How to Optimize Your Cybersecurity Stack With a Preventative Approach

Deploy AppGuard, Your Ultimate Line of Defense

Prepared for a large enterprise (ABC Corp.) by AppGuard Inc.

March 2020

V2, March 2020

703.786.8884
sales@appguard.us
www.appguard.us

Table of Contents

Key Cybersecurity Frameworks & How to Optimize Cybersecurity Stack with a Preventative Approach

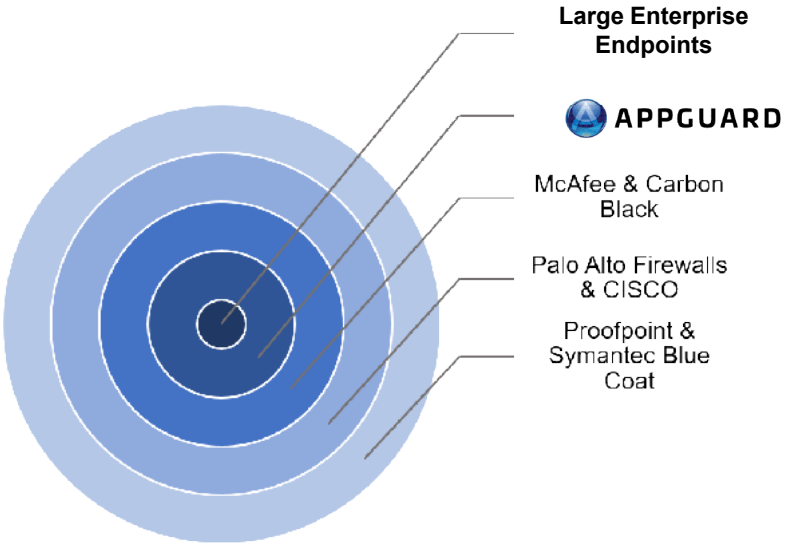
BACKGROUND

ABC Corporation (ABC Corp.), a large enterprise, engaged AppGuard, LLC (AppGuard), to determine if the Enterprise product patented by AppGuard would help strengthen their cybersecurity posture. In this technical deep dive whitepaper, we have outlined how AppGuard Enterprise aligns with the NIST Cybersecurity Framework, Lockheed Martin's Cyber Kill Chain® and the MITRE ATT&CK Framework. As part of the threat assessment, we provided specific recommendations for each element of the cybersecurity stack, and how to optimize their cyber defense while reducing their overall cost.

The information shown in the tables below under the NIST Cybersecurity Framework, Lockheed Martin's Cyber Kill Chain®, and the MITRE ATT&CK Framework sections reflect what each cybersecurity product is capable of addressing in ABC Corp.'s current cybersecurity stack.

However, it is important to note that although a product may address certain activities or phases in the tables below, that does not mean the product is necessarily effective. For example, McAfee Antivirus checks off several boxes in tables 1–4 below, but independent testing confirms it is less effective when compared to other similar products like Microsoft Windows Defender. To fill the security gaps posed by different products, it is critical to deploy a layered defense. Although it may seem repetitive to address certain activities or phases multiple times with various cybersecurity products, these products are implemented at different layers, ultimately creating layers of protection that attackers and threats must defeat in order to complete their objectives of causing harm to ABC Corp., their customers, and their stakeholders. This is commonly known as the "onion" approach in the cybersecurity industry.

The Onion Approach



703.786.8884
sales@appguard.us
www.appguard.us

AppGuard — Your Ultimate Line of Defense

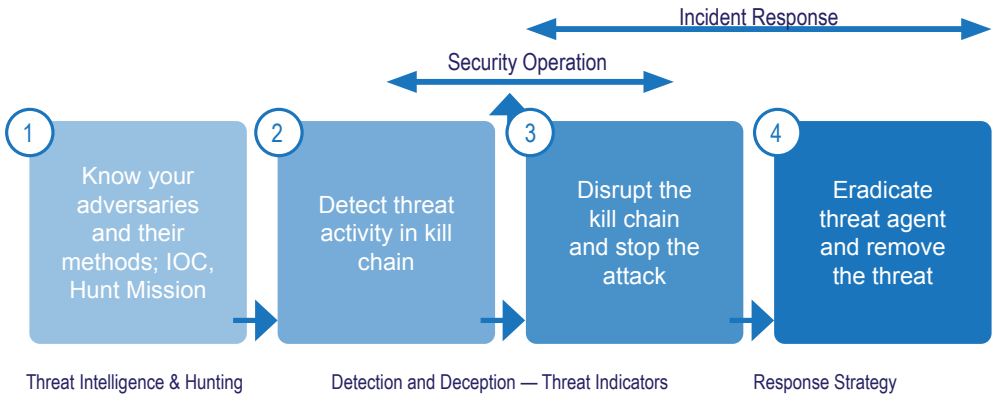
Almost all cybersecurity tools rely on known indicators of compromise (IOC) and pattern matching. However, in a dynamic, ever-changing, and ever-evolving organization, this traditional approach has been shown to fail. This is especially true in large, complex enterprise environments with hundreds of applications that must be routinely updated, with thousands of endpoints that need to be patched regularly, thousands of highly accessible locations across the country, and more; simply put, it is easy for things to slip through the cracks and organizations don't know what they don't know. Attackers continue to evolve their attack vectors and are constantly looking for ways to exploit your enterprise.

