SONICWALL

SonicWall Capture Client

勒索软件和其他基于恶意软件的攻击的威胁日益增大，这证明不能仅根据端点合规性来衡量客户端保护解决方案。传统防病毒技术采用的是受到长期诟病的基于签名的方法，这种方法已经无法跟上新出现的恶意软件和隐蔽技术的步伐。此外，随着远程办公、移动办公和 BYOD（自带设备）的涌现，迫切需要随时随地为端点提供一致的保护。

SonicWall Capture Client 是一个具有多种保护功能的统一端点产品。借助由 SentinelOne 提供技术支持的下一代恶意软件防护引擎，Capture Client 应用了先进的威胁防护技术，如机器学习、网络沙箱集成和系统回滚。通过安装和管理可信 TLS 证书，Capture Client 还可以利用 SonicWall 防火墙上对加密 TLS 流量的深度检测 (DPI-SSL)。

Capture Client 与 SonicWall Global VPN Client 共存，因此所有产品的策略都可以通过单个云端管理控制台进行管理。Capture Client 可以通过 Microsoft Active Directory 组策略或任何其他第三方软件部署技术轻松添加到所部署的任何客户端；也可以通过提供定制 URL 来添加到所部署的任何客户端，其中客户端可以静默地下载并自行安装，无需任何额外的干预。此外，与 SonicWall 防火墙集成时，Capture Client 可通过可选的强制执行功能在未受保护的客户端上提供零接触部署体验。

功能与好处

持续的端点行为监控有助于获得文件活动、应用程序和进程活动以及网络活动的完整概况。这可以防范基于文件和无文件的恶意软件，并提供全方位的攻击视图，其中带有与调查相关的可操作情报。

多层启发式保护技术包括云情报、高级静态分析和动态行为保护。这些技术有助于防范和清除已知和未知的恶意软件。

无需定期扫描或定期更新，可随时提供最高级别的保护，而不会影响用户的工作效率。Capture Client 在安装时执行全面扫描，之后持续监控可疑活动。

Capture 高级威胁防护 (ATP) 集成通过端点无法执行的代码操作，自动上传可疑文件进行高级沙箱分析。在更多威胁执行之前阻止它们，例如内置时间延迟的恶意软件。管理员也可以参考 Capture ATP 的文件裁决数据库，而无需将文件上传到云中进行分析。

独特的回滚功能还支持相关策略，这些策略不仅可以完全消除威胁，而且还可以将目标客户端恢复到恶意软件活动启动前的状态。这样，在 Windows 遭遇勒索软件和类似攻击的情况下就无需手动恢复。

应用程序漏洞情报使管理员能够在每个受保护的端点上对每个应用程序以及与之相关的任何风险进行编目。风险基于是否存在任何有通用漏洞披露 (CVE) 详细信息的已知漏洞，以及为该版本报告的严重性等级，从而为管理员提供可操作的情报以优先安排修补和减小端点的攻击面。

与 SonicWall 第 6 代及以上防火墙的可选集成可提供零接触部署和增强的端点合规性。另外，通过向每个端点部署可信证书，该集成还支持执行针对加密流量的深度包检测 (DPI-SSL)。

内容过滤允许组织阻止恶意网站 IP 地址和域，并通过限制带宽或限制访问不良或低效网络内容来提高用户工作效率。

好处

- 独立云端管理
- 与 SonicWall 防火墙协同
- 安全策略执行
- DPI-SSL 证书管理
- 持续行为监控
- 通过机器学习实现高度准确的判断
- 多层启发式技术
- 应用程序漏洞情报
- 独特的回滚功能
- 轻松加入白/黑名单
- 用于自动分析恶意软件的 Capture 高级威胁防护 (ATP) 云沙箱
- 免上传的威胁情报共享，以便手动检查文件
- 内容过滤
- 设备控制

设备控制允许组织通过细粒度的白名单策略来阻止可能受感染的设备连接到端点。

集中的管理和客户端保护报告 SonicWall 云端管理控制台作为单一管理平台工作以管理所有客户端策略，包括下一代恶意软件防护、DPI-SSL 证书管理和内容过滤。

该管理控制台是一个免费提供的多租户云端平台。它提供客户端保护报告和策略管理，支持细粒度访问控制策略，包括基于 Microsoft Active Directory 属性分配策略的能力。这使托管服务提供商 (MSP) 能够管理和报告多个客户的客户端。同时，其中每个客户只能管理和报告自己的客户端。

