COALFIRE

WHITE PAPER

Advancing Security Maturity with VMware Carbon Black

Carbon Black Cloud Applicability to the NIST Cybersecurity Framework

MICHAEL BURKE, PHD, CISSP, CISA, C|CISO, PCI-QSA
PRINCIPAL

vmware

877-224-8077 | info@coalfire.com | Coalfire.com

Table of contents

Executive summary

Organizations are increasingly reliant on information technology for day-to-day operations, and this ubiquity has exposed more surface area for malicious actors to gain entry to an organization's infrastructure. Additionally, the highly mobile workforce that has evolved in response to COVID-19 has introduced additional challenges for organizations seeking to secure their environments, increasing the likelihood of a cybersecurity event. Costs of such cybersecurity events include intangible costs (e.g., productivity loss, reputation damages, and system downtime and repair) and tangible costs (e.g., fines, lawsuits, and regulatory actions).The cost of cybersecurity breaches for 2021 is expected to reach $6 trillion USD globally, exceeding the GDP of Japan and totalling nearly one-third of the GDP of the United States.

As a result, cybersecurity has become an integral part of the daily operations, risk modeling, and budgetary process of organizations, regardless of the organization's size, industry, or complexity. Continued focus on security programs is an important and integral step toward a sound defense against constantly emerging threats. As threats continue to emerge, organizations can improve their position and ability to protect their key infrastructure, business secrets, and, most importantly, their bottom line by establishing a structured cybersecurity program that leverages a proven framework. The National Institute for Standards and Technology (NIST) Cybersecurity Framework ("CSF" or "Framework") is such a framework and is a collection of best practice controls that have been developed to assist organizations address cybersecurity risks, regardless of industry.

To assist organizations with implementing such a structured cybersecurity program, VMware, Inc. ("VMware") engaged Coalfire Systems, Inc. ("Coalfire"), to conduct an assessment of VMware Carbon Black Cloud ("Carbon Black Cloud") against the NIST CSF v 1.1 standard.

Objectives of this white paper

This white paper seeks to explicate how Carbon Black Cloud platform can assist organizations in meeting cybersecurity challenges and in approaching higher levels of maturity within the NIST CSF. To achieve this, members of the Coalfire Advisory Team evaluated product documentation, system security plans, and technical briefs in conjunction with the security framework controls and standards that were available at the time of publication.

Understanding of Carbon Black Cloud and its capabilities was gained through review of product specifications, documentation, and demonstrations provided, as well as through analysis of information found on VMware's public-facing website. As an advisor to VMware, Coalfire was also provided detailed internal technical materials, configurations, provisional assessment artifacts, and, critical to the review, access to the compliance package materials.

NIST Cybersecurity Framework overview

The NIST CSF is an internationally recognized collection of controls that provides a time-tested methodology for the assessment and management of cybersecurity risk. While the framework is voluntary, more than 20 states use the CSF as a framework. Translated into 15 different languages, the CSF has also become a platform that is being used in the establishment of legislative and regulatory mandates on the international stage, clearly showing that best practices transcend geopolitical boundaries.

NIST published version 1.0 of the CSF in February 2014 in response to Executive Order (EO) 13636 and, subsequently, the Cybersecurity Enhancement Act of 2014, as an effort to improve the cybersecurity of critical infrastructure. NIST released its most current version, version 1.1, of the Framework in April of 2018. Currently, NIST is revising the CSF to version 2.0 and is expected to publish the new standards before the end of 2023.

The CSF is being updated using a process similar to that utilized for the v1.1 update: implementing a public comment period where cybersecurity experts in various industries provide feedback to improve the Framework to better meet the objectives of a mature cybersecurity program. The comment period enables the cybersecurity community to address recently emerging threats, propose strategies to identify threats, and advance methods of risk reduction, in addition to establishing an easily understood method for communicating an organization's ability to address cybersecurity risk to stakeholders. This common language leverages the concept of maturity modeling for easy understanding.

Figure 1: NIST depiction of the CSF security Functions

Currently, in the CSF, maturity is assessed within five (5) security Functions: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover. Each Function consists of various Categories and Subcategories that break the security Functions into prescriptive technical activities or "controls." As represented in Figure 1, each Framework Function represents a "slice" of an organization's cybersecurity management "pie." Only when considered together do they represent a holistic approach to managing security risks.

