**Carbon Black**

This cybersecurity company offers a next-generation antivirus (also known us VMware Carbon Black Cloud Endpoint Standard) for endpoint systems to enhance security on those systems and get better protection and visibility. It is a software as a service (SaaS) solution that provides next-generation anti-virus (NGAV), endpoint detection and response (EDR), advanced threat hunting, and vulnerability management within a single console using a single sensor. The next-generation antivirus replaces traditional antivirus solutions due to its design for advanced malware protection to stop known and unknown attacks. Some of its capabilities include:

* Comprehensive prevention to halt ransomware, malware, file-less, and other attacks.
* A unique feature approach to detect and block malicious activity, taking a completely system-centric view of endpoint security rather than merely focusing on point-in-time malware threats.
* Reduced mean time to detect and respond to every threat by alerting security personnel for an immediate response within the console, thereby quickly isolating the threat.
* A lightweight and easy feature to consolidate one’s security stack and return critical CPU cycle on endpoints within a single cloud-native console and agent.

**COST:** Based on the endpoint package chosen and provided on a tiered yearly subscription model pricing model starting with $30 per endpoint per year subscription.

|  |  |
| --- | --- |
| **PROS** | **CONS** |
| Easy installation on endpoints through a single lightweight agent.  Visual display for stages of an attack and automatic scoring of security alerts. | This solution is primarily designed for cloud services only. Hence, to protect on-premise endpoints that require specialized protection due to their unique purpose or build as well, one must get another type of Carbon Black’s solution such as VMware Carbon Black EDR or VMware Carbon Black App Control depending on what they want to protect. |
| Supports the prevention, detection, proactive hunting, and remediation of active threats.  Offline prevention against signatures and behaviors used by attackers. | The equivalent on-premise malware protection, VMware Carbon Black App Control, includes additional features that VMware Carbon Black Cloud doesn’t provide, such as built-in file-integrity monitoring, device control, and memory protection to block unauthorized change. |

**FireEye**

As a leading cybersecurity company, FireEye offers innovative security technologies to protect against threats. One of these is the FireEye Network Security solution, which is designed to provide adequate protection against cyber breaches for midsize to large organizations. To accomplish this goal, it accurately detects and immediately stops advanced, targeted, and other evasive attacks hiding in Internet traffic. The solution is also composed of multiple engines and analysis techniques that provide advanced malware protection. Some of the capabilities of FireEye Network Security include:

* Integrated, distributed, physical, virtual, on-premise, and cloud deployment options.
* Multi-vector correlation with Email and Content Security.
* Consistent level of protection for multi-OS environments and all Internet access points.
* Extensible, modular security architecture and scalability to thousands of sites.
* Real-time protection against evasive attacks, zero-day, endpoint containment, and incident response.

**COST:** Depends on the type of bundle security chosen and the size of the organization. Typically costs $1,903,200/year in operational expenditure to process all alerts.

|  |  |
| --- | --- |
| **PROS** | **CONS** |
| Validated and prioritized alerts with a low rate of false positives. | Relies on conventional signature-matching methods to identify and prioritize threats. It doesn’t consider behavioral analysis. |
| An estimated 152% ROI savings over three years and payback on the initial investment in 9.7 months. | The cost to maintain the security solution might be too high for small organizations, especially if they have a limited number of assets to protect instead of the full extent that it can support. |
| Comprehensive attack surface Coverage of multiple environments. | The security solution only supports macOS x, Windows, and Linux (CentOS). |

**Cylance**

This software firm develops antivirus software and other kinds of security solutions that proactively prevent, rather than reactively detect the execution of advanced persistent threats and advanced malware. These solutions utilize Artificial Intelligence (AI) and machine learning to protect endpoint systems. One of these solutions, Cylance PROTECT, is an AI-based endpoint software as a service security solution that provides controls for safeguarding against sophisticated threats, thereby preventing the occurrence of breaches. Some of the capabilities of Cylance PROTECT include:

* Device usage policy enforcement to control the use of USB mass storage devices and prevent data theft via removable media.
* Implementation of role-based access control to restrict access to only authorized limited employees.
* Application control to uphold the integrity of installed applications and systems
* Identification of malicious memory use and privilege escalation.
* Rigorous whitelisting and halting of unauthorized executions of scripts that could be malicious.

**Cost:** One-year subscription starting at $45/endpoint for 1-99 endpoints. Price decreases based on volume to $36 for up to 5,000 endpoints and $26 for over $50,000.

|  |  |
| --- | --- |
| **PROS** | **CONS** |
| Device usage access control policy enforcement | This feature seems to be redundant as most organizations use applications that allow administrators to set up proper access controls for employees. |
| A lightweight single-agent allows easy integration with existing software management and security tools. | Cylance PROTECT can’t solely be used as the only security solution since it lacks detection and responding features to potential attacks. |
| Renders malware, ransomware, viruses, bots, and zero-day attacks useless in real-time at machine speed. | Cylance PROTECT doesn’t use traditional means such as signatures analysis, which is still used by some malware to prevent attacks. |

**Expert Decision:**

As most cybersecurity vendors, Carbon Black, FireEye, and Cylance provide unique security solutions to protect organizations against advanced malware and the continuously changing threat landscape. However, careful analysis of these solutions reveals that FireEye’s FireEye Network Security solution is the best fit for our company’s needs. The various reasons for selecting this product with a detail comparison and contrast include:

1. In addition to easy installation or integration with other solutions, FireEye Network Security solution provides enhanced integration across, distributed, physical, virtual, on-premise, and cloud deployment options, which the other two lack. This security capability is critical as most companies have hybrid environments (on-premise and cloud) or will soon transition to using the cloud for their workloads.
2. FireEye Network Security solution provides protection against evasive attacks, zero-day, endpoint containment, and incident response. These capabilities are different from Carbon Black’s solution, which primarily focuses on endpoints and malware protection. It is also different from Cylance’s security solution, which focuses only on prevention and not detection.
3. FireEye Network Security solution uses multi-layer protection, including analysis of internet traffic to accurately detects and immediately stops advanced, targeted, and other evasive attacks, while the other primarily focus on traditional signature monitoring, file integrity, or AI to identify threats.
4. FireEye Network Security solution provides the scalability to scale to thousands of sites, in turn supporting business growth with a short payback period when the organization protects more assets. This cost advantage doesn’t seem to exist with Carbon Black’s and Cylance’s solutions since pricing is determined per endpoint that is protected.