该管理控制台还充当一个调查平台，可以帮助确定所检测到的恶意软件威胁的根源，并提供有关如何防止此类威胁再次发生的可操作情报。例如，管理员可以轻松查看哪些应用程序在客户端上运行。这反过来又可以帮助确定可能在运行易受攻击或未经授权的软件的机器。

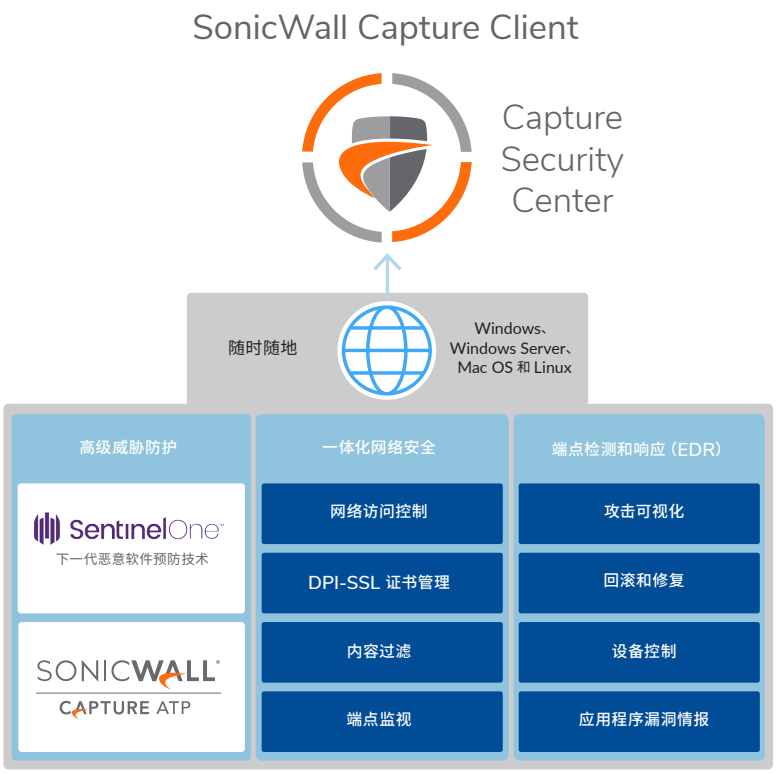
产品版本和平台支持

SonicWall Capture Client 具有两种产品版本：

SonicWall Capture Client Basic 提供所有 SonicWall 下一代恶意软件防护和修复功能，以及 DPI-SSL 支持功能。

SonicWall Capture Client Advanced 提供上面针对 Basic 版本列出的所有功能，另外还有高级回滚功能、Capture ATP 集成、攻击可视化、应用程序漏洞情报和内容过滤。

两个版本均可用于 Windows 7 及更高版本以及 Mac OSX。



功能特性比较		
功能特性	Basic	Advanced
云管理、报告和分析 (CSC)	✓	✓
一体化网络安全		
端点监视	✓	✓
DPI-SSL 证书部署	✓	✓
内容过滤	–	✓
高级威胁防护		
下一代反恶意软件	✓	✓
Capture 高级威胁防护 (ATP) 沙箱	–	✓
端点检测和响应		
攻击可视化	–	✓
回滚和修复	–	✓
设备控制	–	✓
应用程序漏洞和情报	–	✓

系统要求
操作系统
Windows7 及更高版本
Windows Server 2008 R2 及更高版本
Mac OS/OSX 10.10 及更高版本
硬件
1 GHz 双核 CPU 或更高
1 GB RAM 或更高 (如果操作系统需要) (推荐 2 GB)
2 GB 可用磁盘空间

