Boundary Protection, Event Management and Incident Response
OVERVIEW

Mapping a Clear Path to Federal Cyber Security and CDM Compliance

Identifying and deploying the best cyber security solutions that comply with the Department of Homeland Security’s (DHS) Continuous Diagnostics and Mitigation (CDM) Program can be nebulous and challenging.

As you enhance your cyber visibility and defense, your agency goals are:

- **Prevention**: Reduce your threat surface and ensure endpoint protection
- **Visibility**: Gain the most comprehensive view of all user behavior to manage risk
- **Scalability**: Maintain protection across your entire agency
- **Manageability**: Experience low-touch governance, integration, and automation
- **Compliance**: Meet federal requirements; achieve and sustain a high AWARE* score

Cyber security is a crowded, confusing market. Compliance regulations are strict. The burden is on security leaders to select solutions that address the need without creating a host of new operational challenges. From capability to deployment and operation, you need the most mature, proven solution to avoid disruptive pitfalls.

With several options on the market using various technologies and architectures, how do you identify what best aligns with your needs and delivers the greatest security?

Following is a guide to help you evaluate market offerings, understand the subtle differences among these tools and solutions, and prepare you to create your ideal cyber security CDM stack.

* Agency-wide Adaptive Risk Enumeration (AWARE) score
Reduce Your Threat Surface and Ensure Endpoint Protection

Agencies today are looking for proven solutions to successfully identify and address ever increasing and dynamic, sophisticated attacks. Skilled security practitioners are difficult to find and retain. And, many agencies employ tools that are not capable of adequately recognizing, preventing and convicting the breadth of malicious activity levied against them.

Prevention starts with knowledge. Part of DHS CDM DEFEND (Dynamic and Evolving Federal Enterprise Network Defense), Software Asset Management (SWAM) requires agencies to "establish and maintain a software inventory, unique identifiers for software, and other properties such as the manager of the software. SWAM also establishes and maintains the actual inventory of all software in accordance with data currency requirements, along with information needed to assess the risk to and physically locate the software."¹

Software Asset Management: Defined in Black and White

When it comes to SWAM, not all solutions are created equally. You’re operating in a dynamic environment: your workforce, software inventory, and the threats you face. Your endpoint solutions should match and track that. Today’s security landscape requires a proactive defense.

It is widely known and accepted that traditional Anti Virus (AV) software, such as blacklisting, is not sufficient to successfully protect endpoints. CDM’s requirement of a positive security model, or whitelisting, is designed to help agencies address unknown threats, along with new and creative attacks. By only allowing trusted software to run, you can provide the best possible protection for systems—including against next-gen attacks.

Immature whitelisting solutions can be restrictive and cumbersome to deploy. Many solutions require several sensors that can create operational complexity, denigrate system resources and increase costs—both in acquisition and sustainment. And, they often lack the maturity and refinement for hassle-free, robust execution, policy setting and management.

However, whitelisting doesn’t have to be an impossible mission. To be successful, it requires smart flexibility through integration and deployment, setting policy, automation and governance. And, yes, it can be done at scale, even for complex operations.

With the right whitelisting tool, you can collect robust data. Create watch lists, alerts, and mine for potential threats. Make changes easily, even at varying departments within your agency. And, do it rapidly in near real time.

Data Loss Prevention

Removable media and external devices—another point of vulnerability of endpoint security—pose a significant threat to agencies both for data loss and introduced attacks. Again, not all solutions are equal. Many don’t govern trust over USBs, such as preventing unauthorized devices and also allowing trusted ones. For example, graduated controls that allow a specific brand of USB drives designated by a set range of serial numbers. And, many solutions typically require a separate tool with a separate sensor, along with policy controls that include an on/off solution.

File Integrity Monitoring (FIM) and File Integrity Control (FIC)

In addition, monitoring the integrity of and changes to files—for example size, code and permissions—is required to prevent malware, ransomware and next-gen attacks. And, it needs to function whether an endpoint is on or off network to dramatically reduce your agency’s attack surface.

