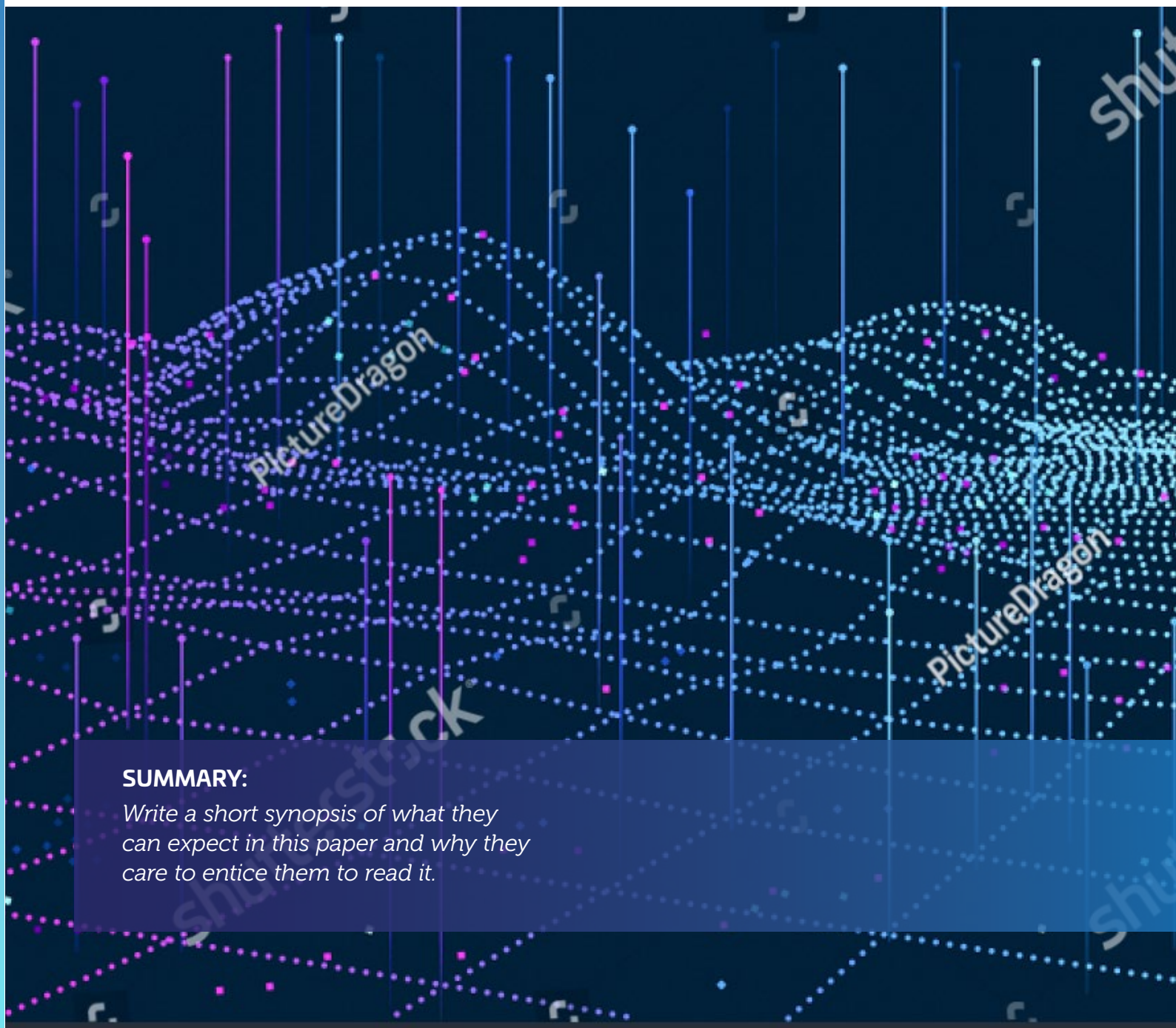
APPGUARD
The Malware Disruptor

Navigating the Confusing Endpoint Security Landscape: Why Prevention is Key

WHITE PAPER



SUMMARY:
Write a short synopsis of what they can expect in this paper and why they care to entice them to read it.

