FORTRA™

WHITE PAPER (DIGITAL GUARDIAN)

Outsider Threat Protection

Building A Kill Chain Defense

Complete Data Protection Against Insider and Outsider Threats with One Agent

Introduction

Companies of all sizes face the problem of defending against outsider threats that vary in tactics and goals. Some attempt to disrupt services, while others are designed to steal sensitive information. Fortra™'s Digital Guardian® focuses on defending against outsider attacks that steal sensitive data. These attacks follow a common series of seven activities: Planning, Malware Introduction, Command and Control, Malware Expansion, Target Identification, Attack Event (Exfiltration), and Retreat or Removal. Organizations face several challenges dealing with this growing threat:

- Attacks are very sophisticated and often significantly different from previously used malware, making detection and defense difficult
- The number and variety of malware kits available continues to grow, offering attackers even more vectors to exploit
- Outsider attacks re-attack a second, third, fourth, or even fifth time to find weaknesses in an organization's defenses
- Attackers are patient; creating malware that will infect networks and then lay dormant for weeks or months until a weakness is identified
- Companies must protect data in a mobile world where laptops, tablets, and smartphones are often off the network
- Companies must protect data through their entire business and supply chains, including outside contractors, vendors, and partners who may be targeted and then later propagate the attack
- Companies must protect their own employees from social engineering attacks such as spear phishing, whaling, and water hole attacks. Employees need training to identify such attacks and respond appropriately

Defining Outsider Threats

The frequency and sophistication of outsider attacks continue to outpace the capacity for companies to defend against them. The most dangerous and effective malware is often designed for a specific organization ("target"), combining stealth, precision, and social engineering to penetrate the target's perimeter, compromise systems, and remain undetected for long periods of time. Targeted attacks occur across every industry where competitive and proprietary information is used, including manufacturing, technology, energy, financial, pharmaceutical, critical infrastructure, and, of course, military and government organizations. The attacks are not limited to the targeted organizations, but include 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.

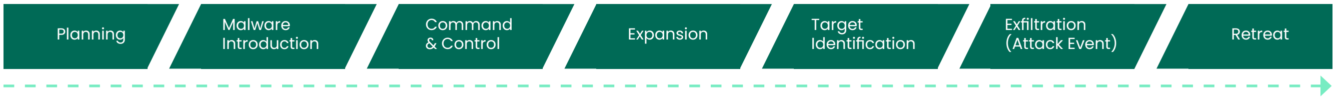

FIGURE 1: STAGES OF AN OUTSIDER ATTACK

Anatomy of An Outsider Attack

The goals of outsider attacks are to prevent detection, maintain a presence in the targeted environment for an extended period, identify targeted data, and exfiltrate the data. As such, most outsider attacks follow a common series of steps:

1. **Planning** – After a target organization is identified, attack planning begins. Planning includes researching the company's infrastructure to determine how the malware will be introduced, the communication methods used while the attack is in progress, and how/where the data will be extracted. In all cases, multiple paths are defined. If social engineering will be used in the attack, research is conducted to identify high value employees and their social media pages. From these, attackers can collect demographic and historical data, personal email addresses, and data about families and friends including birthdays, addresses, and schools attended. Profile intelligence collected from these activities includes likely passwords or lost password answers, people from whom the target would likely open email, whether home machines or networks are easier to compromise, and what the target's likely access to data would be based on their title, role, or relationships.

2. **Malware Introduction** – Malware is often introduced through social engineering attacks such as spear phishing. These attacks are personalized based on the success of the planning stage. Emails with embedded malware or links to compromised websites are common, but may other types of introduction methods may be used, including software and network vulnerability exploits. Social engineering is one of the most successful attack vectors because, even today, most people do not understand the risk of opening suspect emails and files, or clicking on unverified links. Further, most companies do very little to educate their employees about this risk in an effective way.

3. **Command and Control** – In sophisticated attacks, the malware needs to communicate with the attackers to send discovered information and 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 to the attackers and receive new instructions on what identities or machines to infect next, how to identify the targets, and instructions on how to exfiltrate the data.

