MORPHISEC
Breach Prevention Made Easy

THE ULTIMATE RANSOMWARE STRATEGY

Zero Trust + Moving Target Defense

Stopping Ransomware, Zero-Day, and Other Advanced Threats Where NGAV and EDR Are Failing

© 2022 Morphisec Ltd.

MORPHISEC

Contents

 © 2022 Morphisec Ltd.

MORPHISEC

Executive Summary

Despite the growing investment in cybersecurity, damage from cyber attacks continues to rise at an unprecedented rate, projected to reach over $10T by 2025. If existing solutions are supposedly working, then why are ransomware breaches happening and inflicting so much financial devastation, brand erosion, and loss of business? The problem is that today's solutions fail to counter threat actors' advanced attacks.

Next generation antivirus (NGAV), endpoint protection platforms (EPP), and endpoint detection and response (EDR) solutions are adequate at stopping known attacks with recognized signatures and behavioral patterns, but often fail to detect and prevent attacks that most organizations are experiencing today. A new technology has emerged that has been proven to stop ransomware and other advanced zero day attacks, making prevention-first security a reality: Moving Target Defense (MTD).

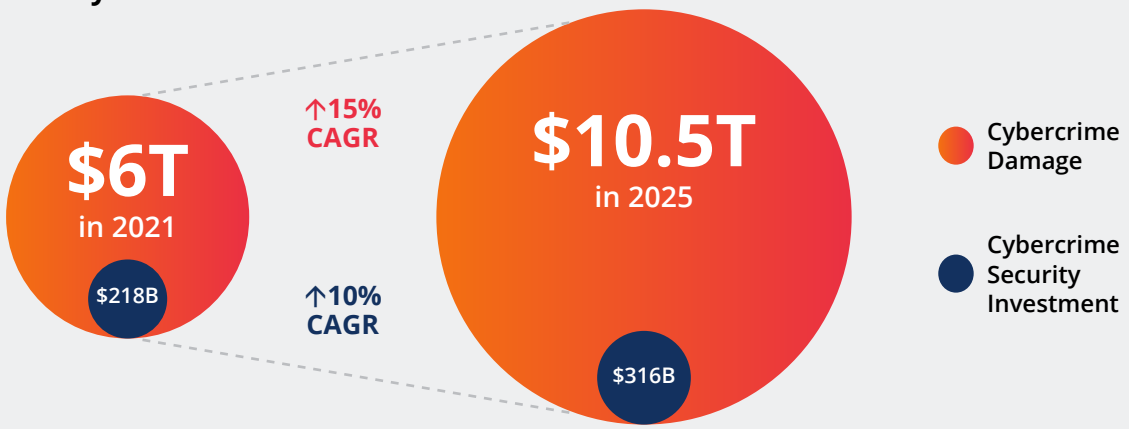
Several years ago, the National Institute of Standards and Technology (NIST) released a new framework called Zero Trust Architecture (ZTA) (800-207). While ZTA predominately addressed Identity and Access Management (IAM), the NIST document also admonishes a zero trust approach for endpoints. As such, ZTA has become an important centerpiece to ensure a mature cybersecurity posture. Within a ZTA framework, nothing has trust status. Instead, everything must undergo verification and authorization, early and repeatedly. MTD enables security teams to adopt ZTA and embrace the changes needed to stop advanced attacks. This white paper introduces and demonstrates the proven power of MTD, and clarifies how it facilitates ZTA and can transform your cybersecurity posture in the process.

© 2022 Morphisec Ltd. | morphisec.com

1 The Cybersecurity Slump

Cyber attacks are growing more audacious in every way. They are relentless, sophisticated, and devastating, driven by increasing numbers of cyber criminals, some with the backing of powerful governments. Despite ballooning investments in cybersecurity, expected to rise to $316B by 2025, damages are rising much faster, on pace to eclipse $10 trillion by 2025. (refer to the below figure) And in the wake of the SolarWinds incident, even the largest companies and most-secure public agencies have had serious vulnerabilities exposed. In this alarming climate, one conclusion leaps to the forefront: disruptive innovation is needed to improve cybersecurity and ensure a ZTA posture.