Typical FIC/FIM tools often rely on a secure hash algorithm, which is processor intensive. Because of the resources required for those solutions, it is often only possible to perform checks once per day, outside of business hours. If your agency supports multiple operating systems it becomes even more cumbersome, likely requiring the deployment of a separate FIM technology.

You need an integrated, manageable solution that can be automated and filtered to avoid over alerts.

¹ Homeland Security Continuous Diagnostics and Mitigation (CDM) Technical Capabilities Volume Two Requirements Catalog v.1.4
VISIBILITY

Gain the Most Comprehensive View of All User Behavior to Manage Risk

When DHS designed CDM Phase 3, their focus was on the need to manage “what is happening on the network?”—including “preparing for and responding to incidents, ensuring that software/system quality is integrated into the network/infrastructure, detecting internal actions and behaviors to determine who is doing what, and finally, mitigating security incidents to prevent propagation throughout the network/infrastructure”.

To do this, you need maximum visibility of all user behavior and activities.

Agency security teams struggle to collect endpoint data required to proactively hunt for abnormal behavior and properly investigate threats. Security and IT professionals need advanced tools to see beyond suspicious activity, dive deeper into the data to make smarter decisions, and arrest cyber attacks faster.

Part of CDM Phase 3, Operate Monitor and Approve (OMA) includes audit data collection and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing). This capability covers verification and validation of processes/procedures to prioritize incidents and associated response actions, to quickly mitigate the impact of an incident, take appropriate remediation actions to eliminate the impact (restore normal operations) of the same incident, and to support information sharing and collaboration (both internal and external) to minimize or prevent the impact of future incidents.

When a malicious event occurs, swift action is paramount. You must shrink the dwell time—the period of time from when the attack occurs until it is identified and neutralized—to safeguard information and prevent data exfiltration.

According to “The 2018 Cost of a Data Breach Study” by the Ponemon Institute, the average total cost of a data breach was $3.86 million. The mean time to identify (MTTI) was 197 days. And, the mean time to contain (MTTC) was 69 days. Companies that contained a breach in less than 30 days saved over $1 million vs. those that took more than 30 days to resolve.

The best approach is to hunt threats in real time using unfiltered data to be able to visualize the complete attack chain. You need the tools to identify, disrupt and remove known bad malware and ransomware. Detect at-risk software and automatically alert an administrator for a patch from an asset management tool such as BigFix or SCCM. Take action to safely isolate a compromised host, monitor attack behavior, terminate processes, and understand change or drift to recover the host without having to reimagine the system.

Attacks are getting more and more sophisticated. So should your defense tools.

SCALABILITY

Maintain Protection Across Your Entire Agency

Maintaining security inside your firewall is one thing. But, scaling to include hundreds of thousands of endpoints in diverse geographical locations is another. Tracking user behaviors, updating policies and pushing updates, determining threat levels of individual endpoints and adjusting enforcement levels accordingly—all in real time—are just a few challenge areas. Not to mention collecting and storing data, hunting for threats and attacks, and detecting and mitigating them quickly.

Agencies need an advanced application control solution that features trust-based, policy-driven approvals managed by IT and/or through the cloud to reduce the administrative burden on IT and minimize user interruption. At the same time, it needs to detonate or deploy unknown or grey files in a secure environment to determine trust values.

Many application control solutions are closed systems—they don’t integrate with other systems well. To meet these challenges, your application control solution should integrate with your security infrastructure, whether existing or planned. And, you need unlimited scale.

1 CDM Phase 3: “What is happening on the network?”
2 CDM Phase 3: Section J, Attachment Y.2, Section II – 4.3
3 Benchmark research sponsored by IBM Security. Independently conducted by Ponemon Institute LLC.
MANAGEABILITY

Experience Low-Touch Governance, Integration and Automation

Your cyber security solutions, and complete CDM stack, need to work in harmony and be easy to manage. Your agency needs to swiftly and effectively combat the growing number of incoming threats. And, you need to make changes easily, even at varying departments within your agency. Skilled security practitioners are difficult to find and retain, and attackers are becoming increasingly sophisticated.