Under the CSF, the concept of maturity is utilized to communicate the level to which the organization is meeting the intent of the control. This maturity measurement is reported as a number 1 through 5, with Level 1 indicating an initial level of maturity and Level 5 indicating that the organization has optimized its mastery of the controls and can demonstrate this repeatedly using a measured and managed approach. The use of a maturity measurement has not only been adopted by compliance frameworks but is also leveraged as a familiar mechanism for describing organizational maturity concepts that is easily understood by all levels of management, from IT management through senior executives and board members. Maturity reporting is done in such a manner so as to provide a consistent and understandable picture of an organization's ability to meet cybersecurity challenges.

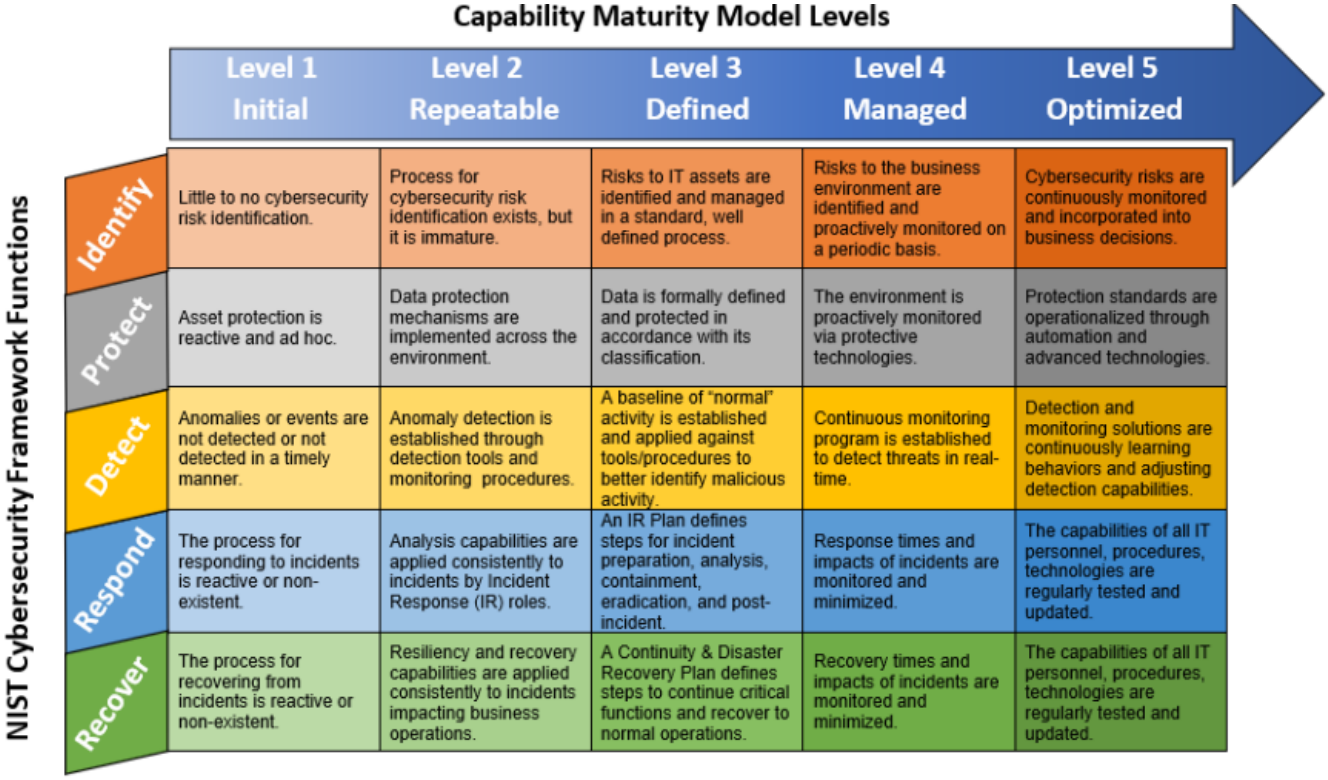

Figure 2: Cybersecurity Maturity Level Scale

As mentioned above, the CSF is organized into Functions, which are further divided into Categories. In turn, these Categories are divided into Subcategories and and associated Informative References, which provide the starting points for implementing practices to achieve the desired outcomes. The Informative References provide the connection between the framework's core Functions and its operational objectives, along with guiding principles from other frameworks. As shown in Figure 3, the CSF best practices are connected closely with other frameworks, such as Control Objectives for Information Technologies (COBIT) 5, ISO 27001, and NIST SP800-53r4. Establishing maturity with these controls under the CSF will ease the uplift for any organization aspiring to achieve certification within the other frameworks.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figure 3: NIST CSF Informative References