In order to most effectively defend an organization in today's threat landscape and for the foreseeable future, a paradigm shift in how cybersecurity professionals secure and defend their organizations and clients is required. AppGuard is uniquely built on the concept of **Zero Trust**, no other cybersecurity product in the market or in ABC Corp.'s cybersecurity stack is built on this concept or offers enterprise level security. AppGuard effectively prevents malware execution, including zero-days and n-days, as opposed to just detecting and responding.

> AppGuard does not trust any unacceptable activity regarding user space or system space and blocks the abnormal activity by default. *However, unlike traditional cybersecurity products, AppGuard only blocks the abnormal activity, not the entire workflow for an end user. This provides tremendous value to large organizations, like ABC Corp., as it allows their employees to continue with normal business operations, undeterred by malware attempting to execute in the background. Because an AppGuard-enabled endpoint does not require constant updating, it will not consume network capacity with daily updates, nor does it consume large amounts of CPU and memory capacity on the endpoint; even while under a malware attack.*

With AppGuard Enterprise's SIEM integration and threat intelligence capabilities, Security Operations Center (SOC) and Security Engineering teams will be alerted of the blocked malware and can take the next steps to determine how to best address it. This is a significantly better security posture for an organization to find themselves in as opposed to having to shift into incident response mode because malware was able to successfully execute on an endpoint.

Threat Management - Our Defense in Cyber Kill Chain



703.786.8884
sales@appguard.us
www.appguard.us

AppGuard: Your Ultimate Line of Defense

NIST Cybersecurity Framework

The NIST Cybersecurity Framework (NIST CSF) is currently used by organizations around the world to assess their cybersecurity posture, abilities, and how they can improve. We evaluated ABC Corp.'s cybersecurity stack against the NIST framework to understand vulnerabilities and provide recommendations to optimize their cyber defense and spend. The cybersecurity community is recognizing the need to adopt a Zero Trust preventative architecture. Industry leaders anticipate "Prevention" will be added to the NIST Cybersecurity Framework in the near future.

SOLUTION	PRODUCT	PURPOSE	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER	PREVENTION
Prevention	APPGUARD	*Prevents malware execution on endpoints — based on Zero Trust, not signatures*	✓	✓	✓			✓
Anti-virus	McAfee / Symantec Endpoint Protection	*Malware detection and removal tool*			✓	✓		
Behavior Detection	Carbon Black.	*Detection of malicious behavior and early containment of threats based on known behaviors & signatures*	✓		✓	✓		
Application Control (whitelisting)	APPGUARD	*Sets policy for IT Application Management and Control*	✓	✓				
Endpoint Detection & Response (EDR)	Carbon Black.	*Detection of malicious behavior and early containment of threats based on known behaviors & signatures*	✓		✓	✓		
Firewalls	Cisco Palo Alto Networks	*Network segmentation and perimeter security. Certificate verification, SDN*		✓				
Sandbox	Symantec + Blue Coat	*Analyze suspicious emails and files*		✓				
IT Log Management	LogRhythm / elastic	*Used as SIEMs to ingest logs and pattern recognition, machine learning*	✓		✓			

Table 1. NIST Cybersecurity Framework.

AppGuard: Your Ultimate Line of Defense

NIST Cybersecurity Framework Functions[1]

Below are the definitions of current functions within the current NIST CSF per NIST.

Identify — Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

The activities in the Identify function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Examples of outcome Categories within this function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

Protect — Develop and implement appropriate safeguards to ensure the delivery of critical services.

The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event.

Examples of outcome Categories within this function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Detect — Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

The Detect function enables timely discovery of cybersecurity events.

Examples of outcome Categories within this function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

Respond — Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

The Respond function supports the ability to contain the impact of a potential cybersecurity incident.

Examples of outcome Categories within this function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

Recover — Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

The Recover Function supports timely recovery to normal operations to reduce the impact of a cybersecurity incident.

