VERDASYS®

CYBER ATTACK DEFENSE

A KILL CHAIN STRATEGY

WHITE PAPER

Executive Summary

Companies of all sizes and across all industries are faced with the increasing problem of defending against cyber attacks. Malicious cyber attackers continue to develop cutting-edge malware that can not only threaten to interrupt your day-to-day business but, more importantly, can steal your most proprietary and confidential intellectual property. These cyber thieves continually design malware that will infiltrate your system and lay dormant until they can access the data they are looking for and exfiltrate it from the network. These thieves are looking for any way possible to get into your network to get at this data, including targeting your supply chains and partners. Their goal is to find the weak link in the defense chain.

There are different types of cyber attacks, each one having a different goal, ranging from disrupting service to destroying technology to stealing sensitive data. Our primary focus at Verdasys is on the cyber attacks that steal sensitive data, commonly known as Advanced Persistent Threat (APT). APT instances must complete a common series of steps in order to complete an attack. These steps are: Planning, Malware Introduction, Command and Control, Malware Expansion, Target Identification, Attack Event (Exfiltration) and Retreat or Removal. As organizations struggle to deal with this new and growing threat, they are faced with multiple issues to overcome:

- Attacks are very sophisticated and often significantly different from previously used malware, making them difficult to detect and defend against.
- The number of malware kits available continues to grow offering cyber attackers even more threat vectors to exploit.
- Attackers have become very patient, creating malware that will infect your network and then lay dormant for weeks or months until a weak point is defined and penetrated.
- Attacks are persistent, meaning they re-attack a second, third, fourth or even fifth time in an effort to find the weak point to break into your organization.
- Companies are challenged to protect their data in a mobile world where laptops, tablets and smartphones are commonly used off the network.
- Companies must protect data through its entire business and supply chain, including outside contractors, vendors and partners.
- Companies must protect their own employees from malicious human targeted attacks such as spear phishing, whaling and water hole attacks, educating employees on how to identify these threats and defend against them.

It's clear that even the best security teams are challenged when it comes to detecting and defending against cyber attacks in their many forms.

The "Kill Chain" is a traditional warfare term defining the command and control process for targeting and destroying enemy forces in such a way as to make it most difficult for the enemy to continue in the battle. However, Lockheed Martin and other leading cyber defense companies have started to use "Kill Chain Defense" to define a new defensive strategy for guarding against APTs and other unconventional cyber threats. The two critical ideas behind the successful execution of Kill Chain Defense are to:

1. Accept the fact that cyber defenses only focused on a single stage in a cyber attack will fail or be circumvented
2. A Kill Chain Defense exploits an inherent weakness in the cyber attack model, namely that the cyber attack must complete all steps in the attack to success. Failure to do so, even breaking one link in the chain, will result in disruption of the attack.

The goal of a Kill Chain Defense is to collect and correlate attack intelligence and challenge the malware's adaptability and stealth in ways it was not designed to circumvent. This is accomplished by gathering and correlating data from all possible stages of a cyber attack and deploying effective defensive controls to the stages where the attack is most vulnerable. This model can be broken down into 4 defensive capacities:

Prevention: Deploy multiple blocking controls targeting the "malware introduction" stage to attempt and stop the initial infection

Detection: Find and alert security teams to malware attacks either in the introduction stage or if the malware has penetrated initial defensive system, detect malware at the command and control, expansion, target identification or exfiltration stages.

Containment: Deploy blocking controls that prevent the malware from spreading in the expansion of command and control stages if an initial infection could not be blocked. Controls focus on blocking bad applications or unknown or suspect cross-network and off-network communications, isolating machines from the network and alerting machine owners to risks and actions to take in real time. This can also include preventing unknown binaries from accessing critical corporate data.

Investigate: Investigation focuses on collecting intelligence on the attack itself in order to determine details of its methodology and its actions. Information collected from this stage (including capturing the initial infection "dropper" files) is used to improve all other defensive postures so that the cyber threat defense process is constantly improving and preparing for the next generation of attack.

To deploy a Kill Chain Defense strategy, companies must have the ability to detect and defend across all stages of a cyber attack. Technologies to help do this include network defenses like next-gen firewalls, intrusion detection systems, malware detection engines, network and endpoint cyber attack detection and prevention technologies, application whitelisting and memory scanning capabilities.