Improving cybersecurity maturity

Once the current maturity level is established, an organization can begin to develop strategies for improving their cybersecurity maturity. To succeed in improving to the next level of cybersecurity maturity, an organization must take a holistic approach to where and how they invest time and resources. A cybersecurity roadmap must include the three elements for successful organizational transformation: people, process, and technology (PPT). Neglecting one or two will slow cybersecurity maturity improvement and could introduce vulnerabilities in the cybersecurity environment.

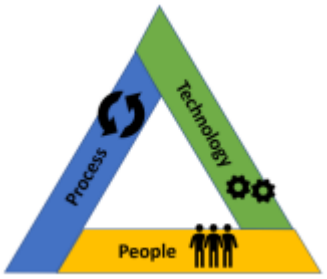

Figure 4: The PPT Triad

The following section focuses on the "technology" portion of the triad and describes how endpoint security technologies applied following the NIST CSF can improve cybersecurity maturity. It is important to keep in mind that, while endpoint security technologies are effective in improving cybersecurity posture, the elements of "people" and "process" are also essential for a mature cybersecurity program.

Endpoint security technologies

Endpoint security protects an organization's endpoint devices (e.g., workstations, mobile devices, tablets, and servers) against both internal and external threats and vulnerabilities. Endpoint attacks attempt to compromise the confidentiality, integrity, and availability of information and IT assets in order to compromise or exfiltrate sensitive information and data. These attacks can lead to reputational and financial damage to organizations.

The cost of responding to and recovering from a successful attack on an endpoint, as reported by the Ponemon Institute in 2020, has increased from an average of $7.1 million to $8.94 million per attack. These costs are attributed to end-user productivity loss, theft, damage and repair of IT infrastructure, brand damage, lawsuits, fines, and regulatory actions. Interestingly, the cost of system downtime has decreased significantly since 2017, which reveals that other costs have increased at higher rates than is represented in aggregate values.

Endpoint security solutions provide the first line of defense for organizations, as they become the interface between the people and process portions of the PPT triad. However, many organizations have found that there are challenges in the implementation of these solutions. End users have complained that endpoint security is both inconvenient and resource intensive. The Ponemon Institute reported in 2020 that organizations are struggling with deploying updates and patches to endpoint security products. The same report stated that “traditional anti-virus solutions, deployed on endpoints, missed 60% of the attacks.”

To alleviate these concerns, advanced endpoint security technologies, when combined with the computational power and operational efficiency of the cloud, provide an improved, proactive alternative to traditional anti-virus solutions for threat protection. As part of a comprehensive security program designed to reduce enterprise risk, organizations should consider leveraging an endpoint protection platform to perform inspection once and then use those results to improve security in multiple different ways. The sections below describe how different endpoint security capabilities delivered from a cloud-native endpoint protection platform can be applied in line with various parts of the NIST CSF Functions, Categories, and Subcategories to improve cybersecurity maturity.

VMware Carbon Black Cloud overview

VMware Carbon Black Cloud 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. Carbon Black Cloud enables organizations to implement NGAV, NGAV remote configuration, vulnerability management, and remote console, along with audit and remediation services. All services are configured using a single console with feature visibility controlled by product subscription level. Threat signatures and identification is managed by VMware, with the ability to define custom behaviors and alerting to provide streamlined detection, prevention, and response to cyber attacks.

