White Paper

Bitdefender®

Hardening the Endpoint

A Future-Proof MSP model for endpoint security

Introduction

Endpoint security is one of the fastest growing revenue drivers for MSPs as the endpoint continues to be the Achilles heel for most organizations. Thirty percent (30%) of all breaches last year were driven by malware via the endpoint. Worse, in healthcare, 85% of the malware was ransomware, and the primary vector for delivering this malware was via email.[1]

From a services planning/delivery perspective, the continual addition of endpoint technologies (e.g., AV, anti-malware, firewalls, IDS/IPS, authentication services, backup, disk encryption, content control, artificial intelligence, and machine learning) and continually changing nomenclature for these technologies (e.g., endpoint security, endpoint protection platforms (EPP), endpoint detection and response (EDR) platforms) is challenging for MSP customers. The question on every MSP business development person's mind is what is the next technology/service we need to deliver and how do we describe this technology so that our customers will understand the value and be willing to pay for it?

The purpose of this report is to take a step back and focus on meeting underlying goals that all MSPs have:

- Delivering high-value, high-growth multi-tenant services that are scalable, and modular
- Meeting customer needs for remote monitoring/support and endpoint security matching their unique business/industry requirements, including meeting privacy and Industry regulations including HIPAA, HITECH, GDPR, and PCI DSS
- Delivering maximum security, minimum impact, and maximum return for the customer

Rather than bolting on the hottest endpoint security technology and justifying the next endpoint security acronym we propose a pragmatic and strategic approach. This future-proof approach leverages the internationally acclaimed NIST Cybersecurity Framework (NCSF) to map out a plan for hardening the endpoint. This approach empowers MSPs to deliver the highest levels of endpoint security and regulatory/industry compliance in a practical, layered, logical, and infinitely expandable way.

The NCSF: Breaking the Cyber Kill Chain

First published in 2014, the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity is the defacto framework for organizations in critical infrastructure – including government, financial services, and healthcare. More commonly known as the NIST Cybersecurity Framework (NCSF), the NCSF focuses on "using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."[2]

For MSPs, the NCSF applicability goes well beyond critical infrastructure organizations. As NIST states, "the Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience."[3] Underscoring the broad applicability of the NCSF, many trade associations including financial services, healthcare, legal, manufacturing, professional services, and retail have jumped onto the NCSF bandwagon.

The NCSF is perfect for MSPs looking to raise the endpoint protection discussion from point solutions to a risk-based, longer-range, more comprehensive approach. As discussed in this report, hardening the endpoint via a layered approach meets today's endpoint security needs while laying out a framework for continual renewal and expansion as new threats, vulnerabilities, and technologies emerge.

LAYERED FLOW

The NCSF defines a layered flow approach.

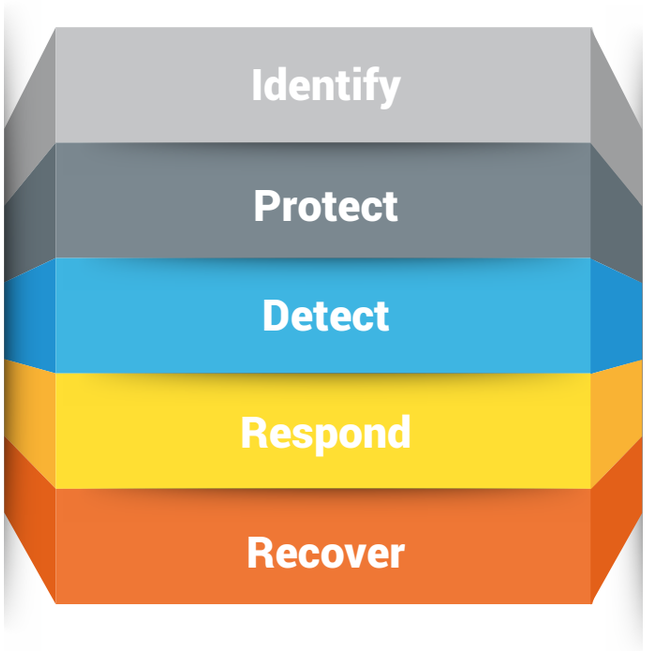
The underpinnings of the NCSF Core is aligning cybersecurity and risk management against the cyber kill chain (CKC), formalized by Lockheed Martin over a decade ago. The CKC maps the typical adversarial path along seven steps from Reconnaissance through Actions on Objectives. Each of the five core functions map directly to the CKC steps.

The NCSF Core defines a layered approach where Identify directs the assets to be Protected which in turn limit the realm of Detection which in turn drives the Response process, ultimately leading to Recovery.