Integration between these products must exist but in a way that does not compromise the integrity of the Kill Chain strategy. SIEM tools offer value in the correlation process with no risk of system degradation but lack the policy controls to execute the next stage of the Kill Chain strategy, often resulting in "after the fact" forensic investigations. To the contrary, integrated autonomous layers of defense offered by advanced cyber defense products can be even more effective.

Another military term that can be effectively transferred to cyber threat defense is "force multiplier." In military terms this is a capability that, when added to a combat force, significantly increases the combat potential of that force and thus enhances the probability of successful mission accomplishment. In the cyber attack world, that force multiplier is an integrated platform that can detect, correlate and create actionable intelligence and then quickly and effectively act on that intelligence with prevention and containment controls.

Most of the existing cyber defense products are point solutions that work at one or possibly two stages of the attack process. In their existing state they do not support a Kill Chain Defense. Worse still, a vast majority focus on the same stage of a cyber attack - the malware introduction stage, which is the most difficult to defend, and is where the enemy has its own force multiplier in multiple flavors of attackers (hackers, hacktivists, cyber criminals), malware kits and exploits to choose from. Many companies are turning to SIEM to deliver data feeds from these point solutions to at least enable some level of timely correlation, but SIEM cannot deliver defensive controls once actionable intelligence is gleaned.

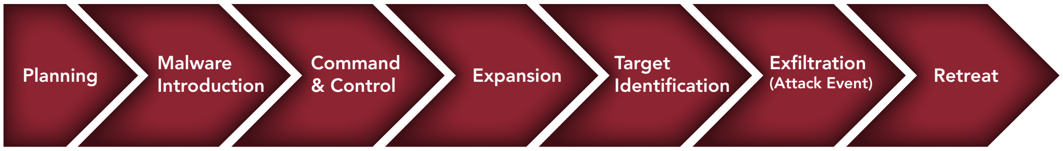
Digital Guardian® is a data-centric technology platform for Enterprise Information Protection (EIP) that integrates endpoint, server and network agents into a coordinated and multi-layered sentry to detect and stop advanced malware designed to steal a particular company's sensitive data. Digital Guardian is the only platform-based solution that utilizes a Kill Chain Defense integrating the four critical capacities of cyber threat defense: prevention, detection, containment and investigation. Digital Guardian capabilities do not focus solely on a single stage in a cyber attack but instead offer visibility and the ability to deploy defensive controls across all stages of an attack. It does this independent of infrastructure and includes the critical protection of laptops and other mobile devices when they are off the network. Digital Guardian provides a comprehensive and integrated Kill Chain Defense against cyber attacks that correlates suspicious activities across endpoints and networks delivering alerts to provide an enterprise-wide overview of threatening activity. Digital Guardian then enforces autonomous prevention and containment controls at different stages of an attack inside or outside the network thwarting any attempt to remove sensitive data.

Introduction

DEFINING CYBER ATTACKS

The rate and sophistication of malicious software ("malware") attacks continues to outpace the capacity for companies large and small to defend against them. Nowadays, the most dangerous and effective malware is most often purpose-built, target-specific malware that combines stealth, precision and social engineering to both penetrate an organization's perimeter and compromise systems without detection for long periods of time. These cutting-edge cyber attacks (sometimes called Advanced Persistent Threat or APT) describe a class of malware designed to carry out stealth missions to steal proprietary data on specific corporate and classified networks. Targeted cyber attacks occur across every industry wherever highly competitive and proprietary information is used, from manufacturing, high tech, oil & gas, financial, pharmaceutical, critical infrastructure and public utilities and, of course, military and government organizations. These attacks not only target large enterprises but they also target the supply chains and partners of these enterprises, regardless of size and location, in an effort to find a weak link in defense systems from which to begin the attack process.

Figure 1: Stages of a Cyber Attack



ANATOMY OF A CYBER ATTACK

Cyber attacks come in many forms with the goals of the attack varying from disrupting operations to destruction of technology assets to stealing sensitive data. In the case of Verdasys, we focus on the type of attack where sensitive data is being targeted, commonly called APT. Interestingly, most attacks follow a common series of steps to complete an attack.

