Technical Reference Guide

MORPHISEC

Adaptive Cyber Resiliency Powered by Automated Moving Target Defense

By Brad LaPorte, Chief Marketing Officer and Gartner Veteran
Jay Kurup, Global Sales Engineering Director

Table Of Contents

Executive Summary

In the face of an increasingly sophisticated and dynamic cyber threat landscape, traditional cybersecurity measures are proving inadequate – the IBM Cost of a Data Breach Report for 2023 found that only one-third of reported breaches were initially detected by an organization's internal security teams and tools.

Furthermore, delays in identifying and containing breach events compromise an organization's overall resilience. According to the report, breaches discovered by an organization's security team and tools take on average 182 days to identify (or MTTI - Mean Time To Identify) and 59 days to contain (or MTTC - Meant Time To Contain). Organizations need a new approach to cybersecurity to ensure cyber resiliency.

This technical white paper introduces a revolutionary approach that not only addresses these evolving threats but also enhances organizational resilience against them. This approach leverages Morphisec's innovative technologies, including Automated Moving Target Defense (AMTD) and Anti-Ransomware Assurance, to provide a proactive, dynamic, and adaptive cybersecurity framework.

Morphisec's strategy shifts the cybersecurity paradigm from a static, reactive posture to a proactive and adaptive model. It integrates continuous monitoring, advanced analytics, automated defenses, and strategic risk management to ensure that organizations can anticipate, respond to, and recover from cyber threats effectively. This approach not only protects against immediate threats but also prepares organizations for future challenges, ensuring continuous operational continuity and safeguarding critical assets.

This technical white paper:

- Explores the factors affecting the cybersecurity landscape
- Introduces adaptive cyber resiliency strategy and required components to build and execute a cyber resiliency framework
- Provides a technical overview of Morphisec AMTD, and its application, capabilities, key use cases and performative outcomes

This white paper aims to illuminate a path towards a more secure and resilient digital future, highlighting how Morphisec's pioneering technology and strategies provide the necessary tools and insights to transform your cybersecurity posture from reactive to proactive, and from static to adaptive.

Introduction

In today's rapidly evolving digital landscape, where cyber threats are becoming more sophisticated and pervasive, traditional cyber defense mechanisms often fall short in providing the necessary protection. Organizations are increasingly vulnerable to a spectrum of cyber threats, from ransomware to advanced persistent threats, which can cripple operations, lead to significant financial losses, and damage reputations permanently. This escalating threat environment necessitates a shift towards more dynamic and adaptive cybersecurity strategies.

Morphisec's Adaptive Cyber Resiliency approach ushers in a new era of cybersecurity, designed to address these multifaceted challenges. By integrating cutting-edge technologies such as Automated Moving Target Defense (AMTD), along with comprehensive solutions like the Anti-Ransomware Assurance Suite and Adaptive Exposure Management, Morphisec not only shields organizations from attacks but also provides a resilience framework that adapts to emerging threats and evolving business needs.

The Adaptive Cyber Resiliency approach is rooted in the philosophy of not just defending against attacks but ensuring that organizations can thrive amid the uncertainties of the cyber world. Organizations can enhance their cybersecurity strategy to include resiliency against evolving threats; leveraging Morphisec's AMTD technology can foster an adaptive cyber-resilient strategy that evolves and adapts to threats in the digital landscape.

This technical white paper delves into the necessity of adopting an adaptive cybersecurity framework. It explores how Morphisec's innovative solutions empower businesses to maintain operational continuity, protect critical assets, and foster trust among stakeholders, all while managing costs effectively and ensuring compliance across diverse regulatory landscapes.

Additionally, this document will detail how Morphisec's Anti-Ransomware Assurance can diminish the blast radius of ransomware attacks by preemptively reducing exposure to risk and proactively preventing attacks at multiple phases, from early infiltration to safeguarding systems when ransomware attempts to execute, helping organizations adapt, protect and defend.

Why Organizations Need a New Approach to Cybersecurity

As digital dependency grows, the cybersecurity landscape changes rapidly, rendering traditional security measures insufficient. Modern cyber threats are increasingly sophisticated and frequent. These threats target vulnerabilities in static and reactive security systems that are reliant on signature-based detection and infrequent updates. The shift toward remote work and greater use of cloud services has expanded the attack surfaces of traditional computing environments, including Windows and Linux servers and laptops.

Traditional cybersecurity models – which focus on perimeter defense to block attackers at entry points – are proving inadequate due to the complex nature of today's IT environments and sophisticated cyber threats. This blurring of network boundaries requires a new approach to cybersecurity, and a strategy that is both adaptive and proactive, and capable of evolving in response to new threats.