You need an automated solution that requires low-touch governance. Agencies can greatly benefit from tools such as automated software inventory and approvals, graduated enforcement policies and geographic awareness that detect risk and adjust enforcement levels, along with automated drift reports that can identify high-risk systems.

COMPLIANCE

Meet Federal Requirements; Achieve and Sustain a High AWARE* Score

While maintaining compliance doesn’t ensure security, agencies are required to demonstrate it on a continuous basis and report via a federal dashboard that shows a broader cyber security risk posture across the government. Agencies are given an AWARE score based on CDM compliance.

Demonstrating compliance can be an onerous task for agencies, and often a manual one of aggregating data from multiple logs and systems.

You need a solution that enables you to more easily aggregate your data demonstrating your agency’s cyber hygiene status that can be fed into the CDM federal dashboard.

With all this in mind, how do you select the best solution to create your ideal CDM stack?

*Agency-wide Adaptive Risk Enumeration (AWARE) score
The Carbon Black Difference

Understanding the major challenges agencies face when implementing CDM, Carbon Black does it differently. We mapped our products and services to meet CDM requirements, so you know you’re compliant.

CB Protection: Application Control and Critical Infrastructure Protection

With our industry-leading application control product, CB Protection, we combine application whitelisting, file integrity monitoring, device control and memory/tamper protection into a single-agent solution. This enables you to:

• Lock down critical systems
• Monitor for behavioral indicators of malicious activity
• Prevent unwanted changes
• Establish policy settings to enforce and monitor access to systems
• Restrict access to portable storage devices that could potentially store sensitive information
• Execute trusted and approved software only
• Infinitely scale across your agency using a scalable management architecture
• Ensure continuous compliance with regulatory mandates

Our device control policies ensure that only authorized staff is allowed to copy sensitive data to portable storage devices. CB Protection offers graduated control levels, for example you can choose to permit specific USB drives with particular serial numbers to gain access.

Our solution also includes embedded File Integrity Monitoring and File Integrity Control. No additional agent is required, and there is no incremental cost. We help you safeguard the integrity of your systems and intellectual property by automatically preventing access, modification, and tampering of high-value and sensitive/critical files.

Our Rapid Configurations greatly reduce the time and manual effort required to deploy CB Protection and establish policies. Our solution puts you in control of how you manage your new positive security model. Instead of limiting customization, we deliver flexibility, allowing you to automate trust on endpoints based upon Publishers, Updaters, Directories, Registry and Reputation. CB Protection sensors can report to a single system or multiple management consoles with unified management controls. And, it allows graduated policy levels—including visibility, low, medium, and high enforcement modes. With nearly infinite variable controls, you can apply settings to both individuals and organizational groups.

CB Protection helps you reduce your attack surface and downtime by automating approval of trusted software and eliminating the burden of whitelist management. It has a FIPS-140 Certification and received NSS Labs’ only Perfect Prevention Score (2017 Advanced Endpoint Protection Test). CB Protection also integrates with leading network security providers, including Check Point, Fidelis, FireEye, Palo Alto Networks, ForeScout, and Phantom.

The Carbon Black Difference

THE SOLUTION

Our solution also includes embedded File Integrity Monitoring and File Integrity Control. No additional agent is required, and there is no incremental cost. We help you safeguard the integrity of your systems and intellectual property by automatically preventing access, modification, and tampering of high-value and sensitive/critical files.