The NCSF Core

The NCSF Core consists of five essential functions: Identify, Protect, Detect, Respond, and Recover. As NIST states, "when considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk."[4]

In this report, we focus the NCSF core exclusively on MSPs hardening client endpoints with an eye to Industry and Regulatory compliance (e.g., HIPAA, HITECH, GDPR, GLBA, and, PCI DSS).



Identify

The first NCSF core function is Identify. As defined by NIST, the function's goal is to "develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities."[5]

The most relevant Identify categories for an endpoint hardening model are:

- Asset management - Identify all assets at the endpoint automatically
- Risk assessment and risk management - Establishing and managing risk including all vulnerabilities and threats
- Governance - Aligning with regulatory, legal, industry requirements such as GDPR, HIPAA, HIGHTECH, and PCI DSS

Automated asset discovery is the cornerstone of the entire model because an unidentified asset is an unprotected, or worse, a malicious asset.

For asset discovery, MSPs must deliver a unified dashboard visually representing all endpoint assets in real-time. This dashboard becomes the display foundation for all five NCSF core functions. For example, the dashboard must show the current vulnerability status of all assets as well as threat context, suspicious activities, and notifications.

Identify ***The MSP offering must include automated asset detection of all endpoints. This must also include ability to detect when new assets join the network.***

Central to identifying assets is also recognizing the asset environment. It is a given in today's IT organization that most servers are virtual (e.g., VMware ESX, Microsoft Hyper-V, Citrix XenServer, and Oracle VM) and many of these virtual instances are running in the cloud (e.g., Amazon AWS, Azure VM, or Google Cloud). The asset environment affects all five NCSF functions. In particular, it is critical that an MSP solution offer Protect and Detect solutions that are hypervisor and cloud agnostic.

Identify also lays out the groundwork for risk management, governance, and regulatory compliance. Compliance is top of mind for many businesses, and it should be part of the initial planning for endpoint hardening. For example, in a recent MSP survey, "among respondents in the Americas, 75 percent said they or their customers are impacted by HIPAA and 59 percent by PCI DSS."[6] While many people consider governance an afterthought –something addressed after the endpoint security discussion – the NCSF moves governance and regulatory compliance to the front of the line.

Identify ***The MSP offering must include a unified dashboard with full visibility and RMM integration along with auto-discovery and immediate notification of new assets.***

In the world of MSPs, dashboard delivery is part of a Remote Monitoring & Management (RMM) solution. In fact, "nearly half of respondents worldwide named RMM as the most important application" in the MSP application portfolio.[7] Whatever endpoint hardening approach an MSP takes, the underlying technology must integrate with RMM.

Identify ***The MSP offering must include a unified dashboard with full visibility and RMM integration along with auto-discovery and immediate notification of new assets.***

Protect

Building upon the asset discovery/management and governance functions of Identify, the Protect function "develops and implements appropriate safeguards to ensure delivery of critical services."[8] The protect function includes all the security technologies associated with EPP: antivirus, anti-malware, firewall, email security, patch management, etc.

Most endpoint security vendors start – and end– the discussion with protective controls. Rather than merely offering EPP, following the NCSF gives MSPs a structured model to put EPP in perspective of the bigger picture: pulling through all the capabilities of asset management, visibility, automatic discovery and full regulatory/industry compliance. For example, implementing AV and anti-malware on a separate console from firewall and device control is entirely out of alignment with the Identify function and therefore, does not fit the model.

The five Protect areas necessary for an endpoint hardening model are:

Identity management and access control

Stealing credentials is the top hacker action for breaches in 2017.[9] Fundamental to security best practice is locking down credentials and access. To illustrate the importance of this, PCI DSS and other privacy regulations specifically call out requirements for identity management and access control.

Protect ***An MSP offering should include a zero-trust policy enforcement mechanism, multi-factor authentication and single sign-on for complete identity management and access control. Implementing these capabilities are essential for blocking insider threat and preventing lateral movement by malicious actors.***

Data security

As with identity management and access control, securing data at rest and in motion are explicit requirements in GDPR, GLBA, HIPAA, HITECH, and, PCI DSS. As stated in the 2018 DBIR, "The theft or misplacement of unencrypted devices continues to feed our breach dataset. Full Disk Encryption (FDE) is both an effective and low-cost method of keeping sensitive data out of the hands of criminals."[10]

Securing data at rest – particularly from a compliance perspective – includes encryption, key management and the policies and reporting associated with encrypted assets. Though Windows and Mac have built-in encryption (BitLocker and FileVault), key management and key recovery become essential MSP service offerings. However, encryption alone is insufficient for compliance. For example, in the event of a breach, the breached organization must prove that breached data was encrypted and that the encryption keys were secure. To support this requirement, the MSP endpoint hardening solution should offer reporting of both encryption and key status for all protected assets.