Examples of outcome Categories within this function include: Recovery Planning; Improvements; and Communications.

1. — https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

AppGuard: Your Ultimate Line of Defense

Lockheed Martin Cyber Kill Chain®

The Lockheed Martin Cyber Kill Chain® (Cyber Kill Chain®) is used by cybersecurity professionals to understand and take action against the activities that attackers must complete to reach their objectives. The table below outlines the cybersecurity technology solutions and products currently in place at ABC Corp. and at what point within the Cyber Kill Chain® each product comes into play. We evaluated ABC Corp.'s cybersecurity stack against the Lockheed Martin Cyber Kill Chain to understand vulnerabilities and provide recommendations to optimize their cyber defense and spend.

			Outside the Enterprise		Inside the Enterprise				
SOLUTION	**PRODUCT**	**PURPOSE**	**RECONNAISSANCE**	**WEAPONIZATION**	**DELIVERY**	**EXPLOITATION**	**INSTALLATION**	**COMMAND & CONTROL**	**ACTIONS ON OBJECTIVES**
Prevention	APPGUARD	*Prevents malware execution on endpoints — based on Zero Trust, not signatures*			✓	✓	✓	✓	✓
Anti-virus	McAfee / Symantec Endpoint Protection	*Malware detection and removal tool*			✓	✓			
Behavior Detection	Carbon Black.	*Detection of malicious behavior and early containment of threats based on known behaviors & signatures*			✓	✓	✓		
Application Control (whitelisting)	APPGUARD	*Sets policy for IT Application Management and Control*				✓	✓		
Endpoint Detection & Response (EDR)	Carbon Black.	*Detection of malicious behavior and early containment of threats based on known behaviors & signatures*			✓	✓	✓		
Firewalls	Cisco / paloalto NETWORKS	*Network segmentation and perimeter security. Certificate verification, SDN*			✓				
Sandbox	Symantec + BLUE COAT	*Analyze suspicious emails and files*			✓				
IT Log Management	LogRhythm / elastic	*Used as SIEMs to ingest logs and pattern recognition, machine learning*					✓	✓	✓

Table 2. Lockheed Martin Cyber Kill Chain®.

703.786.8884
sales@appguard.us
www.appguard.us

Cyber Kill Chain® Steps[2]