1. **Planning** – After a target (organization) is identified, the attack planning occurs. Planning includes how the malware will be introduced, the communications methods and locations used while the attack is in progress and how the data will be extracted and to where. In all cases, multiple paths are defined. Much of this planning is spent on social media sites and the company's website. Understanding organizational structures to determine high value employees, connecting to those employees social media pages to collect demographic and historic data, finding home email or webmail addresses and collecting data about families and friends including birthdays, names and addresses and schools attended are added to profiles. Profile intelligence collected from these activities includes likely passwords or lost password answers, whether home machines or networks are easier to compromise and what the target's likely access would be based on their title, role or relationships all in order to determine weak points for human targeted attacks

2. **Malware Introduction** – A large amount of malware is introduced through human attacks like spear phishing. These attacks are personalized based on the success of the planning stage. Emails with embedded malware or links to infecting URLs are common but many other types of introduction methods may be used, including software and network vulnerability exploits. Human attacks are one of the most successful attack methods because even today, most people do not understand the risk of opening suspect emails or files or clicking on links and most companies do very little in the form of educating their employees in an effective way. Other forms of attack include; pretexting, spoofing and session hijacking.

3. **Command and Control** – In most malware attacks the malware at one point (or often more than one point) has to call out to the attackers to send discovered information and to receive additional instructions. Examples include malware that has installed itself on one or more machines and infiltrated the corporate directories and network. It will send user, network and machine information back and receive new instructions on what identities or machines to infect next, how to identify the target and instructions on how to exfiltrate the data.

4. **Malware Expansion or Lateral Movement** – The malware will need to move laterally to multiple machines in order to find and access the target data, move the target data to an exfiltration point and then exfiltrate the data off the network.

5. **Target identification** – For our purposes this step includes the malware finding the machine where the target data is located and gaining access to that data.

6. **Attack Event (Exfiltration**) – For an APT or data-focused attack, this step usually consists of two parts. Part one is the copying, obfuscating and moving the target data to the exfiltration point. The malware may store the stolen data in temporary password-protected RAR, ZIP or CAB compressed folders or files which go unnoticed. Part two is the exfiltration process itself where malware exploits many different weaknesses to move data off the network. These include remote access applications or FTP sites, email through a malicious SMTP server directly on the compromised system and DNS (domain name server) extraction, which is also common and very difficult to track. Regardless of what event is used, the Attack Event stage in an APT attack can take weeks and months with the malware making multiple attempts to move and extract data, all while remaining stealthy to infrastructure focused security systems.

7. **Retreat or Removal** – After a data compromise is complete, the malware will often retreat and hide within a computer network or destroy itself depending on the target organization and likelihood of discovery by security systems. In high value organizations the attackers prefer to leave malware in the environment to open new back doors or be utilized in later exploits.

The Challenges of Defending Against Cyber Threats

All organizations are struggling to deal with this relatively new and growing threat. The problem is that there are multiple issues to overcome. The attacks themselves are very sophisticated. Over 1/3 of initial malware introductions is a new or a significantly different variant on a previous attack making detection and prevention very difficult. The number and growth of malware kits available to attackers continues to propagate. The attackers are patient with attacks taking months and with portions of malware hiding silently in your environment for even longer. Attacks are persistent, meaning they probe defenses and try a second, third, fourth and fifth time to infect your organization, while constantly looking for weak points.

Common weak points include mobile devices and laptops that connect to the Internet when not on the corporate network. Network systems cannot protect laptops and other machines and devices when they are offline. Whether is it an employee's company laptop, a BYOD machine or the computer of your consultant, contractor or partner, when these systems connect to the Internet and do not have the protection of your network defensive systems they are quickly and easily infected. Then, when the system connects to your network the infection expands and the attack begins. Attacks are also increasing along your business supply and value chains. If your data is in multiple locations in your company, some of which may not have the same level of defense, or it has to be utilized by a partner for some step in the business process and that partner has weak security – the attackers will find and attack those points.

Another reason organizations are struggling to defend against attacks is that existing security products, both older and newer, are incomplete. Antivirus and other signature-based technologies are blind to the 1/3 or more malware kits that have never been seen before. Many of the new products available on the market have an autopsy focus and can only tell you how bad the attack has been and what machines need to be wiped. Most of the next generation technologies advertised in the market focus on the initial infection stage of the cyber attack, yet studies have shown that even with these tools in place there are significant gaps in the malware infection stage of the attack and some of the time malware does get through (http://www.pcworld.com/article/224932/nss_labs_finds_most_firewalls_vulnerable_to_attack.html). When you bring the "persistent" nature of these attacks into play – it means that your organization will be compromised if the defensive focus is on a single layer of your perimeter or network.