Protect ***An MSP offering should include full disk encryption, key management, and reporting for data security. Full disk encryption is the best protection against data breach due to theft or loss.***

Information protection processes and procedures

This category is the heart of the Protect function, including what most MSPs offer as EPP. This area includes AV/anti-malware, firewall (web/network), IDS/IPS, and content controls.

MSPs must be aware that advanced malware is polymorphic and increasingly fileless, evading many AV/Anti-malware solutions. This type of malware is typical of advanced persistent threats (APT) and high-value phishing attacks. Still, many attacks look for "low hanging fruit" relying on older techniques, tactics, and procedures which basic AV/Anti-malware detect. It is essential that the AV/Anti-malware solution be comprehensive, protecting against all forms of malware: basic and advanced.

The MSP endpoint hardening solution is only as secure as its AV/anti-malware effectiveness. MSP customers must look to independent testing methodologies and organizations to determine the accuracy of different offerings. For example, just because a product uses AI and machine learning does not mean the product has high accuracy with low false positives.

Protect ***An MSP offering should include comprehensive antivirus & anti-malware (with independent testing); anti-exploit; email scanning and file quarantining; and, firewall with IDS.***

As discussed below, patching is a critical service to address known vulnerabilities. The MSP offering must also include anti-exploit technology to address unknown vulnerabilities and zero-day exploits.

Maintenance

Good security hygiene is the protection of data confidentiality, integrity, and availability. Maintenance is particularly relevant to MSP services since it includes remote maintenance and patching. As shown in the high-profile 2017 Equifax breach, patching is essential to breach prevention. As a compliance requirement, patch management is explicit in multiple regulations (e.g., PCI DSS 6.2 and HIPAA Administrative Safeguards Protection Against Malicious Software).

Protect ***An MSP offering should include device control for locking down USB ports to specific USB tokens or completely blocking USB access. This also includes web filtering; and, search guidance and content control***

Protective technology

A bit of a catch-all category, protective technology "ensures the security and resilience of systems and assets."[11] Typical technology discussions around protective technology include removable media protection, least privilege, network controls, availability, and resiliency.

Another way to look at protective technologies is these are technologies that significantly reduce the potential of exploit due to human error. For example, blocking USB ports prevent users from inadvertently installing an infected USB stick. Similarly, incorporating advanced content control filters (e.g., blocking access to gambling and pornography sites) significantly reduces the potential a user will click on a malicious link. Following the layered approach concept, the sooner an organization blocks the attack vector (i.e., Protect function vs. Detect function) the more benefit to the organization. Simply put, it is far better to remove the malicious link then to rely on detection and response solutions after the user clicks the mouse.

Detect

At the center of the endpoint hardening model is the Detect function. The Detect function requires developing and implementing "appropriate activities to identify the occurrence of a cybersecurity event."[12] Though this sounds straightforward, this is one of the most involved and complex functions of endpoint hardening. And, this is the area of most significant differentiation between vendors in the EPP and EDR space.

The goal of the Detect function is reducing dwell time. Dwell time is how long attackers persist in the network before detection. On average it takes organizations 6.5 months to detect a breach and over two months to contain the breach.[13] Of course, detection is not just detecting a breach. Ideally, it is detecting indicators of compromise (IoC) well before a breach of private, financial, or protected health data.

Good detection comes with a measurable benefit. As Ponemon states in its 2018 Global Cost of Data Breach Report, "the faster a data breach can be identified and contained, the lower the costs." Companies detecting a breach in under 100 days saved over $1M in comparison to companies taking more than 100 days.[14]

EDR VS. ED&R

oday's hottest endpoint offering is ndpoint Detection and Response EDR). NIST explicitly separates etection and response for good eason. The response is only as ood as the detection and lumping he two functions together can hide olution weakness. Plus, detection nd response must integrate with yers above and below.

The Detect function succeeds only when the organization identifies all assets correctly, and associated compliance requirements and protective controls are in place to meet the compliance mandates. For this reason, just delivering an EDR solution is insufficient without integrating with the Identify and Protect functions.

NIST defines three categories to the Detect function.