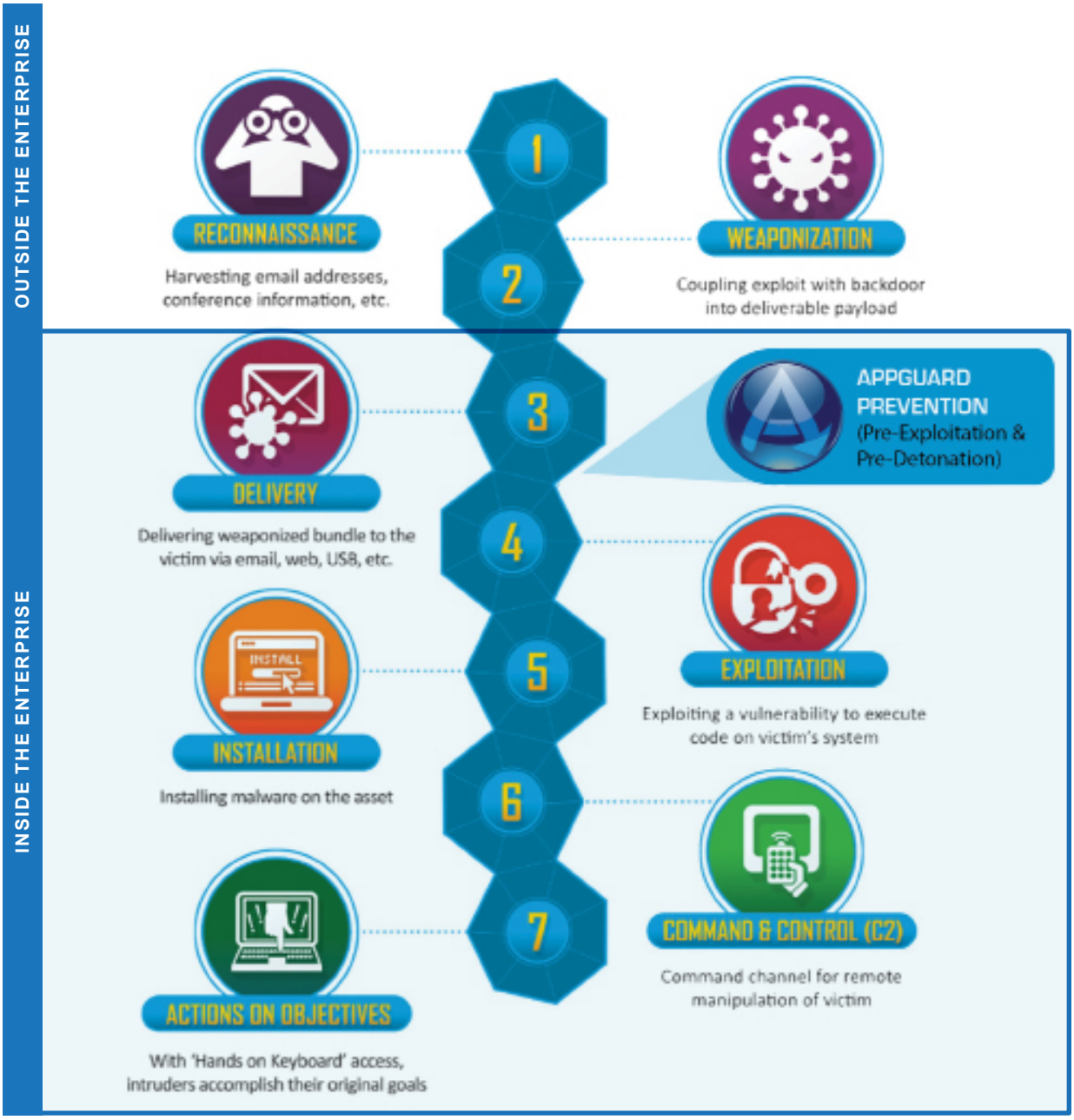


Figure 2. Lockheed Martin Cyber Kill Chain®.

2. Source — https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

MITRE ATT&CK Framework

The MITRE ATT&CK Framework (ATT&CK) is used by cybersecurity professionals and developers to understand the types of attacks used by attackers and, ultimately, to defend their organizations and products best. The table below outlines the cybersecurity technology solutions and products currently in place at ABC Corp. and what phase of the ATT&CK Framework they address. We evaluated ABC Corp.'s cybersecurity stack against the MITRE ATT&CK Framework to understand vulnerabilities and provide recommendations to optimize their cybersecurity defense and spend.

			PRE-ATT&CK		*ATT&CK for Enterprise*				
SOLUTION	**PRODUCT**	**PURPOSE**	**RECONNAISSANCE**	**WEAPONIZATION**	**DELIVERY**	**EXPLOITATION**	**INSTALLATION**	**COMMAND & CONTROL**	**ACTIONS ON OBJECTIVES**
Prevention	APPGUARD	*Prevents malware execution on endpoints — based on Zero Trust, not signatures*			✓	✓	✓	✓	✓
Anti-virus	McAfee / Symantec Endpoint Protection	*Malware detection and removal tool*			✓	✓	✓	✓	✓
Behavior Detection	Carbon Black.	*Detection of malicious behavior and early containment of threats based on known behaviors & signatures*			✓	✓	✓	✓	✓
Application Control (whitelisting)	APPGUARD	*Sets policy for IT Application Management and Control*			✓	✓		✓	
Endpoint Detection & Response (EDR)	Carbon Black.	*Detection of malicious behavior and early containment of threats based on known behaviors & signatures*			✓	✓	✓	✓	✓
Firewalls	Cisco / paloalto NETWORKS	*Network segmentation and perimeter security. Certificate verification, SDN*			✓				
Sandbox	Symantec + BLUE COAT	*Analyze suspicious emails and files*			✓				
IT Log Management	LogRhythm / elastic	*Used as SIEMs to ingest logs and pattern recognition, machine learning*			✓	✓	✓	✓	✓

Table 3. MITRE ATT&CK Framework.

MITRE ATT&CK Framework Image[3]