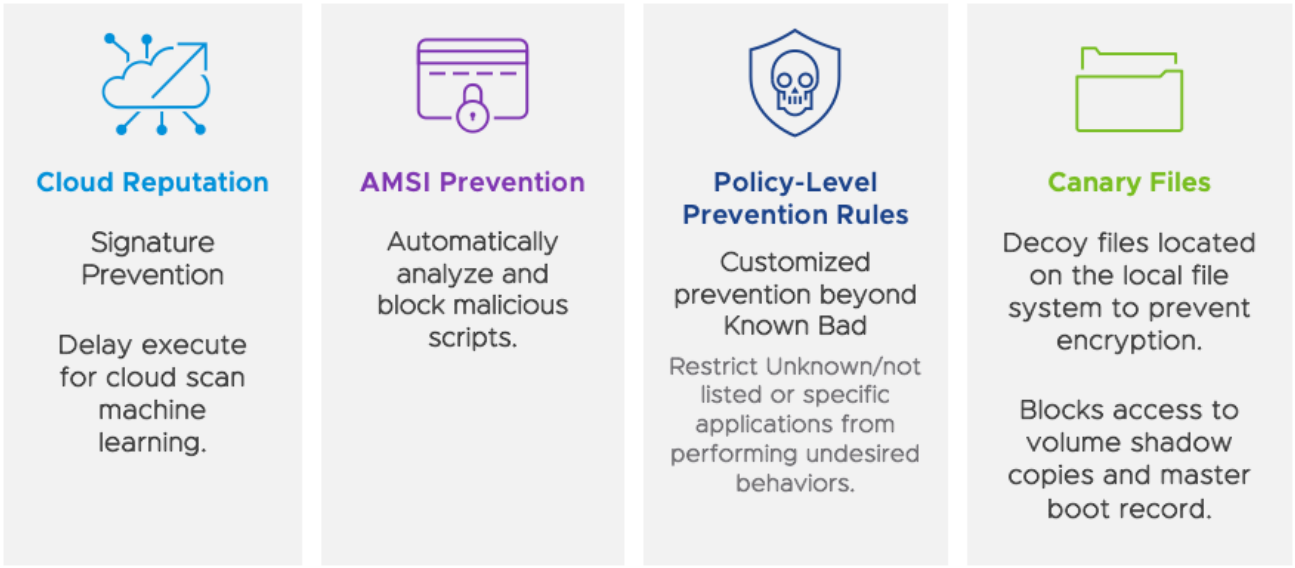

Figure 5: Carbon Black Cloud

Carbon Black Cloud, organizational operations, and the NIST CSF

The NIST CSF Identify Function

The NIST CSF Identify Function assists in formalizing a process of identifying and managing cybersecurity risk to systems, people, assets, data, and business processes. Having a clear understanding of the business environment and the related cybersecurity risks enables an organization to focus, prioritize, and align risk mitigation efforts with its risk management strategy and business needs. Categories within this Function include Asset Management and Risk Assessment.

A consolidated endpoint security solution, like Carbon Black Cloud, helps achieve the objectives of Asset Management by providing an organization with a centralized platform to view, update, and manage the security of its endpoints. Consolidating this with a fully integrated platform enables the organization to have a single and complete source of truth for its assets. With all assets in a centralized tool, management has visibility into the environment and is better positioned to make well-informed decisions.

The Carbon Black Cloud endpoint security solution offers real-time risk assessment of the threats in an environment. These threats can be quantified to further understand the likelihood and impact of the threat if it were to successfully exploit an organizational asset. With comprehensive insight, management can make more informed decisions and

respond to the threat with the appropriate action on those risks (i.e., acceptance, avoidance, mitigation, and transference) that corresponds with the organization's tolerance for risk.

A visual depiction of the systems and services that constitute the Carbon Black Cloud management plane is represented below.