We Need an Intro Subhead

Endpoint security is not a new concept. For over thirty years companies have been working hard to keep corporate endpoints and assets secure. Today's digital transformations, driven by cloud computing, virtualization, and the shift to remote and hybrid work environments, have changed the nature and number of endpoints – further expanding the attack surface. The concept of a defined perimeter is obsolete with once hardened perimeters now blurred, porous, and open to attacks. Previously effective endpoint security solutions are unable to protect endpoints against the evolving malware techniques hackers use to gain access to critical, sensitive data.

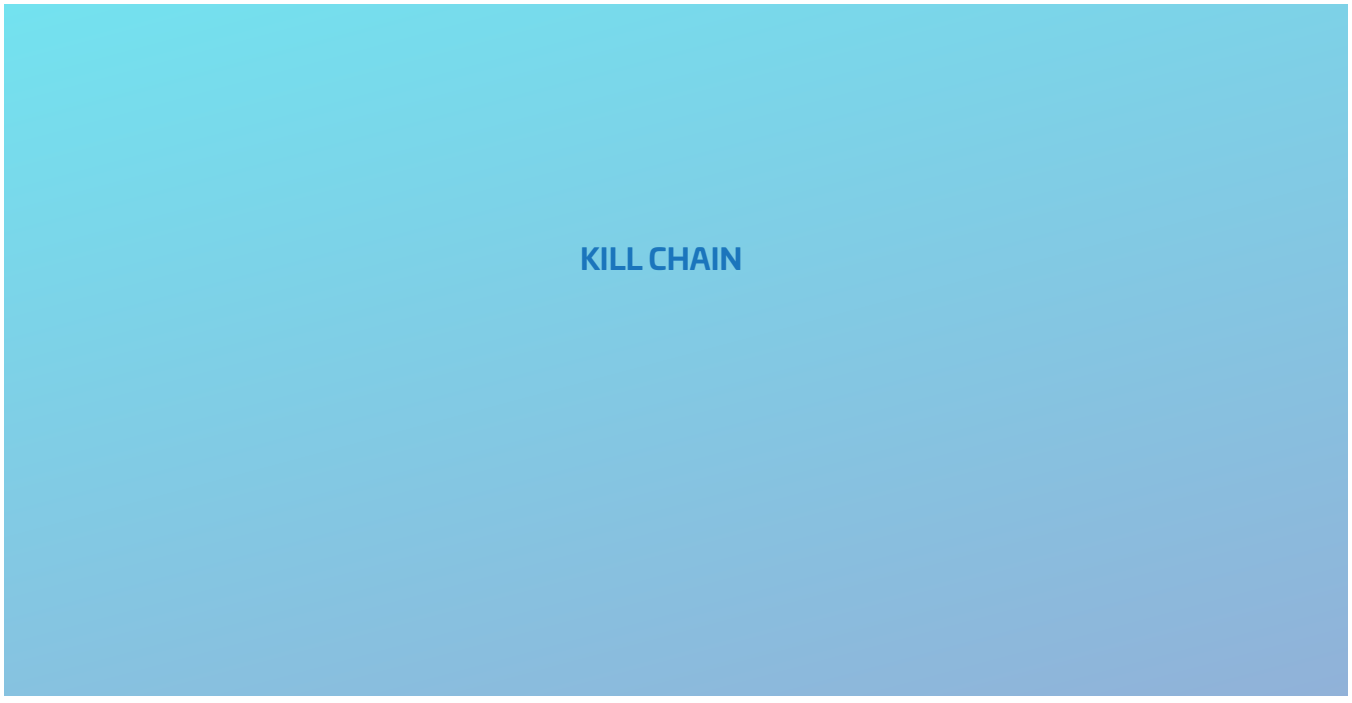
Cybercrimes, particularly endpoint exploits, are now an everyday concern for businesses. As a result, investments in cybersecurity are expected to reach over US $200 billion globally by 2023, and according to Fortune Business Insights, the global endpoint security market is expected to reach US $22 billion by 2027. Heavy investments in endpoint security shouldn't be a surprise given endpoints are the prime target for today's sophisticated hackers. In fact, recent reports indicate that more than 70% of threats now occur on endpoints.