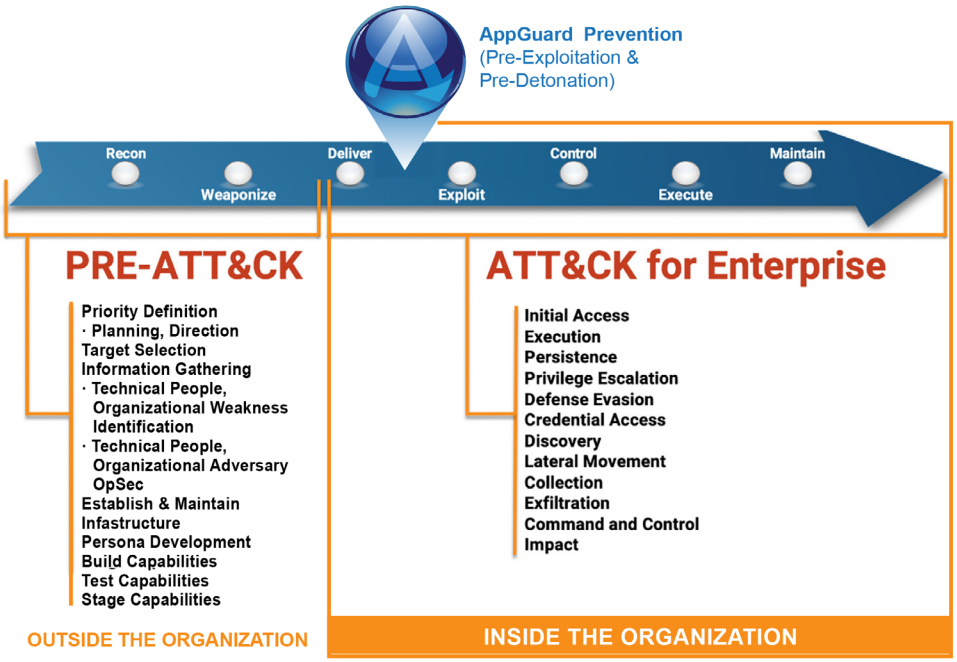


Figure 3. MITRE ATT&CK Framework.

The ATT&CK Framework shown in Figure 3 above highlights that the Pre-ATT&CK activities are separate from the ATT&CK for Enterprise activities, which happens once an attacker actively begins to deliver their attack to the victim enterprise. Essentially, enterprises have little control over Pre-ATT&CK activities other than training, keeping their infrastructure up to date, and practicing good cybersecurity hygiene. This is shown in Table 3 above, as none of the products can stop an attacker from performing reconnaissance or weaponization prior to their attack.

Although several products address the Exploit, Control, and Execute activities (AppGuard, McAfee, Carbon Black), these products handle these activities in different ways. AppGuard profoundly changes the way ABC Corp. complies with the ATT&CK Framework by not only addressing Exploit, Control, and Execute activities, but by being proactive in its approach.

Unlike traditional anti-virus and EDR solutions (McAfee and Carbon Black, respectively, currently in use at ABC Corp.), AppGuard does not rely on known signatures or behaviors. Instead, AppGuard is based on the concept of **Zero Trust**, which does not allow any abnormal actions in user space or system space by default and is currently being tuned by AppGuard's product implementation team with the help of the ABC Corp's IT team.

3. Source — https://attack.mitre.org/resources/enterprise-introduction

ABC Corp. Current Cybersecurity Stack and Recommendations to Optimize

The ABC Corp. a large enterprise with 15 thousand employees across the United States, engaged AppGuard to determine if AppGuard Enterprise would help strengthen their cybersecurity posture. In this section we are providing specific recommendations for each element of the cyber stack and how to optimize their cybersecurity defenses while reducing their overall cost.

SOLUTION	PRODUCT EXAMPLE	PURPOSE	EVALUATION
Prevention	APPGUARD	*Prevents malware execution on endpoints — based on Zero Trust, not behaviors or signatures*	AppGuard is the industry-leading solution for endpoint malware execution prevention. AppGuard is tuned to work with your environment and will block all abnormal activity pertaining to user space and system space. Solution is **proactive** compared to traditional Anti-virus and EDR solutions — based on **Zero Trust** and not behaviors or signatures. AppGuard is the **ultimate line of defense**
Anti-virus	McAfee Symantec Endpoint Protection	*Malware detection and removal*	Currently have eight (8) different agents. Resource intensive, limited effectiveness, and creates excessive alerts. We recommended a better product that is more effective.
Behavior Detection	Carbon Black.	*Detects malicious activities or patterns of known malicious behaviors*	Effective against known indicators of compromise and malware. Not effective against zero-day/new malware, tactics, techniques, and procedures out of the box. Reactive tool, resource intensive, requires extensive tuning and custom watchlist/ signature creation, and built-in admin. Tools don't scale well for large organizations with thousands of endpoints — alerts and logs should be ingested into a SIEM.
Endpoint Detection & Response (EDR)	Carbon Black.	*Detection of malicious behavior, detection and early containment of threats*	Effective against known indicators of compromise and malware. Not effective against zero-day/new malware, tactics, techniques, and procedures out of the box. Reactive tool, resource intensive, requires extensive tuning and custom watchlist/ signature creation, and built-in admin. Tools don't scale well for large organizations with thousands of endpoints — alerts and logs should be ingested into a SIEM.
Firewalls	CISCO paloalto NETWORKS	*Network segmentation and perimeter security. Certificate verification, SDN*	Palo Alto Firewalls generally perform well but require multiple feature and feed subscriptions and extensive configuration and logging tuning. Cisco itself is effective for access control but logs should be ingested into a SIEM for the SOC/Security Engineering teams.