Anomalies and events

Typically, anomaly detection techniques rely on big data analytics/mining methods involving some form of machine learning (ML) (supervised and unsupervised) and artificial intelligence (AI). Having this level of detection is a primary way to reduce dwell time and significantly reduce the risk of breach. Key things MSPs should consider when planning anomaly and event detection offerings:

- Scale matters. The larger the behavior base, the higher the anomalous behavior detection rate and more likely the detection algorithms will separate anomalous from malicious activity (reducing false positives).

- Pre-exploit and post exploit detection. As discussed above, the NCSF follows the Lockheed Martin Cyber Kill Chain (CKC) which maps out three steps before exploit and three steps after exploit. It is imperative that detection includes pre-exploit and post-exploit detection.[15]

Detect ***An MSP offering should include pre-execution and post-execution detection of anomalous events. This reduces dwell time, reducing risk and potential impact of a breach.***

Security continuous monitoring

Security continuous monitoring is for both externally focused (e.g., malicious inbound activities and external service provider activities) and internally focused (e.g., vulnerabilities and insider threat). Unfortunately, the time it takes to identify and contain a breach is going up as hacking techniques become more sophisticated and stealthy.[16] Addressing this requires advanced threat detection. Key things MSPs should consider when planning security continuous monitoring are:

- Customers demand a single pane of glass, so all threats and vulnerabilities against assets and protective controls must be part of an integrated console.

- Detection services must be environment agnostic, supporting coordinated detection across desktop, virtual server, physical, server, data center, and cloud environments. Being environment agnostic requires both agent and agent-less detection technology.

Detect ***An MSP offering should include continuous process monitoring to monitor endpoints at the process level and detect threats sooner. This must support all endpoint environments including cloud.***

Detection processes

Detection only works when configured correctly and analyzing the right data. Though there is much hype among endpoint security vendors about "set it and forget it." To ensure awareness of anomalous events the detection controls must be updated and checked on a regular basis. This level of checking is also a compliance requirement to update detection and verify vulnerability scanning continually, explicitly mentioned in PCI DSS and other requirements.

Detect ***An MSP offering should include advanced threat detection with a unified dashboard showing all assets with real-time status displaying threat context, suspicious activities, and notifications.***

Respond

The Respond function goes well beyond being just the second half of EDR. As NIST states, Respond is developing and implementing "appropriate activities to take action regarding a detected cybersecurity incident." Much of the Respond function focuses on correctly implementing incident response (IR).

If Identify, Protect, and Detect are implemented correctly, Respond is necessary only when a protective or detective control is unable to prevent an exploit. The stronger the Identify, Protect and Detect solution, the less the need for IR. However, even the most robust security controls and best practices can fa il in the face of an advanced attack vector such as file-less malware, ransomware, zero-day exploits or insider threat. For this reason, MSPs must offer a Respond function that is highly reactive, accurate, fast, and effective.

The reality for most MSP customers is they do not have internal IR teams or even an IR function. Because of this, the endpoint hardening solution must provide built-in IR functionality. At a minimum, this must include:

- Automated Response (e.g., termination, quarantine, and deletion) to mitigate the exploit and minimize the impact)
- Response prioritization by building upon the pre-exploit and post-exploit detection controls to conduct root cause analysis
- Categorization of IoCs in context of assets, threats, and vulnerabilities to streamline and accelerate response

Respond ***An MSP offering should include IR support functions including automated response, response prioritization, IoC categorization and integration with threat hunting to identify the attack vector and to model the threat kill chain, quickly.***

Recover

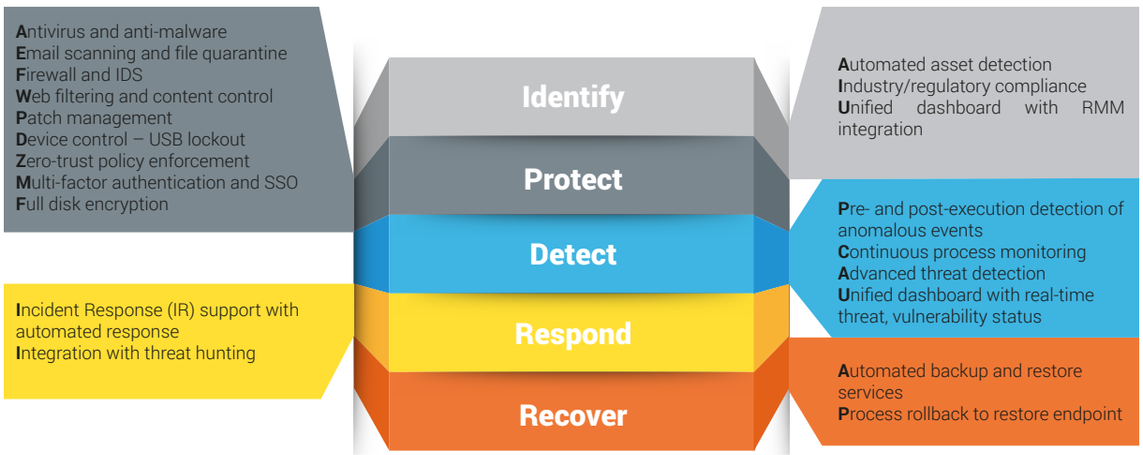
The Recover function is the last layer of the NCSF endpoint hardening model. NIST defines the Recover function as developing and implementing "appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident."[17] As with the previous layers, Recover ties directly to the Respond layer, below. The goal of this function is making sure the organization can recover from a cyber incident.