The challenge is not limited to inadequate technology. The favorite infection vector of the attacker is your employee and their work computer. Spear phishing, whaling and waterhole attacks fool unwitting employees into infecting their machines as the initial point of an attack. If employees are made aware of threats and how to recognize them, they offer an additional and very valuable line of defense. Yet security teams in many companies are notoriously bad at communication with and educating employees effectively.

Add up all of these variables and it quickly becomes apparent that even the best security teams cannot keep up with this constantly changing and continuously growing threat. Security teams must understand the methods and models of emerging attacks, must manage and utilize the many technologies and point products used in cyber defense to correlate information and determine if an attack is real and what it is attempting to or has stolen. Then they must figure out how to put upgraded or additional defenses in place to try and prevent the next attack. The workload can be daunting. The real straw that breaks the camel's back is the fact that any one of these technologies in and of themselves and focused on defending against one or two stages of an attack will fail.

How to Defend Against Cyber Threats

The "Kill Chain" is a traditional warfare term often used by the US Air Force in defining the command and control process for targeting and destroying enemy forces in such a way as to make it most difficult for the enemy to continue in the battle. A common execution of the strategy was in the initial air attacks on Iraq in Operation Desert Storm. However there is another use for this term: describe what experts believe is the most effective defense against cyber attacks. The US Military and leading cyber threat defense teams at Mitre and Lockheed Martin are using "Kill Chain Defense" to define a new defensive strategy for guarding against APT and other unconventional cyber attacks.

There are two critical ideas behind the Kill Chain Defense. One is that an organization must accept that fact that cyber defenses at any given stage in a cyber attack will fail. This has been proven by independent testing and it must be accepted before an effective cyber defense model can be put in place. The second critical idea is that the Kill Chain Defense exploits a critical weakness in the cyber attack model, namely that for the attack to be a success all steps must be completed and the target data exfiltrated from the organization while a successful defense needs only break one link in the chain to stop an attack or re-attack. Looked at in this way, the overwhelming defensive problem becomes manageable and the ability to successfully stop an attack before it is complete becomes reasonable.

Building a Kill Chain Defense

The goal of a Kill Chain Defense is to collect and correlate attack intelligence, identify anomalies that signal malware and challenge the malware's adaptability and stealth in ways it was not designed to circumvent. This is accomplished by gathering and correlating data from all possible stages of a cyber attack and deploying effective defensive controls to the stages where the attack is most vulnerable. This model can be broken down into 4 defensive capacities: prevention, detection, containment and investigation.

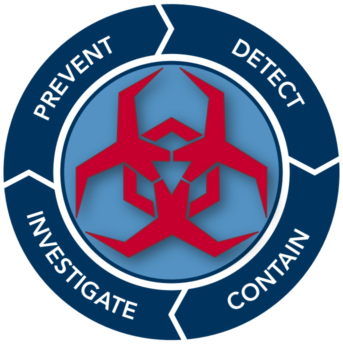


Figure 2: Kill Chain Defense

Prevention: Deploy multiple blocking controls targeting the "malware introduction" stage to attempt and stop the initial infection

Detection: Find and alert security teams to malware attacks either in the introduction stage or if the malware has penetrated initial defensive system, detect malware at the command and control, expansion, target identification or exfiltration stages.

Containment: Deploy blocking controls that prevent the malware from spreading in the expansion of command and control stages if an initial infection could not be blocked. Controls focus on blocking bad applications or unknown or suspect cross-network and off-network communications, isolating machines from the network and alerting machine owners to risks and actions to take in real time.

Investigate: Investigation focuses on collecting intelligence on the attack itself in order to determine details of its methodology and its actions. Information collected from this stage is used to improve all other defensive postures so that the cyber threat defense process is constantly improving and preparing for the next generation of attack.

As mentioned, an important assumption in the Kill Chain Defense is that an attack will defeat one or more individual technology layers and succeed in infecting one or more systems. This does not mean you disregard the defensive of any particular layer even if the technologies available are nascent. The Kill Chain Defense relies on the ability to detect and defend across all stages of a cyber attack and all layers of a network system. This includes network defenses like next-gen firewalls, intrusion detection systems, malware detection engines, network and endpoint detection capabilities, application whitelisting and memory scanning detection capabilities.