SOLUTION	PRODUCT EXAMPLE	PURPOSE	EVALUATION
Sandbox	Symantec + BLUE COAT	*Analyze suspicious files on virtual environment and detect malware*	Relatively effective against known indicators of compromise and malware. Not effective against zero-day/new malware, tactics, techniques, and procedures.
IT Log Management	LogRhythm elastic	*Used as SIEMs to ingest logs and pattern recognition, machine learning*	Effective tools, but not being effectively managed currently. No insight into user endpoint logs, Cisco ISE logs, etc. Highly recommend ingesting endpoint logs (currently a huge blind spot for ABC Corp.) and consolidating SIEMs to use only Elastic, it scales well and will provide a better value to ABC Corp. due to the cost of LogRhythm, which will increase substantially once endpoint logs are ingested.

Table 4. Current Cybersecurity Stack.

Detailed Listing of Each Technology & Recommendations

Prevention

AppGuard is the industry-leading solution for endpoint malware execution **prevention** and is currently being deployed at ABC Corp.

Unlike most cybersecurity solutions, which are reactive, AppGuard is **proactive** because it is based on the concept of **Zero Trust** and not known behaviors or signatures. Traditional Anti-virus and EDR solutions can only detect and respond to known malicious behavior and malware. AppGuard assumes any abnormal activity pertaining to user space and system space cannot be trusted and therefore blocks it.

RECOMMENDATION: **Install AppGuard Enterprise** (the only commercial **Zero Trust** Pre-ventative Solution in the Market). ABC Corp. wanted a rapid deployment and to move to great-er security without impacting day to day operations. In order to maintain everyday operations AppGuard utilized **Passive Monitoring Mode**. The AppGuard implementation team is already working closely with ABC Corp's IT team to tune AppGuard to tailor its protection to each workgroup. By utilizing the **Passive Monitoring Mode**, ABC Corp. can develop a full and complete asset inventory to identify all endpoints and corresponding applications and web applications per endpoint. This, in turn, highlights all potential threats and ensures application compliance and conformity. In **Passive Monitoring Mode**, AppGuard does not actively block application activity but scans to identify existing applications and web applications on each endpoint within the enterprise. Security policies are fully enabled to provide full protection while not interrupting the users' day to day activity.

During this process, we also recommend that AppGuard's logs be shipped to a Security Incident and Event Management (SIEM) platform — this, coupled with AppGuard's threat intelligence capabilities, will provide ABC Corp. with the information their security teams need to further harden their systems. In order for malware to have been blocked by AppGuard and not another tool, the other layers of the cybersecurity stack will have to be bypassed first — see Figure 1 above, which shows that AppGuard Enterprise sits at a layer between McAfee/Carbon Black and ABC Corp. endpoints. This will help ABC Corp. to determine strengths and weaknesses in the other cybersecurity products they have and further configure and tune them.

Anti-virus

The endpoints are protected with McAfee Anti-virus, which provides little in the way of detection and prevention of malware. If malware has a signature that McAfee has in its definitions, it will get quarantined. Custom malware will likely escape detection and execute without issue.

RECOMMENDATION: We recommend that ABC Corp. switch from McAfee Anti-virus to another vendor that offers better protection. We highly recommend using independent testing results to determine which product they should pick to replace McAfee. Once deployed, we highly recommend feeding logs into a SIEM for the SOC and Security Engineering teams to have full visibility.

Behavior Detection

Carbon Black is deployed on ABC Corp. endpoints, and AppGuard notes that this tool can be used effectively to *detect* compromises if used properly. However, Carbon Black can only detect what it knows and is therefore unlikely to detect an advanced attacker or zero-day malware. It is important to note that **detection is not prevention**; Carbon Black can detect malicious behavior, but it does not block it. Carbon Black offers separately licensed protection features. Carbon Black Defense and Carbon Black Protect — currently, ABC Corp. only has Carbon Black Response. If added, both would increase endpoint agent load, potentially exacerbating existing issues in the current Carbon Black Response platform, including alert fatigue, and could potentially block legitimate application activity if not carefully tuned over time.

There are also challenges with using Carbon Black in an environment of ABC Corp's size. AppGuard noted that there are over 2 million alerts not currently being triaged in the Carbon Black console.

Ideally, alerts would be forwarded and triaged in a managed Security Incident and Event Management (SIEM) platform like Elastic or LogRhythm.