Cybercrime is Rampant Despite Rising Cybersecurity Investment



Sources: Statista, Cybercrime Magazine

Unfortunately, the vast majority of security teams have resource and time constraints, and are often unable to implement a complete ZTA framework. They usually focus on building strong and sizable defenses that are static by nature – a defensive "wall" around vital endpoints. Obviously, this approach is no longer working.

A familiar, unchanging attack surface only makes it easier for bad actors to find, reach, and compromise their intended targets. This also places huge pressure on security and IT teams to deal with emerging threats and mitigate attacks that bypass existing defenses, including NGAV, EPP, and EDR solutions. If it feels like cybersecurity is always playing catch up, that's the byproduct of using these "dug-in" defenses against evasive attacks.

Like a fighter that is able to bob and weave, cybersecurity defenses need better agility than the attackers. That's the basic philosophy behind MTD. It's also the goal of ZTA cybersecurity,

© 2022 Morphisec Ltd. | morphisec.com

which is quickly becoming the dominant paradigm for digital defenses. In this white paper, we explore the intersection of MTD with ZTA cybersecurity and illustrate how they create a unique synergy between tools and techniques.

As noted, traditional defenses like NGAV, EPP, and EDR often fail. Advanced attacks that lead to ransomware are winning. It's time to rethink the fundamentals of cybersecurity – starting with a ZTA strategy based upon MTD.

> "Morphisec proved that security can be effective while being intuitive, ultimately disputing the theory that prevention never works."
>
> — SANS Institute

2 Why NGAV and EDR Are Never Enough

MTD and ZTA cybersecurity (which we will cover shortly) were born out of necessity. NGAV, EPP, and EDR solutions deserve some blame for the uptick in successful cyberattacks. Improving on these tools hasn't worked, as the recent outbreak of ransomware illustrates. Continuing with the status quo in cybersecurity will only make this situation worse.

Why? Because traditional solutions often rely on file signatures, behavioural patterns and other known tactics and procedures to identify attacks. Even those aided by AI, machine learning, or anomaly detection need prior exposure to attacks to "learn" how to stop subsequent threats. This makes signature and behavior-based defenses great at thwarting known attacks - the low-hanging fruit of cyber crime. However, for unknown zero-day, fileless or custom packed malware, in-memory whitelist bypassing, runtime, and other advanced persistent threats such as credential theft and sophisticated user account escalation, they are essentially blind.

This problem creates several important implications. First, currently trusted technologies meant to be pillars of cybersecurity are actually missing many (even most) attacks, including many of the most damaging. It also gives every new attack devised by criminals a strong chance of succeeding. And when these defenses can't detect or prevent an incoming attack, the security team can only respond after the damage has already started. Therefore, cybersecurity based on traditional solutions expose firms to substantial risks, including potential compliance fines, lawsuits, and brand damage.

Signature-based and similar defenses can still be indispensable for any security strategy; as known attacks must also be stopped. NGAV, EPP, and EDR are still important tools when striving to achieve a ZTA framework; however, given the current landscape where attacks have become more nimble and novel, these tools are no longer enough. Where they end is where a ZTA strategy based on MTD begins.

© 2022 Morphisec Ltd. | morphisec.com

3 Introducing Moving Target Defense

MTD leverages a simple, potent, and proven strategy to prevent cyber attacks: a moving target is harder to hit than a stationary one. An analogy from physical security explains how MTD works. Every bank has locks on the doors (NGAV) to keep crooks out, and perhaps video cameras (EPP or EDR) to warn perpetrators and record illicit activity once criminals have penetrated defenses. MTD takes a prevention-first approach to complement more reactive fortifications that may miss more sophisticated zero-day threats by constantly shifting and hiding entry points from criminals to prevent them from getting in. Even better, it sets a trap to capture threat actors' movements to further secure against future attacks.