Morphisec's Adaptive Cyber Resiliency approach addresses these challenges by adopting a proactive stance that uses real-time threat intelligence and advanced analytics to anticipate and respond to cyber adversaries' tactics and techniques. This strategy ensures a continually evolving defense system, providing strong protection for traditional computing platforms against an ever-changing threat landscape.

Exploring Adaptive Cyber Resiliency

Organizations must evolve their cybersecurity strategies to address the increasingly sophisticated and organized tactics of adversaries. Current strategies often rely on a reactive approach, centered on threat intelligence that informs common defense mechanisms including signatures, heuristics, and behavior analysis, and Indicators of Attack (IOA) and Indicators of Compromise (IOC).

To counter these evolving threats, a proactive and continuously evolving strategy is necessary. This will strengthen the existing security framework, making it more resilient to cyber-attacks and providing a more robust defense.

Key Aspects of an Adaptive Cyber Resilient Strategy

Continuous Monitoring – Ongoing surveillance of both internal and external attack surfaces is crucial for quickly identifying and mitigating threats.

Agility – The strategy must be flexible, allowing for rapid adaptation to changing threat landscapes using agile processes and tools.

Adaptive Security Controls – Incorporation of emerging technologies is vital for enhancing the current security measures. These technologies should complement the existing tools to build a comprehensive defense-in-depth framework.

Risk Assessments – Dynamic risk assessments should replace static measures to reflect the real-time risk landscape, aiding in timely decision-making.

Continuous Validation – Regular validation of security controls and processes is essential to maintain and improve cyber resilience.

An Adaptive Cyber Resilient architecture is designed to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources.

Detailed aspects of an Adaptive Cyber Resilient Architecture include:

1. Proactive and Predictive Security Measures

Continuous Monitoring:

This involves real-time scanning and analysis of telemetry data, network traffic, system logs, and other relevant data sources to identify unusual patterns or activities that could indicate a security threat.

Security Analytics:

This aspect focuses on leveraging security analytics that gather and analyze data from various sources worldwide. This allows organizations to predict potential attack vectors and vulnerabilities before they are exploited.

Behavioural Analysis:

By establishing a security baseline and employing behavioral analytics to detect anomalies that signify potential security incidents.

2. Automated Response and Adaptation

Automated Defenses:

Implementing systems that can automatically disrupt and respond to threats without human intervention. Not only do these systems detect threats but also automatically block malicious activities based on predefined security rules, security policy settings, and real-time analysis that can be tailored to the specific needs of an organization or its subsidiaries.

Self-healing Systems:

These systems are designed to automatically detect faults and perform necessary actions to restore functionality without human intervention, thus maintaining service continuity and operational resilience.

Dynamic Configuration Changes:

Systems and networks are set up to automatically adjust their security configurations in response to evolving threat indicators, analytics, and intelligence, ensuring that defenses remain effective under changing attack scenarios.

3. Redundancy and Resilience

Fault Tolerance:

Techniques such as redundancy, clustering, and failover are employed to ensure systems continue to operate smoothly even if some components fail.

Distributed Architecture:

Spreading out data and processing across multiple, geographically dispersed systems to minimize the impact of localized failures and attacks.

4. Risk Assessment and Management

Regular Risk Assessments:

Continuous assessments that adapt to new threats and changes in the business environment, helping organizations prioritize and focus their defensive strategies effectively.

Risk Mitigation Strategies:

Strategic application of risk handling options, including transferring risk, avoiding risk through alternative strategies, accepting some level of risk where appropriate, and mitigating risk through security measures.

5. Incident Response and Recovery

Incident Response Planning:

Developing, maintaining, and regularly testing an incident response plan that outlines roles, responsibilities, and procedures for managing and recovering from security incidents.

Rapid Recovery:

Capabilities focused on quickly restoring critical functions and services post-incident to minimize downtime and associated costs.

6. User and Entity Behavior Analytics (UEBA)

Profiling and Anomaly Detection:

Systems create and maintain baseline profiles for normal activities of users and entities, using these baselines to spot significant deviations that might indicate a breach or malicious insider activities.

7. Secure by Design

Security by Default:

Systems are configured with security as a primary consideration, minimizing the risk of misconfigurations and vulnerabilities.

Principle of Least Privilege:

Access rights are minimized to only those necessary for a specific job role, reducing the potential damage from compromised accounts.

8. Data Protection and Privacy

Encryption:

Strong encryption protocols are applied to protect data at rest and in transit, ensuring data integrity and confidentiality.

Data Rights Management:

Tools and policies are used to control who can access information and what actions they can perform with it, ensuring compliance with privacy laws and regulations.

9. Identity and Access Management (IAM)

Multi-Factor Authentication (MFA):

This security measure requires multiple forms of verification to strengthen access controls and prevent unauthorized access.

Access Controls:

Detailed policies and technologies ensure users can only access resources necessary for their roles.