4. **Malware Expansion or Lateral Movement** – Attackers assume the data they want will reside on multiple machines. Therefore, the malware will need to move laterally 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 a data-focused attack, this step usually consists of two parts. First, it will copy, obfuscate, and move the target data to an exfiltration point. The malware may store the stolen data in temporary passwordprotected RAR, ZIP, or CAB compressed folders. Next, the malware exploits defensive weaknesses to move data off the network. Weaknesses include remote access applications or FTP sites, email through a malicious SMTP server directly on the compromised system, and DNS (domain name server) extraction. Regardless of what event is used, the Attack Event stage in an outsider attack can take weeks or months, with the malware making multiple attempts to move and extract data, all while remaining hidden to infrastructurefocused 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 used in later exploits.

The Challenges of Protecting Against Outsider Threats

Organizations often struggle to deal with this relatively new and growing threat, and multiple challenges are present. The attacks are very sophisticated. Over 1/3 of initial malware introductions are a new or a significantly different variant of a previous attack, making detection and prevention by signature-based solutions difficult. The tools available to attackers are growing; malware kits are widely available on the Internet. The attackers are well-financed and patient, with attacks taking months to execute and portions of malware hiding silently in a victim's environment for even longer. Finally, the attacks are persistent. They probe defenses and try a second, third, fourth, or fifth time to infect the 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 devices not connected to the network. Whether it is an employee's company laptop, a BYOD machine, or a contractor's computer, a system can be infected quickly and easily without the protection of a network's defensive systems. When the device reconnects to the network, the infection expands and the attack begins. Attacks are also increasing along business supply and value chains. If a business partner needs confidential data and that partner has weak security, attackers will find and exploit those weaknesses.

Organizations often struggle to defend against these attacks because most security products are incomplete, or point solutions. Antivirus and other signature-based technologies are blind to any new attack. Many products have a forensics focus, and can only analyze the damage inflicted and identify which machines were infected. Most next generation technologies focus on the initial infection stage of the attack, yet studies show that even with these tools in place there are significant gaps in the malware infection stage of the attack. It is clear that a defensive focus is on a single layer of the perimeter or network is ineffective.

The challenge is not limited to inadequate technology. Spear phishing, whaling, and waterhole attacks fool unwitting employees into infecting their machines. If employees are made aware of threats and how to recognize them, they can be an additional and valuable line of defense.

Even the best security teams struggle to keep up with this constantly changing and continuously growing threat. Security teams must understand the methods and models of emerging attacks and manage the defensive point products. Then, they must correlate information to determine if an attack is real and the goal of the attack. Finally, they must determine what upgraded or additional defenses are needed to prevent the next attack.

The "Kill Chain Defense"

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. A common execution of the strategy was in the initial air attacks on Iraq, in Operation Desert Storm.

Security experts have adopted the term to describe the most effective defense against outsider attacks. There are two critical ideas behind the Kill Chain Defense as applied to outsider threat protection. One is that an organization must accept as fact that defenses at any given stage of an attack may fail. An organization cannot assume that any single solution will stop all attacks it is designed to stop, all the time. The second is that the Kill Chain Defense exploits a critical weakness in the outsider attack model; for an attack to be successful, all steps must be completed and the target data exfiltrated from the organization. In defending against multi-stage attacks, one needs only to disrupt one stage to stop the attack or reattack. When looked at this way, the defensive problem, and the ability to stop an attack successfully before it completes, becomes more 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 an attack and deploying effective defensive controls to the stages where the attack is most vulnerable. This model can be broken down into four defensive capacities: prevention, detection, containment, and investigation.

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

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

Containment: If an initial infection could not be blocked, deploy controls that prevent the malware from spreading to the command and control stages. Containment controls focus on blocking unknown executables and suspect cross-network or offnetwork communications, isolating machines from the network, and alerting users to risks and remediation actions in real time.