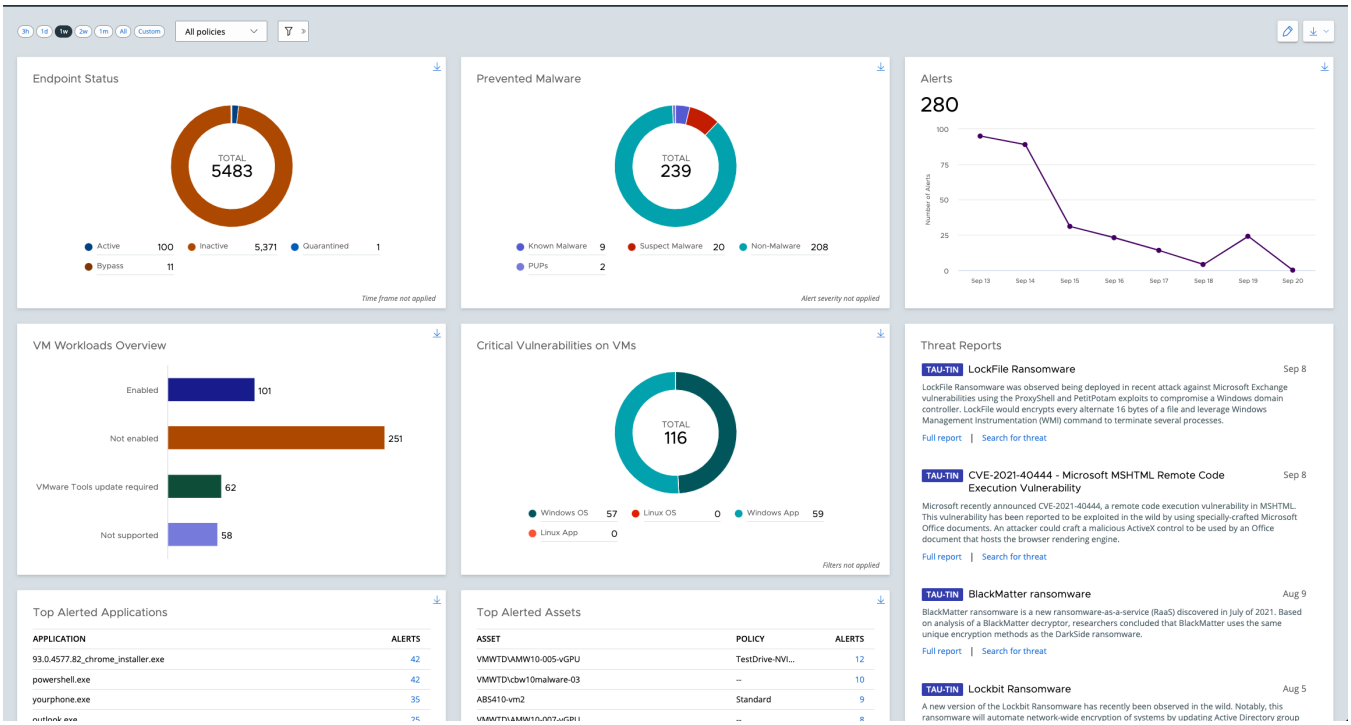

Figure 6 Carbon Black Cloud Management Plane

The NIST CSF Protect Function

The NIST CSF Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services and to defend against threats to business processes, critical assets, data, and information. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Categories within this Function include Data Security and Protective Technology.

Endpoint security solutions are one of the key technology solutions required to protect data-at-rest stored on endpoints. Next-generation endpoint products include both traditional anti-virus functions and next-generation intelligence abilities to protect endpoints against known and unknown attacks. The traditional anti-virus part of these solutions restricts unauthorized access to environment through malware, spyware, and viruses. The next-generation intelligence part involves integrity checking mechanisms to verify that activity on the hardware and software is legitimate and authorized. Endpoint security solutions give an organization visibility in order to protect sensitive data from sophisticated threats by providing data security controls to the environment.

Protective technologies enable organizations to rely on their security mechanisms to meet business standards, processes, and expectations. An organization's Configuration Management Program should be built around the principle of least functionality. Essentially, systems should be configured to allow only essential functions and capabilities and to prevent circumvention of these controls. Endpoint security configuration management is an essential piece of the Configuration Management Program, as endpoint security solutions block and alert on unknown, unauthorized, or malicious activities occurring on or within the organization's IT environment. This creates a hardened environment and allows an organization

to meet the configuration management requirements, thus improving their overall cybersecurity maturity and reducing risk.

The NIST CSF Detect Function

The NIST CSF Detect Function enables the timely discovery of cybersecurity events and threats in the environment. Categories within this Function include Anomalies and Events and Security Continuous Monitoring.

The objective of the Anomalies and Events Category within the NIST CSF is to detect and analyze threats in the environment. A well-developed process for analyzing threats allows an organization to take quick action to contain and eradicate a threat before it can cause significant damage. Endpoint security solutions are valuable tools for identifying and detecting anomalies and events in assets throughout the environment. Endpoint security solutions are backed with threat intelligence feeds, based on big data analytics, in order to segregate "normal" user behavior from anomalous activity. These solutions alert on unauthorized or suspicious behavior to enable the organization to perform further analysis in real-time. These rapid detection solutions allow organizations to make proactive decisions to further protect their information and information assets.