Our Rapid Configurations greatly reduce the time and manual effort required to deploy CB Protection and establish policies. Our solution puts you in control of how you manage your new positive security model. Instead of limiting customization, we deliver flexibility, allowing you to automate trust on endpoints based upon Publishers, Updaters, Directories, Registry and Reputation. CB Protection sensors can report to a single system or multiple management consoles with unified management controls. And, it allows graduated policy levels—including visibility, low, medium, and high enforcement modes. With nearly infinite variable controls, you can apply settings to both individuals and organizational groups.

CB Protection helps you reduce your attack surface and downtime by automating approval of trusted software and eliminating the burden of whitelist management. It has a FIPS-140 Certification and received NSS Labs’ only Perfect Prevention Score (2017 Advanced Endpoint Protection Test). CB Protection also integrates with leading network security providers, including Check Point, Fidelis, FireEye, Palo Alto Networks, ForeScout, and Phantom.

CB Protection: Your Comprehensive View to Detect, Respond and Recover

Many solutions available today limit your ability to gather comprehensive data to hunt threats effectively. By recording partial data, they potentially create critical blind spots.

With Carbon Black’s CB Response—the most sophisticated and mature Endpoint Detection and Response (EDR) tool on the market—you can continuously record and store unfiltered endpoint data to see the entire picture of your endpoints, even if they’re offline. Gain complete visibility to rapidly create watch lists and alerts, mine info for potential threats, proactively identify threats, visualize the complete attack kill chain, significantly reduce attack dwell time, and accelerate your hunting and response.

Engineered from the threat perspective and mapped to NIST, CB Response delivers:

• Faster end-to-end response and remediation
• Accelerated IR and threat hunting with unfiltered endpoint visibility
• Secure remote access to infected endpoints for in-depth investigation
• Better protection from future attacks through automated hunting
• Unlimited retention and scale for the largest installations
• Reduced IT headaches from reimaging and help desk tickets
• Rapid identification of attacker activities and root cause

Skilled threat hunters are a scarce resource. Empower them to accomplish more with their time. With CB Response, investigations that typically take days or weeks can be completed in just minutes.

We understand the increasing complexity of emerging threats. Carbon Black, founded by offensive cyber experts in the U.S. Intelligence community, developed our CB Response solution to outpace increasingly sophisticated attacks.

CB Response is refined to give you rapid configurations and automated processes to simplify deployment and governance. It offers flexible enforcement levels for a graduated rollout. You can detect and ban malware from running on a host that may be deemed compromised from a single management console. And, like all of our solutions, it features an open API and is pre-integrated with a wide range of critical tools in the CDM stack, such as Splunk, IBM’s BigFix, ForeScout, and others.

CB Protection and CB Response are both cross-platform compatible and operate on Windows, Mac and Linux machines to keep all endpoints and servers secure, whether they are on or off the network. Both solutions are on the CDM Approved Products List. 4

Carbon Black engineered CB Protection and CB Response to increase your visibility and protection through an integrated management infrastructure, making it easier to analyze information and report quickly. Summary information can be delivered to the CDM dashboard, contributing to the broader cyber security risk posture across the federal government. This allows agencies to increase metrics and raise their AWARE score.

Based in the USA, Carbon Black is dedicated to protecting your agency’s and our country’s sensitive information. We give you the tools to defend our nation against cyber attacks.

---

1 NSS Labs’ Advanced Endpoint Protection (AEP) Test
2 CDM Approved Products List

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the CB Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,600 global customers, including 35 of the Fortune 100, trust Carbon Black to keep their organizations safe.

Carbon Black was founded by former members of the U.S. government’s elite team of offensive security hackers. Trained by the NSA and CIA, our founders possessed early insights into the tools and techniques of 21st century cyber hackers; namely, how to get around defenses. For more than 15 years, our leadership and software have used that experience to outpace increasingly sophisticated attacks.

Carbon Black, CB Protection, CB Response and CB Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and/or other jurisdictions.

1100 WINTER STREET, WALTHAM, MA 02451, USA • P 703.587.7559 • F 617.393.7499
WWW.CARBONBLACK.COM/FEDERAL