Acronis Detection and Response

实时防范攻击并深入了解每个网络攻击

Acronis Detection and Response 是最后一道防线，能够保护贵组织免受能绕过防恶意软件防御的威胁。该解决方案专为“零信任”方法而设计，可检测并阻止任何偏离合法操作系统行为的活动，并提供实时可见性以及自动和手动补救功能。

可防御各种威胁的安全保护	实时威胁保护	集中且详细的可见性
增加了威胁检测和响应功能，从而增强了终端安全保护。阻止能绕过防恶意软件防御机制的攻击，包括新的或未知的恶意软件和勒索软件、无文件攻击、零日攻击和高级可持续威胁 (APT)	部署能够自动阻止损害发生且经实践验证的解决方案，而不是被动地对安全漏洞做出反应。无需手动追踪威胁，也无需昂贵的基础架构或云连接	让您的安全团队可以非常细致地了解攻击的时间表和来源，策略、方法和步骤 (TTP)，以及与攻击者试图达成目的有关的信息，从而加强贵组织的安全状况

保护终端和数据免遭其他“漏网之鱼”的攻击

最大限度地降低网络风险/阻止任何威胁	确保快速响应事件	最大程度利用现有资源
• 检测并阻止能绕过防恶意软件防御机制的高级攻击 – 新的或未知的恶意软件、无文件攻击、零日攻击和 APT • 添加最后一道安全防线来加强现有的防御能力，从而阻止漏洞损害企业资产 • 采用“零信任”方法并捕获任何偏离合法操作系统行为的活动 • 适用于网络状况不佳或离线的环境	• 通过自动防御功能来缩短响应威胁所需的时间 • 让您的 SOC 团队能够详细了解每一个攻击 • 利用自动和手动补救功能 • 持续监控整个组织的终端和网络活动 • 获得由 Acronis 安全专家管理的检测和事件响应服务的访问权限，实现终极保护，让您高枕无忧	• 通过集中而详细地了解威胁并消除不必要的干扰，减少对其他资源的需求 • 与其他防恶意软件解决方案相辅相成 – 无需更换解决方案 • 对终端性能和带宽消耗的影响较小 • 优化总拥有成本 (TCO)，而无需额外的人员配备或昂贵的基础架构

受益于现代威胁防护方法

Acronis Detection and Response 为您的安全堆栈增加了入侵后威胁检测和响应功能。识别并拦截绕过了其他防御层的威胁，同时让网络安全团队能够对每个事件进行深入的取证分析。

自动的实时防护	可防御各种威胁的防护	零信任方法	避免数据泛滥	低 TCO
此解决方案一旦检测到威胁，就会立即自动对其进行拦截，不需要以人工或半人工方式进行威胁追踪和补救。	检测并阻止能绕开下一代防病毒软件（NGAV）的高级攻击，如新的或未知的恶意软件和勒索软件、无文件攻击、零日攻击和 APT。	使用“零信任”方法提高威胁检测准确率，并识别任何偏离合法操作系统行为的活动，而不必识别不断发展的攻击方法。	无需在海量数据中手动搜索并分析威胁，就可以集中而详细地了解威胁和事件，从而大大增强安全团队的能力。	凭借自动的威胁搜索功能和较低的带宽消耗量，进一步降低总拥有成本（TCO）。利用现有资源和基础架构。

经过 ICSA LABS 认证的解决方案

ICSA Labs
Advanced Threat Defense
Certified

测试时长	测试运行	恶意样本	检测率	无害应用程序	误报率
33 天	1162	441	100%	721	0.1%

灵活的部署选项

本地部署
利用现有的 IT 基础架构并在本地部署解决方案

云部署
采用软件即服务（SaaS）部署模型来降低维护成本和保养成本

了解更多信息