CAPTURE CLIENT SKU		
产品	有效期	SKU
ADVANCED		
SONICWALL CAPTURE CLIENT ADVANCED，5-24 个端点，含全天候支持	3 年	02-SSC-1518
SONICWALL CAPTURE CLIENT ADVANCED，5-24 个端点，含全天候支持	1 年	02-SSC-1519
SONICWALL CAPTURE CLIENT ADVANCED，25-49 个端点，含全天候支持	3 年	02-SSC-1520
SONICWALL CAPTURE CLIENT ADVANCED，25-49 个端点，含全天候支持	1 年	02-SSC-1521
SONICWALL CAPTURE CLIENT ADVANCED，50-99 个端点，含全天候支持	3 年	02-SSC-1522
SONICWALL CAPTURE CLIENT ADVANCED，50-99 个端点，含全天候支持	1 年	02-SSC-1523
SONICWALL CAPTURE CLIENT ADVANCED，100-249 个端点，含全天候支持	3 年	02-SSC-1524
SONICWALL CAPTURE CLIENT ADVANCED，100-249 个端点，含全天候支持	1 年	02-SSC-1525
SONICWALL CAPTURE CLIENT ADVANCED，250-499 个端点，含全天候支持	3 年	02-SSC-1454
SONICWALL CAPTURE CLIENT ADVANCED，250-499 个端点，含全天候支持	1 年	02-SSC-1455
SONICWALL CAPTURE CLIENT ADVANCED，500-999 个端点，含全天候支持	3 年	02-SSC-1456
SONICWALL CAPTURE CLIENT ADVANCED，500-999 个端点，含全天候支持	1 年	02-SSC-1457
SONICWALL CAPTURE CLIENT ADVANCED，1,000-4,999 个端点，含全天候支持	3 年	02-SSC-1458
SONICWALL CAPTURE CLIENT ADVANCED，1,000-4,999 个端点，含全天候支持	1 年	02-SSC-1459
SONICWALL CAPTURE CLIENT ADVANCED，5,000-9,999 个端点，含全天候支持	3 年	02-SSC-1460
SONICWALL CAPTURE CLIENT ADVANCED，5,000-9,999 个端点，含全天候支持	1 年	02-SSC-1461
SONICWALL CAPTURE CLIENT ADVANCED，10,000 个端点以上，含全天候支持	3 年	02-SSC-1462
SONICWALL CAPTURE CLIENT ADVANCED，10,000 个端点以上，含全天候支持	1 年	02-SSC-1463
BASIC		
SONICWALL CAPTURE CLIENT BASIC，5-24 个端点，含全天候支持	3 年	02-SSC-1510
SONICWALL CAPTURE CLIENT BASIC，5-24 个端点，含全天候支持	1 年	02-SSC-1511
SONICWALL CAPTURE CLIENT BASIC，25-49 个端点，含全天候支持	3 年	02-SSC-1512
SONICWALL CAPTURE CLIENT BASIC，25-49 个端点，含全天候支持	1 年	02-SSC-1513
SONICWALL CAPTURE CLIENT BASIC，50-99 个端点，含全天候支持	3 年	02-SSC-1514
SONICWALL CAPTURE CLIENT BASIC，50-99 个端点，含全天候支持	1 年	02-SSC-1515
SONICWALL CAPTURE CLIENT BASIC，100-249 个端点，含全天候支持	3 年	02-SSC-1516
SONICWALL CAPTURE CLIENT BASIC，100-249 个端点，含全天候支持	1 年	02-SSC-1517
SONICWALL CAPTURE CLIENT BASIC，250-499 个端点，含全天候支持	3 年	02-SSC-1444
SONICWALL CAPTURE CLIENT BASIC，250-499 个端点，含全天候支持	1 年	02-SSC-1445
SONICWALL CAPTURE CLIENT BASIC，500-999 个端点，含全天候支持	3 年	02-SSC-1446
SONICWALL CAPTURE CLIENT BASIC，500-999 个端点，含全天候支持	1 年	02-SSC-1447
SONICWALL CAPTURE CLIENT BASIC，1,000-4,999 个端点，含全天候支持	3 年	02-SSC-1448
SONICWALL CAPTURE CLIENT BASIC，1,000-4,999 个端点，含全天候支持	1 年	02-SSC-1449
SONICWALL CAPTURE CLIENT BASIC，5,000-9,999 个端点，含全天候支持	3 年	02-SSC-1450
SONICWALL CAPTURE CLIENT BASIC，5,000-9,999 个端点，含全天候支持	1 年	02-SSC-1451
SONICWALL CAPTURE CLIENT BASIC，10,000 个端点以上，含全天候支持	3 年	02-SSC-1452
SONICWALL CAPTURE CLIENT BASIC，10,000 个端点以上，含全天候支持	1 年	02-SSC-1453

关于 SonicWall

SonicWall 为超分布式时代和每个人都远程办公、每个人都移动办公、每个人都不太安全的工作现实提供了 Boundless Cybersecurity。通过了解未知、提供实时可见性并实现经济学突破，SonicWall 为世界各地的大型企业、政府和中小企业弥补了网络安全业务缺口。有关详情，请访问 www.sonicwall.com。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
有关详情，请访问我们的网站。
www.sonicwall.com

Datasheet-CaptureClient-US-VG-2139