Investigation: Investigation requires collecting intelligence on the attack to determine details of its methodology and actions. Information collected from this stage is used to improve all other defensive postures and prepare for the next generation of the 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. The Kill Chain Defense relies on the ability to detect and defend across all stages of an attack and all layers of a network system.

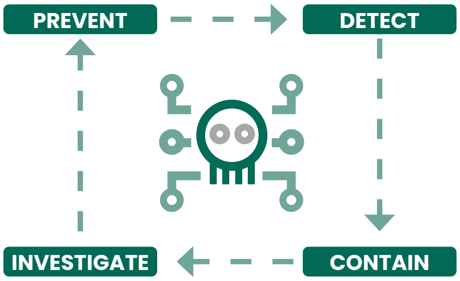

FIGURE 2: KILL CHAIN DEFENSE

Kill Chain technologies require autonomy; if one system becomes infected and compromised, it cannot degrade the ability of other systems to operate effectively. At the same time, the intelligence collected needs to be correlated so that attacks are quickly and accurately defined. Integration between products must exist, but in a manner that does not compromise the integrity of the Kill Chain strategy.

Digital Guardian – The Force Multiplier

Another military term that can be effectively transferred to outsider 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. In the advanced threat 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.

Digital Guardian provides a Kill Chain Defense platform, with the correlation and integration needed to act as a force multiplier. It can effectively detect and stop an attack, even if the code or methodology has not previously been seen "in the wild." Digital Guardian's kernel-level agents afford visibility to all data movement and use, and data-level access controls to provide early warning and blocking to stop outsider threats at any point of an attack.

Protect the Data for the Best Defense from Outsider Threats

Digital Guardian is security's most advanced endpoint agent. Its data-centric approach combines deep data visibility and knowledge of process-level malicious behaviors to protect against the loss of your sensitive data — whether the threat originates inside or outside your organization. To enable a Kill Chain Defense, Digital Guardian delivers:

Endpoint threat detection

The "network" now extends to wherever employees are, wherever data is, and wherever data can be accessed from. In this environment, keeping pace with constantly evolving attack vectors is a challenge for security professionals — and an opportunity for insider and outsider threats. Digital Guardian can detect, understand, and stop threats as they unfold at the endpoint, before sensitive data is compromised. Because the Digital Guardian agent is autonomous, your endpoints are protected whether they are on your corporate network, on a third-party network, or have no network access.

Process execution

The Digital Guardian agent identifies process starts, dynamic library loads, and other system-level behaviors that — independently or in combination — signal an attack on your data. When an attack is identified, Digital Guardian stops it in its tracks and immediately alerts your incident response (IR) team about what has happened. The compromised machine may then be quarantined from the network to stop the lateral spread of the malware.

Visibility

The Digital Guardian agent has knowledge of all kernel and higher-level activity related to file access, and reports the activity to the Digital Guardian console. By seeing key data interactions from all endpoints, your incident IR team can perform forensic analysis on intelligence from the full range of potential attack vectors across your endpoints.

Data classification

Industry-leading, automated data classification ensures the focus is always on the data that matters most. As you respond to threat alerts, you can prioritize those that threaten your most valuable data assets.

A platform approach

The Digital Guardian platform is extensible, built for scale, and centrally managed for unified policy and consistent data controls. Tens or even hundreds of thousands of agents can be monitored from a single console. This is particularly important since breaches often stem from the same weaknesses, whether they are the product of insider actions or bad outside actors.

Network integration

Digital Guardian offers APIs for direct integration with network security providers and threat intelligence services. This provides additional analysis capability and a choice of actions based on the intelligence information. For example, automatic submission of a file hash that's deemed a threat could result in all endpoints being set to block and alert should the threat be seen by any endpoint, whether on or off the network.