There is a Catch 22 here — these defenses need to be autonomous, meaning that if one system becomes infected and compromised it will not degrade the ability of the other systems to operate effectively. At the same time the detection intelligence collected needs to be easily correlated so that attacks are quickly and accurately defined. Integration between products must exist but in a way that does not compromise the integrity of the Kill Chain strategy. SIEM tools offer value in the correlation process with no risk of system degradation but lack the policy controls to execute the next stage of the Kill Chain strategy, while integrated autonomous layers of defense offered by advanced cyber defense products can be even more effective.

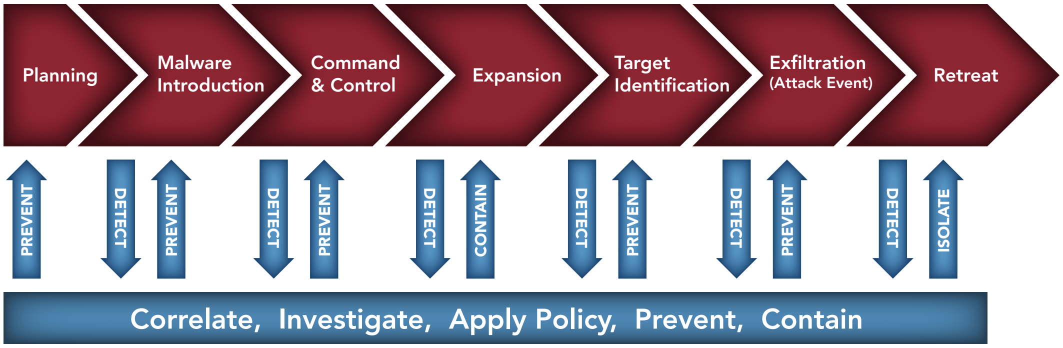


Figure 3: An Integrated Platform Offers Security Teams a Power Force Multiplier in the Fight Against Cyber Attack

Platform — The Force Multiplier

Another military term that can be effectively transferred to cyber threat defense is “force multiplier.” In military terms this is a capability that, when added to a combat force, significantly increases the combat effectiveness of that force and thus enhances the probability of successful mission accomplishment. An example is the addition of a C3 aircraft to a ground operating unit. This C3 aircraft (command, control and communications) is an advanced sensor platform that gathers all of the battlefield intelligence in the ground units area of operations, correlates it and sends it back down to the ground force commander as actionable intelligence (think infrared video of enemy formations that are out of view of the ground force but moving toward them — then think of the air to ground ordnance called in by the ground commander that neutralizes the enemy before it can cause any damage).

In the cyber attack world, that force multiplier is an integrated platform that can detect, correlate and create actionable intelligence and then quickly and effectively act on that intelligence with prevention and containment controls. The platform becomes your C3 aircraft — the force multiplier.

Most of the existing cyber defense products are point solutions that work at one or possibly two stages of the attack process. In their existing state they do not support a Kill Chain Defense. Worse still, a vast majority focus on the same cyber attack stage, malware introduction, which is the most difficult stage to defend against. This is where the enemy has its own force multiplier in trained attackers (hackers, hacktivists and cyber criminals), malware kits and exploits that can be purchased from multiple global sources. Many companies are turning to SIEM as a partial force multiplier, collecting data feeds from point solutions to at least enable some level of timely correlation, but SIEM cannot deliver defensive controls once actionable intelligence is gleamed.

Verdasys Digital Guardian Cyber Defense

Digital Guardian® is a data-centric technology platform for Enterprise Information Protection (EIP) that integrates endpoint, server and network agents into a coordinated and multi-layered sentry to detect and stop advanced malware designed to steal sensitive data. The Digital Guardian Platform provides multi-layered kill chain defense for targeted cyber attack prevention, detection, containment and investigation. Capabilities include:

- Deep system-level event visibility correlation and policy-based automated rules for malware prevention, detection, containment and investigation at the endpoint for host systems on and off the network.
- Signature-less malware detection and behavioral analysis for advanced investigation of code in physical memory on the endpoint.
- Network visibility and detection of threats including deep session level inspection of all traffic inbound and outbound across all ports, malware threat analysts in near real-time and correlation against threat intelligence feeds offering prevent, detect, contain and investigate capabilities.
- Ability to interact with the end users in a direct and timely manner to elicit defense assistance, decrease response times and provide on-the-spot cyber security training opportunities (e.g spear phishing identification training)

