WEBROOT
Smarter Cybersecurity™

BATTLE CARD

## WEBROOT SecureAnywhere® Business Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection is a proven, next-generation endpoint security solution for preventing malware infection. Its cloud-driven collective intelligence is powered by the Webroot® Threat Intelligence Platform. It is designed to be highly effective at countering and preventing infections from both known and zero-hour malware. Webroot SecureAnywhere Business Endpoint Protection replaces outdated, reactive endpoint protection that needs constant updating and hogs system resources with – a predictive solution that stops malware, doesn't slows users down, and reduces operational overheads. It provides a Smarter Cybersecurity™ solution for endpoints.

## CYLANCE

Cylance was founded by ex-McAfee Global CTO Stuart McClure and ex-McAfee Chief Scientist Ryan Permeh. Its flagship product, CylancePROTECT, is a next-gen antivirus built on AI and machine learning, with improved prevention capabilities compared to conventional antivirus. Cylance offers antivirus, pen testing, security & compromise assessments, advanced threat protection, and emergency incident response. They are a small but strong competitors.

| | |
|---|---|
| **Established** | 2012 |
| **Headquarters** | Irvine, CA, USA |
| **Revenue** | Funding $35M Blackstone, Khosla, Fairhaven. B round $30M |
| **Company Status** | Private |
| **No. of Employees** | 50-200 |
| **No. of Endpoint Customers** | Unknown |

| Deployment | Webroot | Cylance |
|---|---|---|
| **Agent Deployment Size** | <1MB | 55 MB |
| **Full Installation Time** | 5 seconds | Unknown |
| **Full Installation Size** | 2 MB | Unknown |
| **Memory Used During Initial Scan** | 13 MB | Unknown |
| **Scheduled Scan Time** | 91 seconds | Not a Cylance function |
| **Memory Usage – Idle** | 5.5 MB | Service 109MB + 45MB GUI |
| **File Write, Open, Close** | 19.2 seconds | Not a Cylance function |

| Positioning Webroot SecureAnywhere® Business Endpoint Protection | |
|---|---|
| **Key Differentiators** | **Supporting Messages** |
| **Smallest Endpoint Security Client** | Full installation software package is less than 1 MB in size. |
| | Lowest scanning RAM usage of any endpoint solution. |
| | Ultra-fast scan times, typically < 2 minutes. Doesn't slow user endpoints down or impede user productivity. |
| **Easy to Deploy, Configure and Use** | Very fast and easy to deploy, typically ~2-3 minutes, including initial scan. Deployment Tool, MSI, Group Policy options. |
| | No-conflict agent, compatible with existing antivirus software, no need to uninstall old software to trial or install Endpoint Protection. |
| | Easy-to-use cloud management console, no hardware/software required. |
| | Auto-updating software generates minimal network traffic – typically <250KB per day, per endpoint. |
| **Powerful Threat Protection and Remediation** | Proven next generation using cloud-based machine learning, file pattern, and predictive behavior recognition technology combined with collective threat intelligence to predict, detect, and prevent malware. |
| | White and black listing plus undertermined/unknown containment for high efficacy, zero false positives. |
| | Multi-vector malware prevention includes web browser, user behavior, identity and privacy, and real-time anti-phising protection. |
| | Unique dwell-time alerting and reporting giving full visibility of endpoint infection type and time to detection/remediation. |

| De-Positioning Cylance Endpoint Security | |
|---|---|
| **Cylance Position** | **Supporting Messages** |
| **Strengths** | Looks at applications that execute and hooks "CreateProcess" and "LoadImage" function calls to evaluate the application. |
| | Like Webroot, requires no updates, which reduces operational costs. |
| | Offline protection like Webroot but also has App/Whitelisting version for tying down non-dynamic systems like POS. |
| | Forensics give pre-execution and detonation intelligence. Useful to security experts. |

## De-Positioning Cylance (continued)

| Cylance Position | Supporting Messages |
|---|---|
| Vulnerabilities | No automatic remediation, so malware that successfully circumvents Cylance will mean the endpoint needs reimaging. |
| | Approach has high potential for false positives without extensive white listing. Recent tests show 4x industry average FPs.[1] |
| | Few endpoint management controls (no Agent Commands or Overrides). Not as intuitive, automated or informative as Webroot GSM Console. |
| | Completely lacking in multi-vector threat defenses, no outbound firewall, web browser, web reputation, or phishing defenses. |
| Sales Tactics | Webroot minimally impacts system performance at idle or during scans. Detects most malware in milliseconds and detection accuracy means zero false positives. |
| | More comprehensive and accurate malware protection with application white and black listing, plus our Web, Identity, Behavior, Self-protection and System Shields. |
| | Webroot offers individual and collective protection for all endpoints and doesn't require daily definition updates: auto-updating agent. |
| | When Cylance does not detect a malicious application, they are slow to update their detection model. They offer no real-time dynamic. They either trigger or fail. |
| | Unlimited trial: Offer instant free 30-day trial to run alongside existing antivirus so our capabilities and more advanced management shine through. |