The objective of the Security Continuous Monitoring Category is to monitor the organization's network, endpoints, and connections (internal and external) to detect threats and vulnerabilities in the environment. An effective continuous monitoring program enables an organization to identify threats in real-time and take timely action. A comprehensive Security Continuous Monitoring Program is incomplete without an endpoint security solution. Endpoint security solutions reside on endpoints in the environment (e.g., workstations, servers, and mobile devices) and continuously monitor activity, comparing activity against a "normal" baseline to detect anomalies that could be indictors of a threat. These solutions improve cybersecurity maturity and reduce risk by providing organizations with improved visibility into their environment while reporting and alerting on any suspicious activities. Leveraging the computing power of the cloud and the continuous improvement of threat intelligence enable these endpoints to detect more threats.

The NIST CSF Respond Function

The Respond Function includes activities around taking appropriate action when responding to a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Categories within this Function include Analysis and Mitigation.

The Analysis Category's objectives include the ability to effectively triage and investigate alerts from detection systems. A triage process enables an organization to determine the impact of alerts and to prioritize responses. In addition to the advanced threat protection capabilities, most endpoint security solutions offer in-depth analysis on identified threats. Supported by big data analytics and advanced forensics, endpoint security solutions provide immediate access to a more complete picture of an attack, including root cause, vulnerability source(s), and the number of hosts impacted. This aids in improving an organization's analysis and investigation processes, improving response time from days to minutes. As a result, organizations with effectively implemented endpoint security solutions experience a higher level of cybersecurity maturity and reduced cyber risk.

The objective of the Mitigation Category is to contain and mitigate incidents. Containing incidents is essential for limiting the impact and the breadth of damage to assets and IT infrastructure. As most malicious hackers can steal data or do significant damage to IT infrastructure within the first 12 hours after a breach, once an attack penetrates the environment, the clock starts. With this tight timeframe, every minute counts. To counter these attacks, many endpoint security solutions offer the capability of "live response," or real-time remediation services. Endpoint security threat responders provide services to isolate threats and stop processes, reducing potential overall damage to an organization's operations. The ability to isolate and block threats in near real-time is a substantial benefit to organizations deploying and maintaining an efficient endpoint security solution.

The NIST CSF Recover Function

The Recover Function includes the activities necessary to maintain resiliency plans and to restore capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. One Category within this Function is Recovery Planning.

The objective of the Recovery Planning Category is to establish and execute sound processes in response to an event in order to efficiently return to normal operations. The impact of a cyber event or incident is significantly reduced based on the speed at which an organization can return to normal operations. Advanced endpoint security solutions assist with all phases of incident response (e.g., preparation, detection, analysis, and mitigation), making recovery a streamlined process. Organizations that include their endpoint security solution's forensic capabilities into their Incident Response Plan(s), Business Continuity Plan(s), and Disaster Recovery Plan(s) enable them to make quick decisions, respond effectively, remediate efficiently, rapidly recover, and improve their overall cyber security maturity.

VMware Carbon Black Cloud NIST CSF control considerations

The Detect Function of the NIST CSF, and the subcategories contained within that function, are Carbon Black Cloud strong points, as the product is specifically designed to detect and report cybersecurity events. The Detect Function is split into three Categories: Anomalies and Events, Security Continuous Monitoring, and Detection Processes. Further, these categories are split into their Subcategories for measurement. The Carbon Black Cloud product provides the underlying foundation for organizations to meet these control groups. Below are some examples of how Carbon Black Cloud provides support for controls (dependent on configuration and licensing):

- Carbon Black Cloud agents monitor USB port status and alert for unauthorized devices. (NIST CSF DE.CM-7 and PR.PT-2)
- Carbon Black Cloud agents aggregate security event data and correlate that data across all alert sensors. (NIST CSF AE-3)
- Carbon Black Cloud agents alert responsible personnel when events are detected. (NIST CSF DE.DP-4)

Utilizing Carbon Black Cloud also provides additional control benefits as a function of the service itself. Due to the inherent properties of a cloud-based, SaaS product, organizations are no longer responsible for the daily management of the Carbon Black Cloud platform itself. This permits customers to gain the benefits of the detection and management platform being maintained and updated by staff who are product experts. The benefits of using this model yield specific control considerations. Some examples where these benefits are apparent:

- The Carbon Black Cloud product is continuously improved. (NIST CSF DE.DP-5 and PR.IP-7)
- Events detected are consistent with established criteria. (NIST CSF RS.CO-2)

The Carbon Black Cloud Audit and Remediation and Enterprise EDR offerings are closely tied to the NIST CSF Respond function in the Category of Analysis (RS.AN).The Audit and Remediation module allows for organizational understanding of the incident and enables organizations to collect and analyze data in real time and to formulate response activities. In addition, the use of the Audit and Remediation modules permits organizations to establish responses that meet the NIST CSF Category of Improvement (RS.IM).