Digital Guardian is the only platform-based solution that utilizes a Kill Chain Defense when preventing, detecting, containing and investigating a cyber attack. Digital Guardian capabilities do not focus solely on any single stage of a cyber attack but instead offer visibility and the ability to deploy defensive controls across all stages of an attack. Digital Guardian applies defensive capabilities across multiple stages of cyber attacks independent of infrastructure, including protecting laptops that are off the network offering.

Digital Guardian also acts as a force multiplier internally and externally with other cyber defense products. Digital Guardian's extensive system coverage offers visibility across Windows, Linux and MAC host systems, memory DNA in Windows systems, Virtual environments and all ports across the network. The threat intelligence collected from all of these sensors is analyzed in a powerful threat correlation bus and containment/prevention control policy engine. The result is the timely and accurate creation of actionable intelligence and automated, policy-based prevention and containment rules. Digital Guardian as a force multiplier does not stop there – Digital Guardian can both absorb data intelligence feeds from third party sources or other cyber threat defense products as well as output threat intelligence to SIEM products. Acting as an integration platform, Digital Guardian enhances all parts of a cyber defense program. Combining Kill Chain Defense capabilities and force multiplier integration results in:

- Increased positive detection rates for cyber attacks
- Decreased incident response time to detect and react to threats
- Greater ability to accurately identify infected machines and immediately deploy containment controls to isolate the malware
- Quick forensic investigation to determine malware behavior, elimination steps and improved prevention rules
- Prevention of the malware from compromising sensitive data by quickly and effectively through data exfiltration blocking controls