Most attacks follow a prescribed road map to reach their intended target. Therefore, if attackers can't find what they expect–as in a door or window into an organization–they will fail. Entry points kept in motion, rather than left at rest, are significantly more secure because they are unpredictable and unknown by nature. With Moving Target Defense, attackers must find their way forward and fight their way through. Given the added effort and cost of perpetuating these attacks, most attackers move on to other, easier targets.

Put simply, MTD hides vulnerabilities, weaknesses and critical assets from threat actors without disrupting current NGAV, EPP, or EDR functionality. This ensures that zero-day, ransomware,and other advanced attacks are stopped before they can do damage.

More detailed definitions of MTD include:

MORPHISEC

> "Moving Target Defense prevents unknown and zero-day attacks by using system polymorphism to hide application, operating system and other critical asset targets from adversaries in an unpredictable manner, leading to a dramatically reduced attack surface and security operational costs."

Gartner

> "Moving Target Defense is a set of techniques whereby dynamic or static permutations, morphing, transformations, or obfuscations are used to deflect attacks." Source

U.S. Department of Homeland Security

> "Controlled change across multiple network and system dimensions to increase uncertainty and complexity for attackers by reducing their window of opportunity and increasing the costs of their probing and attack efforts." Source

© 2022 Morphisec Ltd.

> **"Morphisec is the leader in Moving Target Defense."**
>
> — Gartner Peer Insights
> Sr. General Manager, *$500M - $1B revenue financial company*
>
> Gartner peerinsights™

MTD can be applied at the network, host, or application levels. All three types have value, but application level MTD is the most important since applications, operating systems, and endpoint resources are the most popular attack entry points. Stopping attacks at the application level ensures they fail even if they have succeeded at subsequent levels. This is the last line of defense before an attack becomes an incident. MTD stops attacks before malware deploys and/or does any damage, and it does so without straining device resources, requiring any intervention from human analysts, or even necessitating a strong internet connection.

Morphisec, as the leader in Moving Target Defense, has deployed its MTD-driven breach prevention solution at over 5,000 enterprises, protecting over 8.5 million endpoints and servers daily from many of the most advanced attacks. In fact, Morphisec is currently stopping up to 30,000 ransomware, malware, and fileless attacks per day that NGAV, EPP, and EDR solutions have failed to detect or prevent (e.g., Morphisec Gartner Peer Insights reviews, PeerSpot reviews and customer success stories). Examples of such attacks that were stopped at day zero, when other solutions were unable to stop them, include but are not limited to:

Ransomware

(e.g., Conti, LV, Ryuk, Ragnar Locker)

Backdoors

(e.g., Cobalt Strike, other in-memory beacons)

Supply Chain

(e.g., CCleaner, Asus, Kaseya pay-loads, Itunes)

Malware Downloaders

(e.g., Emotet, QBot, Qakbot, Trickbot)

Morphisec's MTD-driven breach prevention solution leverages the same kind of polymorphism used by advanced threats to avoid controls for the benefit of defenders. In doing so, we give organizations the ability to stop threats from unknown vectors, such as ransomware, new malware, and new variants of malware, even when they don't have recognizable signatures or deploy from device memory. Critically, MTD does not put any extra strain on an organization's most valuable security resource — its personnel. By working alongside OS native Microsoft Defender (NGAV, EPP, EDR), MTD is not only more affordable, it is also a much more effective alternative to traditional security controls. Morphisec's MTD technology augments most NGAV, EPP, and EDR solutions, creating the most effective 360 degree security available.