Today's endpoint security market is fragmented and congested with many different solutions making indefensible claims – rendering it difficult to make an educated choice. Endpoint security is not just about protecting the endpoint, it's about protecting the broader environment in which the endpoint operates. Hackers, determined to exploit endpoints, continually look for ways to create stealthy attacks designed to outsmart today's endpoint protections.

Defense-in-Depth: A Strategy for Protecting Endpoints

Security defenses have evolved from the launch of primitive anti-virus solutions in the 1980's to more advanced technologies and techniques of today. Yet, despite the evolution of endpoint defenses, endpoints continue to be breached at unprecedented volumes. To combat today's sophisticated cyberattacks, organizations must apply a defense-in-depth strategy that utilizes a mix of advanced protection tools and methodologies. With defense-in-depth, different tools focus on protecting different points along the Cyber Kill Chain (i.e. the malware attack cycle). This multi-layered approach, with built in redundancies, assumes attackers will penetrate, or have already penetrated different layers of the organization's defenses. Using a defense-in-depth approach, if one mechanism fails, another can step in to thwart the attack.

A defense-in-depth strategy assumes there is no one single method that can protect against every type of attack. To establish an effective defense-in-depth strategy, one must take the time to understand the endpoint protection options available, including their strengths, weaknesses, and level of protections they provide.



> *Pull quotes or sidebar information Ipsuntus animus, ut dolorit aturerc hilisci aspidio ea volo es ipsant es delent.*
>
> *At andignimi, etur? Apellorerum, omnis experum nobis sequi ulpa dis molorposto estrum none vendio officie nihillaborum.*

Anti-virus

Antivirus solutions were introduced in the late 1980s and are proven to be very effective against known threats. Early malware attacks were mainly file-based and could be identified by a unique signature attached to a specific file. In essence, anti-virus solutions are databases of known malware signatures.

Strengths:

Anti-virus solutions are great at detecting and removing well-known threats and cleaning up devices.

Limitations:

Anti-virus tools are simplistic and limited in scope and cannot protect against today's sophisticated fileless attacks and in-memory exploits, as these types of attacks have no signature for them to find. They require constant updates and scans, and can significantly slow down processing times, potentially impacting business productivity. Additionally, anti-virus solutions are known for generating high volumes of alerts, with many false positives – leaving security staff often overwhelmed with alert fatigue.

Next-Generation Anti-virus (NGAV)

In in the late 2000s, next-generation anti-virus systems were introduced to address some of the limitations inherent in traditional anti-virus offerings. While no single definition for the term exists, NGAVs typically expand upon the foundation of anti-virus with the introduction of advanced machine learning and artificial intelligence capabilities to detect basic exploits, as well as fileless attacks.

Strengths:

Unlike traditional anti-virus solution, NGAV solutions can detect some of today's more sophisticated threats by adding an AI component for signature-less attacks.

Limitations:

Machine learning and artificial intelligence-based NGAV tools require ongoing care and feeding by trained resources. Like traditional anti-virus solutions, NGAV systems are known for producing high volumes of alerts – especially when systems are tuned for maximum protection. NGAVs can be a drain on resources required to investigate alerts. All too often, the high volume of alerts needing investigation exceeds resource capacity – leaving potentially identified risks free to cause harm. Last, the concept of machine learning assumes that past malware forms can predict future malware activity – ignoring malware's potential to evolve its method of delivery or attack.

Endpoint Protection Platforms (EPP)

EPPs were introduced to simplify IT and security operations. The idea was to assimilate endpoint device security functions (anti-spyware, application control, antivirus, personal firewall, etc.) into a single, unified security solution designed to detect and stop a variety of threats at the endpoint. This collective approach is designed to be more effective than a collection of siloed security products that lack the ability to communicate.