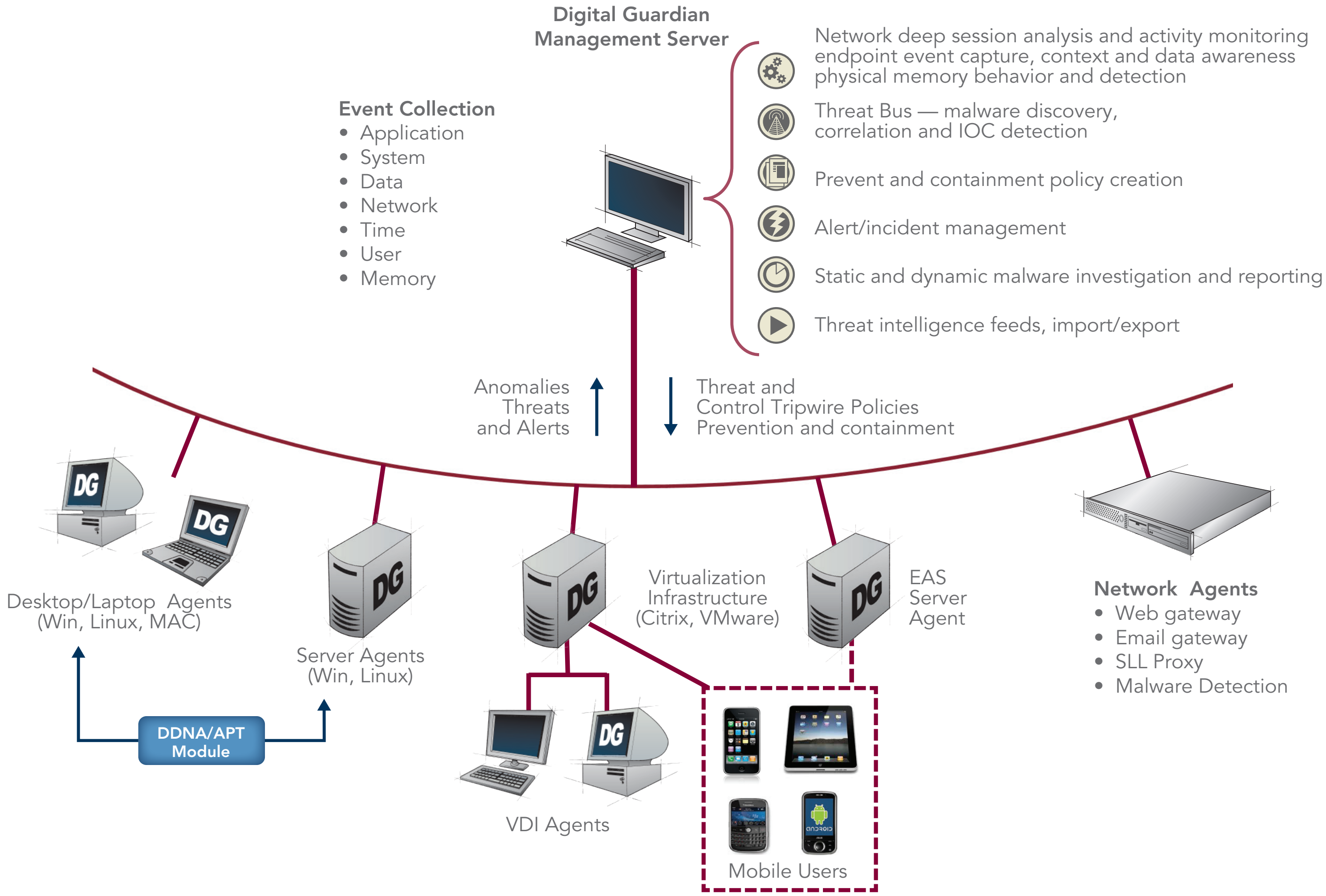

Digital Guardian
Management Server
Network deep session analysis and activity monitoring
endpoint event capture, context and data awareness
physical memory behavior and detection
Threat Bus — malware discovery,
correlation and IOC detection
Prevent and containment policy creation
Alert/incident management
Static and dynamic malware investigation and reporting
Threat intelligence feeds, import/export
Event Collection
• Application
• System
• Data
• Network
• Time
• User
• Memory
Anomalies
Threats
and Alerts
Threat and
Control Tripwire Policies
Prevention and containment
DG
Desktop/Laptop Agents
(Win, Linux, MAC)
Server Agents
(Win, Linux)
DDNA/APT
Module
Virtualization
Infrastructure
(Citrix, VMware)
EAS
Server
Agent
Network Agents
• Web gateway
• Email gateway
• SLL Proxy
• Malware Detection
VDI Agents
Mobile Users

Figure 4: The Verdasys Digital Guardian Cyber Defense Architecture is a Force Multiplier

Conclusion: Cyber Threat Defense Requires a Kill Chain Defensive Strategy

The most effective defense against cyber attacks requires a unified and layered security approach that can identify and isolate different stages of an attack by identifying anomalies challenging the malware's adaptability and stealth in ways it was not designed to circumvent. This Kill Chain defensive strategy requires the ability to detect and defend across all stages of a cyber attack. Technologies to help do this include network defenses like next-gen firewalls, intrusion detection systems, malware detection engines, network and endpoint cyber attack detection and prevention technologies, application whitelisting and memory scanning capabilities. When a force multiplier is added, in the form of an integration that can detect, correlate and create actionable intelligence and then effectively deploy prevention and containment controls, companies will for the first time have an effective cyber attack defense with a very high probability of success.

Digital Guardian offers both a kill chain defense platform and the integration needed to act as a force multiplier to effectively detect and stop a potential attack, even if the code or methodology has not been previously seen "in the wild". Digital Guardian agents use a powerful combination of technologies which provide early warning, application whitelisting and data-level access controls that can thwart cyber threats at first contact or at any point of an attack. Digital Guardian's integrated cyber threat defense result in:

- Increased positive detection rates for cyber attacks
- Decreased incident response time to detect and react to threats
- Greater ability to accurately identify infected machines and immediately deploy containment controls to isolate the malware
- Speedy forensic investigation to determine malware behavior, elimination steps and improved prevention
- Prevention of sensitive data compromise through data exfiltration blocking controls

Digital Guardian provides a comprehensive and integrated kill chain defense for cyber threat that correlates endpoint and network policy alerts and other suspicious activities to provide an enterprise-wide overview of threatening activity. Digital Guardian then enforces autonomous prevention and containment controls at different stages of an attack inside or outside the network thwarting any attempt to remove sensitive data.