RECOMMENDATION: In similar-sized organizations, AppGuard successfully deployed and used a different endpoint tool that monitors and logs system activity, to detect and respond to indicators of compromise. The data from this tool can be sent to a SIEM for the SOC and Security Engineering teams to monitor and act upon. By switching to AppGuard's recommended tool, ABC Corp. can provide the same level of insight they currently have while reducing costs. Both Carbon Black and our recommended tool are respectable products and will meet ABC Corp's needs. The biggest advantage of going with the latter is cost. However, the area of greatest improvement here would be shipping the logs to a SIEM and training the SOC and Securing Engineering teams to properly triage, investigate, escalate, and/or close out the alerts.

Application Control (Whitelisting)

Before the AppGuard Enterprise deployment, there was not any application control (whitelisting solution) being used in production at ABC Corp. A whitelisting solution typically relies on comprehensive lists of allowed files and not allowed files. These systems require a lot of maintenance to ensure legitimate business applications can execute. For example, updates and changes in existing software frequently break application whitelisting policies and may interfere with legitimate applications operations.

The patented Application Control feature within the AppGuard product provides a greater deal of protection and control than a standard whitelisting solution. Failed conformance controls such as whitelisting, HIPS, and sandboxing require too much endpoint-state information that has to be revised after application updates and patches, or similar changes. AppGuard's **Zero Trust** Application Control is based on higher abstractions that simplify policy formulation and automatically adapt to lifecycle changes. For example, application control/containment begins with its parent executable and automatically extends to any resulting process from the application's operation. This not only means very little state information is required for policy formulation, but it also means updates/patches do not necessitate policy updates. Further, application hijacking due to vulnerability exploits, weaponized documents, SQL injections, etc. illustrate that whitelist launch control is not enough. In addition to controlling what applications user groups have access to, AppGuard controls and contains what applications may or may not do after the launch. So, as Microsoft Word's "parent" executable may not alter core operating system components, for example, AppGuard's "higher abstraction" ensures the same applies to all of Microsoft Word's "children" processes and other applications the parent might launch. This adaptiveness simplifies administration and also accounts for the unanticipated – **Prevention through Zero Trus**t.

RECOMMENDATION: Although there are many application whitelisting tools on the market, the biggest advantage of using AppGuard Enterprise is simplifying workflow and products for the ABC Corp. IT and cybersecurity teams. Most Application Control solutions are both difficult to deploy and will confer minimal Protection ability. AppGuard's solution based upon a **Zero Trust** architecture has capabilities to identify binaries resident on the endpoints it protects for IT Asset Management (Identify), as well as provide threat intelligence feeds to your SIEM solutions (Detect and Respond). No other whitelisting software currently in the market can directly protect endpoints.

Endpoint Detection and Response (EDR)

Carbon Black is the current EDR tool at ABC Corp., and as noted previously, this tool can be effective when used properly in detecting and responding to compromises. However, EDR tools, by definition, are for detection and response, they do not prevent unknown malicious activities or unknown/zero-day malware from executing.

RECOMMENDATION: As mentioned above in the Behavior Detection section, AppGuard recommends that ABC Corp. consider another vendor as an alternative to Carbon Black. Although Carbon Black is a good EDR solution, its current setup at ABC Corp. is not optimal, and the Carbon Black console is not ideal for a large organization. Whether ABC Corp. decides to stay with Carbon Black or switch, we highly recommend configuring the tools properly to reduce alert fatigue and to send endpoint data into a SIEM for the SOC and Security Engineering teams to monitor and analyze.

Firewalls

Palo Alto firewalls are currently being used at ABC Corp. During the Configuration Review phase of the Threat Assessment, AppGuard determined that the firewalls are largely configured to industry standards with a few best practice exceptions that are noted in the report.

However, the existing firewalls, sandboxes, and proxies did not block the download of the malicious executable from our web server during the spear phishing phase, nor did it block the outbound traffic back to our command and control server.

RECOMMENDATION: AppGuard recommends further tuning and testing of the existing firewalls as it may be possible to configure these devices to block download of malicious executables. This can be achieved through testing various configurations, based on industry best practices and ABC Corp.'s environment, either internally using ABC Corp's Security Engineering and IT teams or in partnership with outside cybersecurity consulting firm.

Sandbox

Proofpoint and Symantec Blue Coat each have built-in sandboxes to detonate potentially malicious emails and files, respectively.

However, neither of these systems blocked the malicious document used in the spear phishing phase. Additionally, other sandbox technologies may have better capabilities in dynamic analysis. For example, some commercially available appliances have been able to detect malicious document payloads.