| Features | Webroot | Cylance | Notes – How to Win |
|---|---|---|---|
| **Deployment & Installation** | | | |
| Fast installation | Yes | Yes | CP – Agent is small so expect install is quick, including initial scan |
| Fast scheduled scanning | Yes | No | CP – Does not offer scheduled scanning, as not a traditional antivirus |
| No-conflict compatibility with all software | Yes | No | CP – Likely requires other endpoint security to be removed |
| Minimal system resource usage - Memory, CPU & Disk | Yes | Partly | CP – Quite resource hungry at idle |
| Support for Mac, PC, Server, VMware & Citrix | Yes | No | CP – No Mac OS and no VM capability or mobile for Android and iOS |
| **Threat Detection and Remediation** | | | |
| Global security & threat intelligence network | Yes | No | CP – Does not have an equivalent of BrightCloud Threat Intelligence |
| Advanced zero-day/unknown malware detection | Yes | Yes | CP – Uses machine learning model to detect, versus Webroot that uses a combination of methods, including machine learning |
| Protection against viruses, Trojans, worms, spyware & rootkits | Yes | Yes | CP – Uses predictive matching like Webroot |
| Advanced file pattern & behavior recognition technology | Yes | Yes | CP – Advanced mathematics, machine learning/neural networking to identify APTs, unknowns in real time |
| Adjustable heuristics for Age, Popularity, Uniqueness | Yes | No | CP – No adjustable heuristics |
| Intelligent cloud-based outbound firewall | Yes | No | CP – No outbound firewall control, no visibility of packets leaving endpoint, no ability to block |
| Comprehensive range of System Protection shields | Yes | No | CP – No shields to protect browsers or online identity and privacy, very narrow protection |
| Automatic journaling of unknown processes | Yes | Partly | CP – No journaling, but gives some forensics information |
| Automatic malware remediation & removal | Yes | No | CP – No rollback remediation, so infected endpoints need reimaging |
| Comprehensive application override controls | Yes | No | CP – Does not offer this level of agent/management integration |
| Dwell Time | Yes | No | CP – Does not measure or report Dwell Time |
| **Web Browser Security** | | | |
| Browser vulnerability protection | Yes | No | CP – Offers no browser protection |
| Identity Shield, sensitive data safe-mode | Yes | No | CP – No Identity Protection or ability to limit unknown browser malware |
| Real-Time Anti-Phishing protection | Yes | No | CP – No real-time anti-phishing, no blocking of phishing sites |
| Secure Web Gateway service option | Yes | No | CP – Endpoint-only focus |
| **Management and Reporting** | | | |
| Cloud-based management console | Yes | Yes | CP – Cloud-based but basic, no flexibility of Standard/GSM consoles |
| Advanced management reporting & analytics | Yes | No | CP – Analytics available in separate module, reporting very basic |
| Zero client/agent definition file updates | Yes | Yes | CP – No updates, relies on math approach |
| Device policies for Network, Disk, USB, CD/DVD Usage | Yes | No | CP – No device policies for on or offline |
| System Cleaner & System Analyzer performance tools | Yes | No | CP – No Analyzer or Cleaner functionality |
| System viewer, control and file submission tools | Yes | No | CP – Not exactly, but gives detonation details for forensic use |

## Key Findings

- AV-Test.org tested (December) Cylance and prevention performance wasn't great. Many FP's too.
- Very limited antimalware solution with poor multi-layered security protection compared to Webroot.
- Poor management console and little functionality e.g. no System Optimizer.
- No access to real-time contextual threat intelligence, as Webroot provides.
- Cylance is startup and augmentation solution, Webroot is a proven replacement solution.
- Cylance only has limited threat intelligence on application files, not Webroot's contextual awareness of files plus links to URL, IP, Mobile app, or Web reputation intelligence.

## Notes and Comments

- No Agent Commands.
- Far fewer remote endpoint management capabilities or instant application override controls.
- No System Analyzer, System Cleaner, or Identity/Privacy Shield and protected applications.
- No integrated proactive support, and support is web-based.
- No automatic roll-back remediation. No real-time anti-phishing defenses.
- No support for Virtual environments or Citrix servers.

[1] Source of high FPs: https://www.av-test.org/en/antivirus/business-windows-client/windows-10/december-2015/cylance-protect-1.2-154676/



* PassMark Software, "Webroot SecureAnywhere® Business Endpoint Protection vs. Seven Competitors", (August 2015)