Appendix 1:

Detailed Cyber Threat Requirements

Cyber Defense Solution Requirements	Value
Integrated, autonomous layers of defense across: network, endpoint and servers including operating system and system memory	Cyber attacks take many forms and new forms emerge as old attack models fail. The attackers can use a mix of attack vectors including compromised insiders. Attacks have multiple stages and include multiple paths of infection, account compromise and data movement. Defensive systems must offer independent means of detection and control so that a compromised layer does not compromise the whole system. Those layers must however be integrated so that their information can be correlated for faster detection, investigation and mitigation. Early detection and reduced reaction time are critical to cyber attack defense.
Inbound attack detection: executable detection, application control, inbound traffic monitoring, threat detection engines, attack threat feeds	Of all the stages of a cyber attack the initial penetration stage is probably the most difficult to detect and defend due to the sheer number of machine and human vectors. Therefore cyber threat defense must include a variety of capabilities covering rogue applications, inbound communications, the ability to check suspect code for malware and the input of the latest attack intelligence information to update detection and mitigation policies.
Education & awareness prompting to end user before a data incident occurs	End user prompting during a cyber attack is a highly effective means of alerting a user to a human targeted attack in real time and defeating potential phishing and spear phishing attacks. Prompting can also be used to enforce best practice polices and keep employees from making simple but risky mistakes like clicking on a dangerous links or going to a known bad website. In some cases, prompts can even delay or prevent a data exfiltration by providing a simple but unexpected barrier to malware activities.
Command & control detection and blocking: inbound outbound monitoring, intel feeds on known command and control systems	A significant weakness in many cyber attacks is the need to contact a control system to update attack models and stages. During the reconnaissance stage and exfiltration stage multiple calls are made. A defensive system can defeat many types of attacks by monitoring inbound and outbound traffic for these types of calls. Intel feeds with the latest intelligence on the types, formats, destinations and encryption models of these calls are critical in blocking them and defeating the attack.
Secondary infection, recon stage blocking: system, memory and network	Verdasys MSIP enforces data access and usage policies based on user-privilege, file sensitivity level (classification), and a user's IP access permissions

Cyber Defense Solution Requirements	Value
In particular departments, monitor the copying of documents or data	Once a system is infected, the attack moves to infect other more critical systems, compromise additional user accounts and gather information about the network in hopes of locating the targeted data for theft. Defensive systems that monitor internal traffic, endpoint systems that look for malware code running in system memory and endpoint event collection that alerts IT teams to user activities outside of normal operating parameters all help is recognizing and defeating the attack.
Data exfiltration blocking: network blocking, host blocking, encryption, threat intelligence on known bad destinations.	In the final stage of the attack, the malware attempts to move the targeted data to an exfiltration point and then from that point off the network. This is where the DLP 2.0 capabilities can help defeat a 3.0 threat. Endpoint and network agents work together here to recognize, through context and data classification the movement of sensitive data and fire off automated controls to defeat the attack. Controls can include data movement blocking across the network or at the endpoint and automatic encryption so that any exfiltrated files are useless.
Data access, data usage, data movement, application usage, and memory events — collected and aggregated in a centralized forensic analysis engine from across the enterprise including network, endpoint and virtual systems	When cyber attacks are detected it is critical to collect as much forensic evidence about the attack as possible to reconstruct the attack and determine its nature and structure. This information offers immediate defense value by modifying policies and controls to defeat similar attacks. It offers a wealth of forensic information to pass to SIEM and other analysis tools that can correlate even more data a broader set of systems.
Malware detection engine, static and dynamic analysis, virtual execution of malware	Another defense in depth layer, any potential code that comes inbound to the enterprise must be intercepted, inspected and even executed in a sandbox environment to determine if it is a threat. Malware will often disguise Trojans, rootkits, worms, viruses and other complex malicious software as innocuous looking items on a network. A malware detection engine offers a significant layer of defense in the initial attack stage.
Adaptive policies: combination of risk factors elevates response control	Another advanced defense in depth capability critical to detecting and defeating a cyber attack is the ability to create and deploy adaptive policies that will, based on cyber attack risk factors, deploy a control or series of controls to gather forensic evidence of an attack or defeat an attack. An example being when an endpoint agent detects an anomaly or the result of a memory scan reports an elevated risk, lock down policies are enacted at the affected endpoint while the incident is investigated.

VERDASYS®

Corporate Headquarters
860 Winter Street, Suite 3
Waltham, MA 02451 USA
info@verdasys.com
781-788-8180

www.verdasys.com