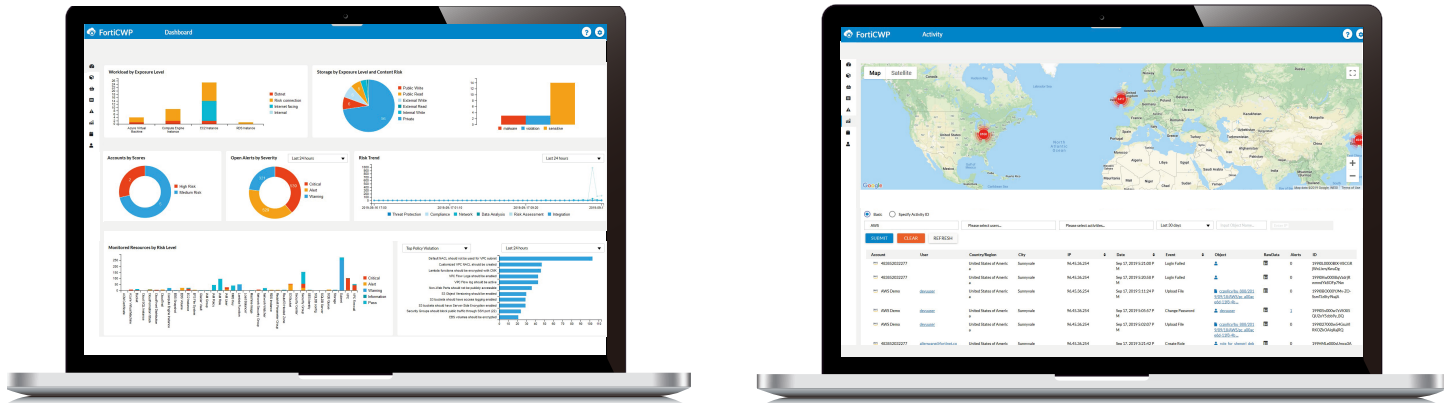


FortiCWP™

为IaaS环境提供更好的可见性与洞察



FortiCWP 是 Fortinet 提供的云原生工作负载保护服务，以 SaaS 模式进行交付。FortiCWP 通过调用 AWS, Azure, Google 等云平台提供的 API 来持续监控并追踪所有安全组件的态势，包括配置信息，用户行为 / 活动，流量 Flow log，同时也会扫描存储在云中的数据，检查其敏感性和是否包含恶意内容，并执行常规合规检查与生成报告。

 FortiCWP提供中央化Dashboard，报表和流量与实例地图来跟踪安全事件和用户行为。
此产品功能包括：

- 中央化可视化
- 按需数据扫描
- 用户洞察与策略
- 合规与DLP
- 威胁防御与响应
- 风险评估与账户评分
- 反恶意软件与高级威胁检测
- 配置评估与合规报表

通过加载预定义开箱即用的安全策略，FortiCWP能监控如下安全风险：



恶意流量



可疑用户行为



有安全隐患的配置



敏感数据泄露和恶意软件



违反合规

产品亮点

基于 API 的交互，FortiCWP 能够与市场领先的 IaaS 平台紧密集成，获取多个云的用量信息和数据存储信息。FortiCWP 让 IT 安全专家能够扫描在云资源中的配置和数据，来防范潜在威胁，错误配置和违反合规要求的操作。无论使用 IaaS 的用户在哪或使用什么设备，FortiCWP 都可以确保所有使用组织提供的 IaaS 资源的用户都是被监控并保护的。

作为 Security Fabric 的关键成员，FortiCWP 可以与其他 Fabric 成员产品进行深度整合，以为用户提供完整的云安全管理能力，并对云环境进行合规检查与生成报表。

特性

中央化可视化

FortiCWP 为用户的多云环境提供中央化视图与报表能力。FortiCWP 提供 Dashboard，日志和报表来让管理员能够以简单方便的形式快速理解当前安全状态。用户活动，云资源，数据和文件，以及策略等等都可以被集中化查看。用户活动可以在地图上或列表中展示出来。资源间的关系是通过地理化方式展示的，这样管理员可以快速理解所有被监控云账号的基础设施，进而方便理解云资源和服务之间的关系。

按需数据扫描

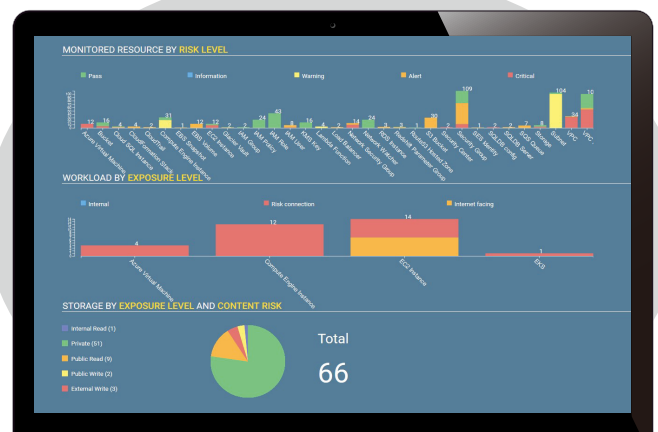
不像代理服务或硬件设备，FortiCWP 直接与云平台连接，并访问存储在组织账号中的数据和文件。一旦有新的数据上传到云平台中，FortiCWP 就会自动监测是否有违反数据泄露策略和是否包含恶意软件，来帮助用户提升数据安全水平。已经存在的数据也可以被执行扫描来确保符合企业安全规范。

