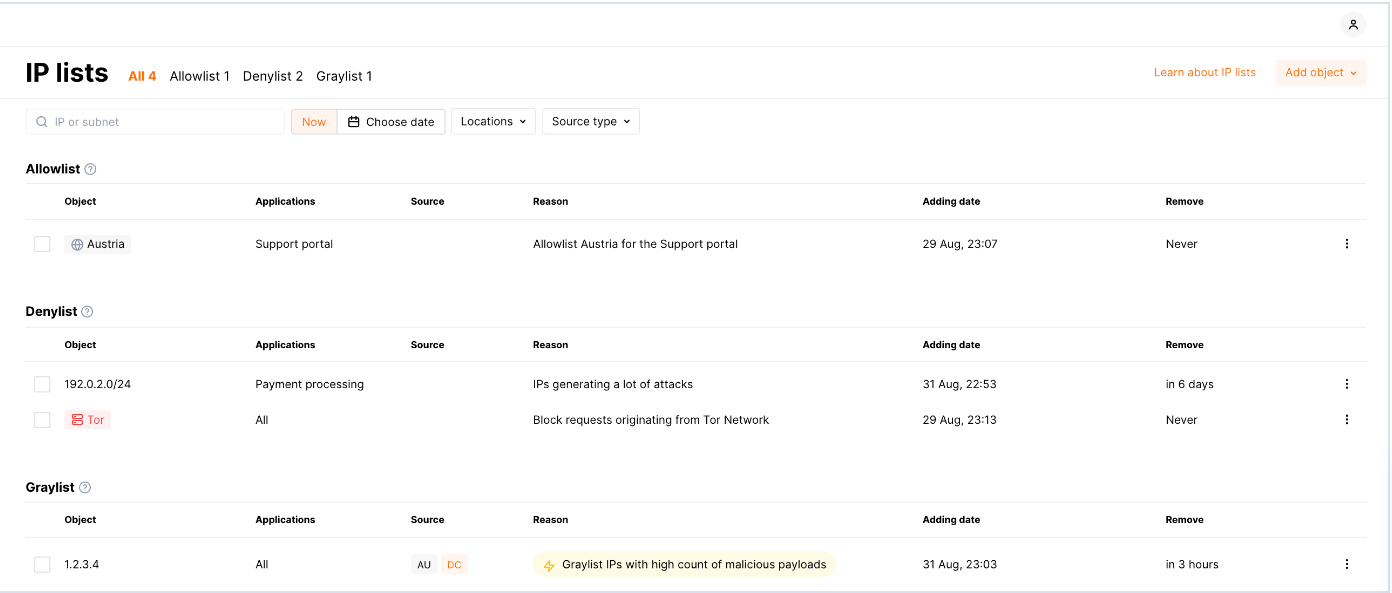
IP列表的类型和核心逻辑

在控制台的IP列表部分，您可以通过列出、拒绝列出和灰显IP地址来控制对应用程序的访问。

Allowlist是允许访问您的应用程序的受信任IP地址列表，即使来自它们的请求包含攻击迹象。

拒绝列表是不允许访问应用程序的IP地址列表。筛选节点阻止来自拒绝列表IP地址的所有请求。

Graylist是一个IP地址列表，只有当源于应用程序的请求不包含攻击信号时，才允许访问应用程序。



# **配置**

**检查您的个人资料**

要查看您的配置文件数据和设置，请转至“设置”→ “配置文件”选项卡。

在您的个人资料中，您可以检查您的帐户信息：

电子邮件

分配的角色-管理员、分析员或只读

姓名和电话

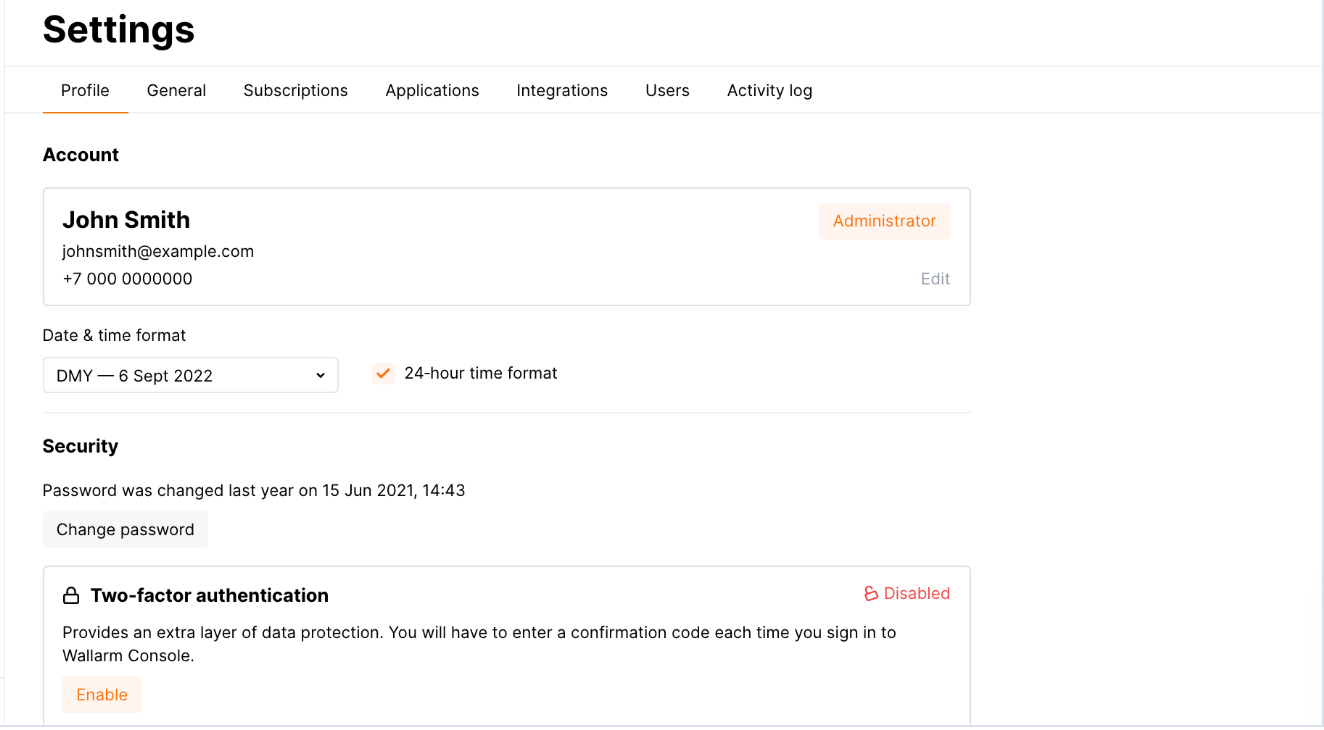
系统中使用的首选日期和时间格式

安全性：上次密码数据更改和双因素身份验证状态。如果使用SSO身份验证，某些元素可能不可用。

API凭据

登录历史记录

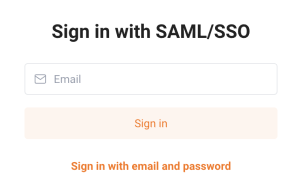
您可以单击“注销”按钮注销帐户。



# **单点登录**

**使用单点登录API安全门户**

本指南将介绍使用单点登录（SSO）技术在赞腾门户上进行用户身份验证的过程。



# **迁移和升级**

**API安全节点新增功能**

赞腾节点的新次要版本已经发布！赞腾节点4.2具有新功能，使攻击缓解更加强大和可用，包括BOLA保护和危险的JWT中和。