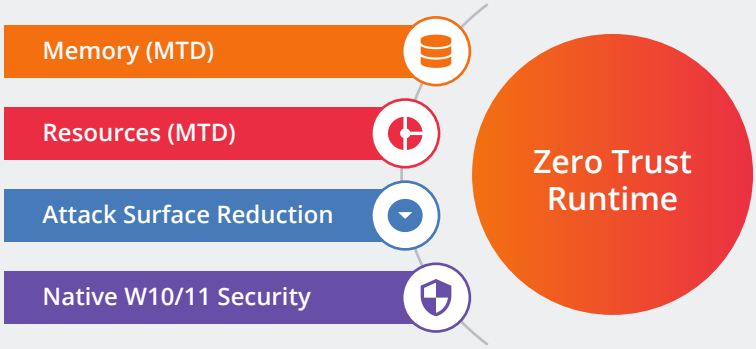
© 2022 Morphisec Ltd. | morphisec.com

> "Moving Target Defense is one of the most impactful emerging technologies in the security market
>
> — Gartner Research

Gartner

The Morphisec Secret Sauce: Moving Target Defense
Differentiated value driven by disruptive technology

- Prevent Zero Days, Unknown, Fileless, Evasive attacks
- No reliance on prior knowledge
- Easy to set up and operate
- No runtime performance impact



The concept of Moving Target Defense seems simple, but the impact is profound: cybersecurity no longer stands still. Instead, it does everything possible to outrun and outsmart attackers. When defenses stay on the move, they remain one step ahead of attacks at all times. Against MTD, the attackers, not the defenders, are at a disadvantage.

4 The Concept of Cybersecurity Zero Trust Architecture Explained

In the span of a decade, cybersecurity ZTA has evolved from a hypothetical framework to become the centerpiece of cybersecurity. With the signing of executive order 14028, the Biden administration recently instructed NIST to update mandates, such as the ZTA framework. All federal agencies and those who do business with these agencies must comply. Moreover, any firm using NIST or similar frameworks are motivated to adhere to these guidelines to mitigate ransomware risks. Countless security teams are either embracing NIST ZTA for the first time, or pushing it to the forefront of their security strategy. All signs suggest that ZTA will become even more of a cybersecurity standard – something that protection depends upon and every organization relies on.

ZTA has emerged in response to the repeated failures of prevailing cybersecurity strategies. Security based around the idea of a defensive perimeter admits access to anyone with authorization, then "trusts" everything happening inside the perimeter to have broad privileges. The problem is that attackers have found countless means to obtain credentials to sneak through perimeters. Once inside, they weaponize their trusted status to move around at will without triggering alerts.

© 2022 Morphisec Ltd.

In a ZTA framework, *nothing* has trust status–including endpoints. Instead, everything must undergo verification and authorization, early and repeatedly. Limiting access as much as possible while verifying anything given access is at the heart of zero trust. This approach can be applied in all facets of cybersecurity so that attacks must overcome repeated obstacles and evade constant scrutiny.

As trust relationships become both more expansive and riskier, they put an entire cybersecurity infrastructure in jeopardy. Recent history shows that anytime defenses decline, attackers can exploit weaknesses to their advantage. ZTA is the only logical step: trust nothing, verify everything, and always stay on guard.

This also holds true for protecting applications across the enterprise and across their lifespans with zero trust code execution. Only verified executable code should be allowed to access critical assets, and any code exhibiting suspicious behaviors or tactics should be blocked.

> **"Morphisec's unique approach to blocking endpoint threats means prevention is no longer a forgotten topic."**
>
> **— SANS Institute**

SANS

© 2022 Morphisec Ltd. | morphisec.com

5 The Ultimate Strategy: Moving Target Defense and Zero Trust

Moving Target Defense transforms the zero trust philosophy into an actual security strategy. Morphisec Guard, the market leading solution empowered by MTD, illustrates how keeping endpoints moving does exactly what ZTA advocates. Here's a simplified explanation of how Guard MTD works:

MORPHISEC GUARD

1. Morphisec Moving Target Defense allows for endpoint Zero Trust Architecture by creating a dynamic attack surface to ensure untrusted access to process memory is prevented.

2. MTD creates a barrier around process memory and associated resources, then morphs and moves this to prevent access by foreign code compiled by threat actors.