用户洞察与策略

FortiCWP 提供很多工具来提升对用户行为和活动的洞察。管理员可以监控云资源使用情况，并查看用户权限，僵尸用户，以及配置评估详细信息。使用 FortiCWP 的 API，包括 FortiGate 和 FortiSIEM 在内的其他 Fortinet 产品可以访问 FortiCWP 用量统计和日志来获得更多洞察。

合规与DLP

FortiCWP 提供可以被高度定制化的数据防泄漏工具集，来防御数据泄露并生成合规报表。使用行业通用的正则表达式，FortiCWP 几乎可以被任意配置来满足数据安全检测策略，并基于 DLP 动作提供定制化的报表。



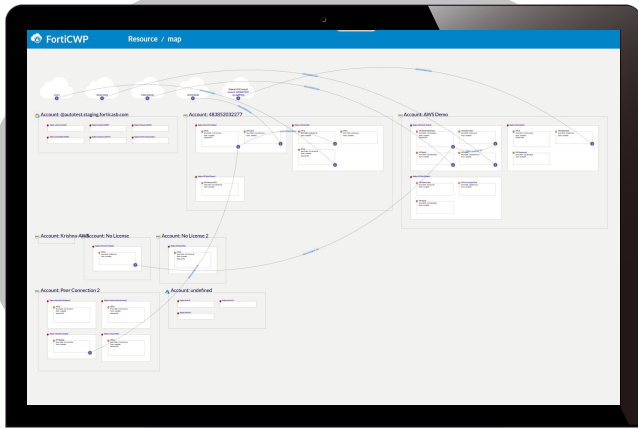
FortiCWP资源监控

对于有较高行业合规要求的企业，FortiCWP 提供开箱即用的策略来为用户提供云环境合规分析并生成合规检查报告，目前支持的合规有：PCI, HIPPA, SOX, GDPR, ISO 27001, 和 NIST。FortiCWP 提供的持续合规分析，能够快速发现违规变化，并帮助用户快速执行必须的整改动作。

威胁防御与响应

FortiCWP 使用 UEBA(用户实体行为分析)来分析可疑或不正常的用户行为，并针对恶意行为发送告警。FortiCWP 使用结合风险评估机制和高级算法的 UEBA 技术来检测用户的异常行为。

特性



FortiCWP 资源映射

风险评估与账户评分

FortiCWP 的深度风险评估和持续分析方案让安全团队能够专注在最高优先级的事件和问题，执行快速响应方案，利用自动修复功能来高效管理和解决风险。可执行的告警以及修改建议让企业能够根据事件严重程度进行不同优先级的响应。为了帮助评估风险，FortiCWP 能够针对不同账户生成相关的安全风险评分。

订购信息

Product	SKU	Description
FortiCWP Workload Guardian	FC-10-FCWPPW-315-02-DD	FortiCWP Workload Guardian - Cloud workload protection. Subscription per 20 hosts/instances for all supported public clouds
FortiCWP Storage Guardian	FC-10-FCWPS-316-02-DD	FortiCWP Cloud Storage Protection, Basic – Subscription per 1TB data
	FC-10-FCWPS-317-02-DD	FortiCWP Cloud Storage Protection, Advanced (with additional DLP scan) – Subscription per 1TB data

Note: The SKUs are newly available for purchase in 2019 Q4.

反恶意软件与高级威胁检测

FortiCWP 原生集成了获得多项殊荣的 FortiGuard 反病毒服务来扫描存储在云中的文件。与 FortiGuard 提供的沙箱技术集成，可以进一步保护 0day 威胁。这两种安全服务都被包含在了 FortiCWP 的订阅中而无需支付任何额外费用。

配置评估与合规报表

FortiCWP 能够为组织的全球 IaaS 部署执行数百个 IaaS 配置安全评估检查项，包括 AWS、Azure 和 GCP。FortiCWP 可以识别不安全的部署和云资源配置相关的风险。通过从持续评估现存云环境配置获取的信息，FortiCWP 能够生成合规报表，并展示出与合规要求的差距。FortiCWP 提供开箱即用的策略来为用户提供云环境合规分析并生成合规检查报告，目前支持的合规有：PCI, HIPPA, SOX, GDPR, ISO 27001, 和 NIST。