Strengths:

EPPs consolidate multiple defense functions into one agent – eliminating the need to deploy and manage multiple siloed. Advanced Endpoint Protection Platforms EPPs prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

Limitations:

EPPs are preventative tools that perform point-in-time protection by inspecting and scanning files once they've already entered your network. Taking a post-execution approach, EPPs detect when you've already been breached. EPPs are typically a full stack solution – often taking an all-inclusive approach. It is not uncommon for EPPs to make previous technology investments obsolete.

Sandboxing

Sandboxing is a cybersecurity practice where you run, observe, and analyze code in a safe, isolated environment that mimics a user's operating environment. Sandboxes are not actively connected to production systems and are designed to prevent threats from getting onto the network. A sandbox is a type of software testing environment that enables the isolated execution of software or programs for independent evaluation, monitoring, or testing.

Strengths:

Sandboxing prevents host devices and operating systems from being exposed to potential threats. Sandboxing allows new, untrusted software to be tested for threats before being introduced into the production environment.

Limitations:

Working in sandboxes can be cumbersome and complex.

They require separate logins from production environment systems, and changes made in the sandbox do not automatically move over to production systems – adding extra steps, and often frustration, for end users. Sandboxing is inflexible, secures limited applications, and does not adapt to changes.

Application Whitelisting

An application whitelist is a list of applications and application components that are authorized for use in an organization. Application whitelisting technologies use whitelists to control which applications are permitted to execute on a host. This helps to stop the execution of malware, unlicensed software, and other unauthorized software.

Whitelisting is designed to ensure users only take previously approved actions on their computer. A list of approved applications are designed to block malicious activities. Instead of trying to keep one step ahead of cyberattacks to identify and block malicious code, IT staff compiles a list of approved applications that a computer or mobile device can access. In essence, the user only has access to functionality an administrator has deemed safe.

Strengths:

Application whitelisting can be very effective at keeping cybersecurity problems at bay by identifying every file and application as a unique item, regardless of which software program it belongs to, and then controls exactly what can run your network, on which machines, and by whom.

Limitations:

Application whitelisting often proves inconvenient and frustrating for end-users. It also requires dedicated resources to implement and maintain lists, and the endpoint protection provided is only as good as the accuracy and maintenance of the list. In a constantly changing environment where patches and updates are frequent, maintaining a whitelist is nearly impossible.

Application Control

Application control is a security practice that blocks or restricts unauthorized applications from executing in ways that put data at risk. In order for computers to talk to one another, their traffic needs to conform to certain standards. The main objective is to ensure the privacy and security of data used by and transmitted between applications.

Strengths:

Application control can reduce the risk of unauthorized applications taking control of endpoints, servers, or other devices, and can protect against zero-day and advanced persistent threats.

Limitations:

By treating software as application packages rather than individual files, trusted software can be compromised to run malicious code. This type of attack commonly occurs through social engineering efforts. Unless the controls are able to adapt the "trust" level in different contexts, it becomes difficult to operate a business or properly protect against evolving attacks.

> *"Pull quotes or sidebar information Ipsuntus animus, ut dolorit aturerc hilisci aspidio ea volo es ipsant es delent.*
>
> *At andignimi, etur? Apellorerum, omnis experum nobis sequi ulpa dis molorposto estrum none vendio officie nihillaborum.*

AppGuard Ultimate Endpoint Security: Prevention without Detection or Inconvenience

While each of the endpoint security tools referenced provide some protections for endpoints, each has limitations. Ideally, an endpoint protection solution should block malware from executing without placing a burden on security teams or disrupting the way end users work.