3. Only the process loader is verified and "trusted" to allow authorized access to the morphed resources, which removes external threats while maintaining seamless functionality.

Similar to Guard, Morphisec Keep for Linux and Windows offers MTD technology for servers, which often contain an organization's most sensitive information. Keep helps ensure ZTA for Cloud Workload Protection Platform (CWPP) and Server Workload environments. Non-dynamic applications or applications that are predictable become easy targets. Keeping them in constant motion ensures they evade attacks rather than risking penetration. Furthermore, randomizing the application memory assets, such as locations, names, links, credentials and more means that only authorized users can reach it, applying a form of identify and access management at runtime. This represents ZTA in action. And since MTD on the endpoint protects the operating systems and applications under the heaviest attacks, it puts zero trust in action where it matters most.

PeerSpot

> "We have peace of mind knowing there is an additional layer of security protecting our endpoints."
>
> — PeerSpot Review by Morphisec Customer

 © 2022 Morphisec Ltd.

6 The Anatomy of Evasive Attacks

Taking a closer look at evasive attacks makes clear why ZTA and MTD are mission-critical for the present and future of cybersecurity. The past year has set records for the number of zero-day exploits and the chaos of ransomware attacks. With massive resources underscoring cyber crime, attacks will only get better at dodging detection and prevention.

There are numerous ways attacks can hide malicious intent and cloak themselves in authenticity. The list is always expanding, but these are some of the key techniques:

- **Polymorphism** – Changes malware signature
- **Metamorphism** – Changes malware code at execution
- **Obfuscation** – Obscures malicious activities
- **Self-Encryption** – Uses encryption to hide malicious code and data
- **Anti-VM/Sandboxes** – Changes behavior to evade forensic analysis
- **Anti-Debugging** – Switches tactics in forensic environments to break debugging
- **Encrypted Exploits** – Changes parameters & signatures to elude investigation
- **Behavior Changes** – Waits for use activity before executing

These techniques have proven brutally effective. The attacker's advantage has only expanded over time. Repeated incidents have shown that NGAV, EDR, and every other method for detecting and stopping threats can't deal with an onslaught of evasive attacks.

Zero trust acknowledges this reality. Since any attempt to keep attacks at a distance from sensitive assets has – and inevitably will – fail, security must surround the assets themselves. By defending targets rather than entry points, ZTA MTD aims to shrink the attack surface and prevent the consequences of attacks that breach higher layers of security.

Morphisec's Moving Target Defense ensures ZTA by treating the process memory as a sensitive asset. It draws a perimeter around the memory and its resources, morphs it, and moves it someplace inaccessible to foreign code compiled by the attacker. Only the process loader is verified to access the morphed resources. This technique removes external interference from the attack surface while maintaining seamless functionality for regular users (unlike whitelisting). With MTD, ZTA principles are put into practice to keep applications accessible for the authorized few and far away for everyone else, evasive attacks included.

© 2022 Morphisec Ltd. | morphisec.com

7 Endpoints: The New Front-lines of Cybersecurity

(Desktops, VDIs and Servers/Cloud Workloads)

From ransomware to zero day threats to social engineering schemes, endpoint attacks are some of the most devastating. Unfortunately, they are also becoming some of the most common. In one survey, nearly 70 percent of respondents had seen an increase in endpoint attacks and fallen victim to at least one.

What explains this sudden surge in endpoint attacks? The sudden shift to remote work, for one, which makes many existing endpoint defenses insufficient or obsolete. But the bigger explanation is the expansion of what constitutes an endpoint, giving hackers a bigger target to strike at and new exploits to work with.