From an endpoint hardening perspective, controls such as automated backup and restore are necessary to recover the endpoint. Further, there should be more granular recovery capabilities. For example, when a user inadvertently clicks on a malicious link, there should be a restore function (e.g., process rollback) to restore the endpoint to a last known "good state" without having to do a full/incremental system restore.

Recover ***Key MSP offerings should include automated backup and restore services and granular recovery capabilities including process rollback to restore the endpoint to the last known "good state."***

The MSP Endpoint Model

Pulling together the five layers of the NCSF core gives MSPs an endpoint hardening model that is highly secure, practical, layered, logical, and infinitely expandable.



When taken together, building an endpoint hardening solution based on the NCSF gives MSPs the ability to deliver a customizable solution with the following key customer benefits:

- **Seamless Integration reduces cost and complexity.** Following a layered model provides the MSP with the flexibility to integrate endpoint hardening solutions with existing platforms: security information event managers (SIEM), remote monitoring and maintenance (RMM), and professional services automation (PSA) systems. Also, by offering environment agnostic solutions (e.g., cloud, data center, virtual server, physical server, and desktop), the MSP guarantees universal endpoint coverage with minimal impact on employee productivity.

- **Modular approach adds flexibility.** Following the five-layer model gives the MSP the ability to layer in specific technologies and services. For example, adding advanced Protect and Detect solutions to catch polymorphic and file-less malware. Or, adding identity management, patch management, disk encryption, and advanced detection capabilities (e.g., pre- and post- exploit detection) to meet specific compliance requirements.

- **Advanced detection reduces dwell time and cost.** The Detection function underlies all other services. Size matters when it comes to detection and having a global reach database of active threats, vulnerabilities and exploits provides the fuel that advanced AI/ML engines require to quickly discern malicious from anomalous and false positive from false negative. The more accurate the detection, the more effective the response and lower the risk and cost of a breach.

- **Planning for regulatory and industry requirements early to guarantee compliance.** MSP customers are overrun with compliance requirements. The NCSF is explicit that compliance requirements – typically protecting private, financial, and protected health data – be part of the initial Identify discussion. By focusing on compliance early, all follow-on endpoint hardening layers (Protect, Detect, Respond, and Recover) will include the necessary controls and procedures to support the compliance requirements.

Delivering an endpoint hardening solution based on the NCSF empowers MSPs to provide high-value, high-growth multi-tenant services that are scalable, and modular while meeting customer needs for remote monitoring/support. Following the NCSF layered approach offers security that matches MSP customer unique business/industry regulatory requirements with maximum security, minimum impact, and maximum return.

1 Verizon, 2018 Data Breach Investigations Report: 11th Edition. 2018. https://www.verizonenterprise.com/verizon-insights-lab/dbir/
2 National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018, page V.
3 National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, page V.
4 National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, page 3.
5 National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, page 7.
6 Kaseya, Kaseya 2018 MSP Benchmark Survey Results Report, 2018, page 3. https://www.kaseya.com/resource/2018-msp-benchmark-survey/
7 Kaseya, Kaseya 2018 MSP Benchmark Survey Results Report, 2018, page 3.
8 National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, page 7.
9 Verizon, 2018 Data Breach Investigations Report: 11th Edition. 2018.
10 Verizon, 2018 Data Breach Investigations Report: 11th Edition. 2018, page 34.
11 National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, page 36.
12 National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, page 7.
13 Ponemon Institute, 2018 Cost of a Data Breach Study: Global Overview, July, 2018.
14 Ponemon Institute, 2018 Cost of a Data Breach Study: Global Overview, July, 2018, pages 9,26.
15 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
16 Ponemon Institute, 2018 Cost of a Data Breach Study: Global Overview, July, 2018.
17 National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, page 8.

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/.

BD-Business-Oct.18.2018-Tk#: CREAT-3095