However, most endpoint protection tools take a reactive approach – they detect when a system has been compromised and then attempt to control the damage. This concept is flawed. Why wait to detect breaches that have penetrated your organization, when you can prevent breaches altogether? By focusing on prevention, rather than detection, endpoints won't be compromised, security staff levels can be reduced, and security teams can redirect their attention to act on true indicators of compromise and focus on more strategic security initiatives. Unfortunately, tools that are more proactive are too burdensome to maintain proper security or operational efficiency – but not AppGuard.

AppGuard is the answer to ultimate endpoint security without detection or inconvenience. AppGuard takes an entirely different approach to securing endpoints. Instead of detecting malware in your network, AppGuard proactively disrupts malware before it successfully compromises the endpoint – providing better protection with less effort and less stress. Applying Zero Trust within the endpoint, AppGuard ensures applications and utilities cannot be exploited to take unintended actions. With AppGuard, businesses can do what they need to do, while malware is prevented from doing what it wants to do.

AppGuard achieves Zero Trust within the endpoint by restricting high-risk applications and utilities from performing the high-risk actions that malware must conduct to cause harm and achieve its goals. By limiting what actions are allowed within the endpoint, instead of having to explicitly recognize good vs bad or normal vs. abnormal behavior, AppGuard increases attack resilience and improves your organization's security posture without exhausting internal resources. AppGuard's Zero Trust approach to securing endpoints enables you to stop attacks before they begin without having to monitor, investigate, or respond to alerts.

Malware Disruption: True Endpoint Security from AppGuard

AppGuard outsmarts malicious actors by applying autonomously adaptive policy controls over application behavior. AppGuard policy controls block the actions that malware must execute on endpoints in order to cause harm (e.g. command and control or data exfiltration). Blocking actions based on context, AppGuard protects systems in real-time against malware, regardless of the attack vector or type of attack – without the limitations and post-compromise costs of detection-based tools.

Maximize Security Investments with AppGuard

By disrupting malware, AppGuard plays a critical role in your defense-in-depth strategy, reducing work at outer layers, and increasing the ROI for existing security tools. If malware does not reach the endpoint, non-endpoint tools (e.g. network intrusion detection, deception grid, SIEM, etc.) will have fewer indicators of compromise to detect and will produce less false positives. AppGuard's preventive controls at the endpoint reduce lateral movement and the workload of other tools, thereby increasing the efficiency of resources and the effectiveness of security programs.

As a component of your defense-in-depth strategy, AppGuard complements and enhances many of your existing endpoint security tools by focusing on removal and mitigation, and eliminating the need for the more burdensome pre-exploit tools like whitelisting, application control, or sandboxing. When unknown, polymorphic or fileless malware eludes NGAV or EDR solutions and prepares to attack the endpoint, AppGuard is there to stop the attack in its tracks - with no quarantine or remediation necessary.

AppGuard: Endpoints without Compromise

As cyber threats continue to grow in both complexity and numbers, now, more than ever, it is critical to have effective endpoint protections in place that can disrupt threats before they cause harm. Understanding the different security technologies available and the nature of the threats you want protections from, is critical. Before embracing any advanced endpoint protection solution, take the time to consider the capabilities of the solution and your organization's maturity level to determine if a tool is right for you.

To ensure optimal protection implement a defense-in-depth strategy that prevents security breaches before they happen. Select tools that are not limited to defending against known exploit signatures, won't impact user or system productivity, or require an army of security experts to support. Implement a preventative endpoint protection approach that allows security resources to move away from constant firefighting chasing and responding to alerts. Achieve optimal endpoint security - choose AppGuard for endpoints without compromise.

Revised Where we Play, What we Complement/ Replace image to be added. Placement possibly near Defense in Depth.

About AppGuard

As people and organizations all over the world become more interconnected via the endpoint devices in their lives, AppGuard delivers simple, effective solutions to the complex security challenges that threaten them every day. Covering a range of devices from personal computers to mission critical servers, AppGuard prevents compromises before they happen by disrupting malware activity without having to recognize it. At AppGuard, we believe we can set a new standard: true cyber protection for all.

APPGUARD
The Malware Disruptor

www.appguard.us | sales@appguard.us