Endpoints in recent years have evolved from physical devices to various virtual equivalents. Popular examples include virtual desktop infrastructure (VDI), cloud workloads, and remote desktops, all of which have seen brisk adoption of late. They've also become prime targets for attack:

3X

Attacks against remote desktop protocols (RDP) have more than tripled

500%

Attacks against cloud services have risen over 500%

100%

VDI usage has increased by 100% despite troubling security vulnerabilities

These three examples of "new endpoints" have several things in common. First, they are not easily or adequately secured by traditional methods of endpoint security. Second, they each rely on numerous trust relationships that make them vulnerable to exploitation for all the reasons outlined earlier. Cloud workloads, VDIs, remote desktops, and similar technologies have become instrumental to the modern office, but they have become a serious security liability in the process - one that attackers are acutely aware of.

That's the bad news and the good news. Knowing that trust relationships are the weak point in today's endpoints makes a loud and clear case for adopting zero trust endpoint security.

Complicating that case, however, are the logistics. Ballooning numbers of endpoints, including shadow IT, makes it difficult to apply ZTA uniformly. Usability becomes an issue as well since the rigorous standards of zero trust may clash with processes and workflows. Bringing ZTA to the endpoint can seem like an impossible endeavor. Yet without it, a zero trust strategy isn't complete, compromising the entire effort by leaving a security gap at the worst place possible – on the endpoint.

© 2022 Morphisec Ltd. | morphisec.com

MTD has an unparalleled ability to make ZTA endpoint security easy and effective to an equal measure. By focusing defenses on the application runtime, where most attacks seek to strike, MTD foils those attacks without needing to detect them in advance or deflect their attack. Endpoints become secure from unknown and evasive threats without needing an expansive security apparatus.

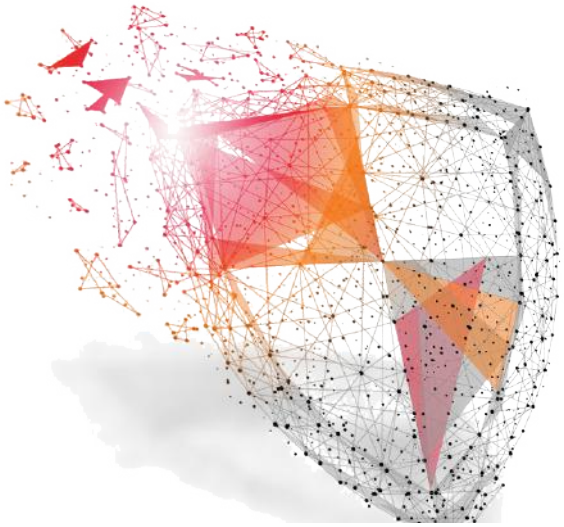
Zero Trust Architecture based on Moving Target Defense makes the final battle the hardest for attackers to win.

8 Morphisec – Pioneering the Next Era of Cybersecurity

As evasive attackers set their sights on endpoints and new breaches capture headlines, security teams must react. And they must think differently.

Morphisec, the leader in Moving Target Defense, brings innovation to endpoint security by combining ZTA techniques with patented MTD technology for desktops, VDIs, servers (e.g., Linux and Microsoft servers) and cloud workloads. It is cybersecurity defined by speed rather than strength, and smarts instead of scale. Imagine the frustration attackers experience when their carefully-laid plans lead directly into quarantine, turning victory into defeat at the very last moment. Morphisec's breach prevention solution for endpoints doesn't just embody the principles of cybersecurity ZTA; it applies them in a practical and clever way to make cybersecurity more resilient, preventative, and manageable – exactly what the future calls for.

The next era of cyber attacks has already arrived. The next era of cybersecurity needs to keep pace. Take a shortcut with MTD ZTA from Morphisec. Contact us now to see how easy threat actors can penetrate your existing NGAV, EPP, or EDR, and how effective Morphisec can be in augmenting your current security stack to stop them.



> **"Anything that is suspected of being ransomware gets blocked immediately.**
>
> — **PeerSpot Review by Morphisec Customer**

PeerSpot

> **"True Zero Day attack protection."**
>
> — **Gartner Peer Insights**

Gartner peerinsights

 © 2022 Morphisec Ltd.