The Respond Function of the CSF acts as an extention to the Protect Function, in that it requires organizations to learn and respond to incidents and reports. The Carbon Black Managed Detection & Response (MDR) offering provides the mechanisms to contain security incidents, modify policy, and quarantine affected devices. The features of MDR provide responses to the Mitigation Category within the NIST CSF RS.MI, providing for the containment and mitigation of risks.

Conclusion

Coalfire reviewed VMware Carbon Black Cloud's effectiveness to meet the NIST CSF controls and their defense-in-depth approach to identifying the environment, protecting the environment, and detecting, responding to, and recovering from threats. Coalfire has determeined that the Carbon Black Cloud platform is highly aligned with the control requirements established by the NIST CSF and that organizations are able to leverage the products within the Cabon Black Cloud suite in a manner that would improve their ability to meet or exceed the control requirements established by the NIST CSF. Coalfire is of the opinion that VMware Carbon Black Cloud **can be effective** in providing the applicable best practices to meet the rigor for NIST CSF controls and that it has the capability to ensure a path for enhancing the maturity level of those programs with respect to technology.

As part of this analysis, Coalfire leveraged the fact that the Carbon Black Cloud architecture has the ability to meet the FedRAMP High baseline by reviewing its FedRAMP package and cross-referencing those controls within the informational resources. The means that Federal agencies, state agencies, public sector entities, and auditing consultancies should have assurance that Carbon Black Cloud is capable of providing services that meet the best practices outlined within the NIST CSF.

Leveraging just one endpoint agent and one cloud-based console, Carbon Black Cloud delivers comprehensive visibility into every endpoint of an organization in which it is deployed. Without ever having to redeploy to use a new service, Carbon Black Cloud scales and provides more advanced capabilities to an organization as it matures its security program, allowing it to not only stay secure today, but to remain resilient as threats change over time. Carbon Black Cloud allows for increased awareness of what is happening in an environment and for a better hardened security posture as each new threat is taken into account. Carbon Black Cloud is currently available for use, and deployment documentation useful to specific compliance objectives may be obtained from VMware.

This Coalfire review is a result of analysis of documentation and demonstrations provided by VMware, documentation from the FedRAMP marketplace (SSP and POA&M), plus a confirming review of the per-control NIST CSF Informative Resource artifacts. VMware Carbon Black Cloud should be implemented in alignment with an organization's mission, values, policies, procedures, and business objectives, as well as their general approach to security and security planning as defined by their Governance, Risk, and Compliance (GRC) program.

A comment regarding regulatory compliance

Coalfire disclaims any product's capacity to establish regulatory compliance strictly by use of a product. Agencies and audit entities attain compliance through a GRC program, not solely through product selection and use. This is true for all organizations leveraging third-party compliance and for customers targeting compliance with other regulations.

Legal disclaimer

information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

Additional information, resources, and references

This section contains a description of the links, standards, guidelines, and reports used for the materials used to identify and discuss the features, enhancements, and security capabilities of VMware Carbon Black Cloud.

https://carbonblack.vmware.com/

About the authors

Michael Burke, Ph.D., CISSP, CISA, C|CISO, QSA | *Principal Consultant, Payments Advisory & Product Guidance*

With over three decades of information technology management and information security compliance experience, Michael is responsible for thought leadership and advocating solutions to the complex requirements of business risk and compliance mandates. His direction, which synthesizes the importance of cybersecurity and sustainable business operation, has helped numerous organizations strengthen their cybersecurity posture.

About VMware Carbon Black Cloud

VMware Carbon Black Cloud is a cloud-native, endpoint and workload protection platform that combines intelligent system hardening with the behavioral prevention needed to keep emerging threats at bay, using a single, easy-to-use console. By analyzing more than 1 trillion security events per day, VMware Carbon Black Cloud proactively uncovers attackers' behavior patterns and empowers defenders to detect and stop emerging attacks.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.