> **"With Digital Guardian, our IR team can stop would-be data thieves in their tracks, ultimately preventing the crime. Other endpoint threat prevention products only allow them to investigate the crime after it happened — after my data has been stolen."**
>
> **- CISO, FORTUNE 50 GLOBAL MANUFACTURER**

Meeting Gartner's Requirements for Endpoint Threat Detection and Response

☑	☑	☑	☑	☑
Collect endpoint data such as running processes	**Centralize the data** by near-real-time collection and make it quickly available	**Post-process the data** to identify anomalies such as rare processes	**Provide an interactive data** UI that allows exploration of the data	**Alert based on patterns** such as new process or connection, or "anomaly score"

Event Collection

- Application
- System
- Data
- Network
- Time
- User
- Memory

- 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

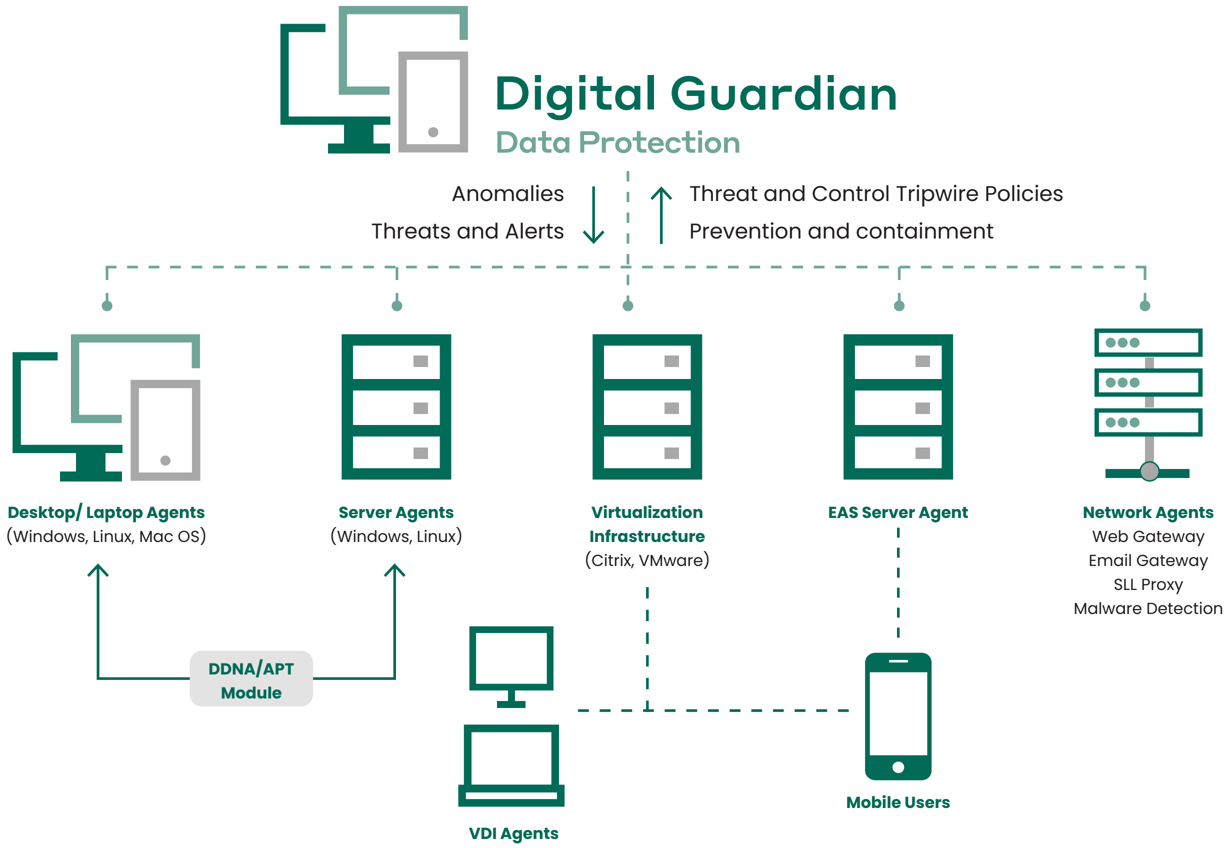

FIGURE 3: The Digital Guardian Outsider Threat Protection Architecture is a Force Multiplier

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.