RECOMMENDATION: We recommend exploring other sandboxing options.

IT Log Management

LogRhythm is currently being used as a SIEM for the enterprise, with the exception of the Amazon Web Services (AWS) setup, which uses Elastic. Both LogRhythm and Elastic are reasonable options for a SIEM solution. However, given ABC Corp's size and needs, AppGuard recommends replacing LogRhythm with Elastic and moving forward with a single SIEM that gives the SOC/Security Engineering teams the clarity, transparency, and resources they need to perform their duties effectively.

During the Threat Hunting phase of the Threat Assessment, AppGuard found that LogRhythm and Elastic are both being used with limited success because they are not configured and utilized per ABC Corp's needs. For example, user endpoint logs are not being ingested into LogRhythm, which means the SOC/Security Engineering teams have very little insight into what is happening on the tens of thousands of endpoints.

Many organizations of ABC Corp's size are turning to Elastic for a SIEM solution and for Threat Hunting. Other options, such as LogRhythm and Splunk, are viable options but can potentially be extremely expensive as their pricing structure is based upon the amount of data ingested. If ABC Corp. were to begin ingesting data from all of their endpoints, as recommended, it is very likely the cost of LogRhythm will increase significantly.

RECOMMENDATION: Due to the potential high cost and time it will take to configure and setup their existing solution to meet business needs, we recommend resources be put into deploying another solution as a SIEM across the entire enterprise. In our experience users prefer our recommended solution over ABC Corp.'s existing solution, once trained on how to use it.

AppGuard reached out to QRadar as a courtesy and depending on log storage needs (should comply with NYDFS, as that has been a goal of the Information Security department — some logs must be kept for up to five years) and due to the size of ABC Corp., the cost of QRadar will likely be between $500,000 and $1,000,000 per year. This is substantially more than what similar-sized organizations typically pay for Elastic — Elastic is open-source, and the bulk of the cost would be for the servers,storage, and support. In addition to the cost of the equipment needed for Elastic (additional equipment would also have to be purchased for QRadar to ingest and store all necessary logs), we highly recommend ABC Corp. purchase Elastic's Enterprise on-prem subscription — we are actively working with Elastic to return a price estimate for ABC Corp. The primary benefits of paying for Elastic's Enterprise on-prem subscription versus just using the open-source version includes support from Elastic, machine learning, the official SIEM application, and more.

Summary

ABC Corp. has many robust cybersecurity products in its cybersecurity stack. The information regarding the NIST Cybersecurity Framework, Lockheed Martin's Cyber Kill Chain®, and the MITRE ATT&CK Framework show what activities/phases each of the current cybersecurity products at ABC Corp. address. Once again, it is important to emphasize that just because a cybersecurity product may address certain activities/phases, it does not mean the product is effective. AppGuard made recommendations for ABC Corp. to optimize its cybersecurity practices for the better without compromising on quality, effectiveness, and efficiency while keeping ABC Corp.'s cybersecurity budgetary requirements in mind. Additionally, the need for a layered approach to cybersecurity is of utmost importance for any organization, but especially for one as large and complex as ABC Corp. The more layers an attacker or threat has to bypass, the more difficult it will be for them to orchestrate a successful attack. By implementing the remediation and mitigation recommendations in the separate Threat Assessment reports, and making the necessary changes to the cybersecurity stack, ABC Corp. will position itself to cost-effectively defend and protect against modern, constantly evolving cybersecurity threats.

APPGUARD

A Blue Planet-works Company

How AppGuard Can Help

About AppGuard

AppGuard is a PREVENTION solution, applying a zero-trust approach within the workstations and servers it protects, in real time. AppGuard takes away all applications' ability to harm the operating system.

Protecting Applications with Enforce, Block and Adapt

AppGuard's policy-based, zero-trust solution mitigates application misuse and hijacking risks by:

- Enforcing policies, so applications do only what they are supposed to do
- Blocking actions that do not conform to policies
- Adapting in real time to application updates, patches, and other changes to avoid administrative burdens and mitigate unanticipated attack vectors.

To learn more about AppGuard, visit *www.appguard.us*

VA Office

14170 Newbrook Drive Suite LL-01
Chantilly, VA 20151
USA

LA Office

530 Wilshire Boulevard
Suite 206
Santa Monica, CA 90401
USA

NY Office

333 Seventh Avenue
10th Floor
New York, NY 10001
USA

Tokyo Office

(Blue Planet-works, Inc.)
Daiwa Jingumae Bldg.,
3Fl2-4-11 Jingumae
Shibuya-Ku Tokyo,
150 - 0002
Japan