Credential Theft Protection:

Implementing measures to prevent the theft of credentials, such as using secure credential storage, regularly updating and rotating credentials, and employing advanced threat detection mechanisms to identify and respond to attempts at credential theft.

10. Compliance and Standards Adherence

Regulatory Compliance:

Ensuring adherence to laws, guidelines, and standards relevant to the industry and geography in which the organization operates.

Standards Adherence:

Following recognized cybersecurity frameworks and standards, such as NIST, ISO, PCI DSS, HIPAA, GDPR, and others, to guide security practices.

11. Training and Awareness

Cybersecurity Training:

Employees are regularly trained in the latest cybersecurity threats and defensive tactics, enhancing their ability to recognize and respond to security incidents.

Security Culture:

A strong culture of security awareness is cultivated, where all employees understand their roles in maintaining and enhancing the organization's security.

Protecting the Human Firewall:

Implementing comprehensive measures to mitigate the risks associated with human error and inadvertent actions. This includes ongoing awareness programs, simulated phishing exercises, and clear, straightforward procedures for reporting suspicious activities or potential breaches. These initiatives help strengthen the organization's first line of defense–their employees–by ensuring they are vigilant and prepared to act correctly under various scenarios.

12. Collaboration and Information Sharing

Threat Information Sharing:

Engaging in partnerships with other organizations and industry groups for the exchange of information related to cyber threats and vulnerabilities, which enhances collective security intelligence and response capabilities.

Interim Security Measures:

Implementing solutions and best practices such as Virtual Patching, which provides a security policy enforcement layer to prevent the exploitation of a known vulnerability until a formal patch is released. Additionally, system hardening techniques are applied to reduce the system's attack surface by disabling unnecessary services, applying the principle of least privilege, and configuring security settings appropriately. These measures help protect against zero-day attacks and other vulnerabilities for which patches have not yet been developed.

13. Constant Evolution

Continuous Improvement:

The security architecture is not static; it undergoes continual assessment and enhancement to incorporate new technologies, address emerging threats, and refine response strategies.

By rigorously integrating these aspects, an organization can build an Adaptive Cyber Resilient Architecture that not only defends against current threats but is also agile enough to adapt and recover from future cyber events swiftly.

This approach ensures that cybersecurity measures evolve in alignment with both technological advancements and emerging threat landscapes, establishing a robust defense mechanism that promotes sustained security and trust.

Adopting AMTD for Adaptive Cyber Resilience

AMTD represents a significant shift in cybersecurity strategies. Unlike traditional security measures that typically focus on strengthening a static defense, AMTD introduces a dynamic approach, continuously altering the attack surface to confuse and deflect attackers.

Evasive threats like fileless, in-memory and ransomware attacks are becoming increasingly complex. The 2023 Verizon Data Breach Investigations Report ranks ransomware among the leading types of actions seen in breaches, as evidenced by increasing use of undetectable techniques like fileless and in-memory attacks that can slip past traditional, signature-based defense measures with ease. The latest approaches in ransomware protection emphasize not just resilience, but also the critical need for visibility and autonomous adaptability.

AMTD draws inspiration from a core military strategy: moving targets are inherently more challenging to strike than stationary ones. By orchestrating dynamic shifts or alterations within IT environments, AMTD aims to elevate uncertainty and complexity for potential attackers. This approach involves a variety of tactics, such as relocating, altering, obfuscating, or morphing attack surfaces, ultimately disrupting adversaries' cyber kill chain.

Key Features and Benefits of AMTD

Dynamic Defense Mechanisms

AMTD operates on the principle of regularly changing system configurations, IP addresses, and even code environments. This constant fluctuation makes it exceedingly difficult for attackers to find a stable target, thereby disrupting their planning and execution phases.

Proactive Security Posture

Traditional security systems often act reactively, responding to threats after they have been detected. By contrast, AMTD is inherently proactive. By continuously modifying the attack surface, it prevents attackers from gaining a foothold in the first place, which significantly reduces the chances of successful breaches.

Disruption of Attacker Methodologies

According to insights from Gartner analysts, AMTD is seen as the natural evolution in the security landscape as it directly challenges and disrupts the methodologies used by attackers. By not allowing threat actors to rely on gathered intelligence about a system, AMTD forces them to constantly start their reconnaissance from scratch, which is resource-intensive and frustrating for them.

Key Outcomes of Implementing AMTD

Integration with Existing Systems

AMTD can be integrated into existing security infrastructures, enhancing other defensive measures such as other endpoint security tools like endpoint protection platforms (EPP) and endpoint detection and response (EDR), a Security Information Event Management (SIEM), firewalls, intrusion detection systems, and anti-malware tools. This integration helps create a more robust and comprehensive defense strategy.

Cost-Effectiveness

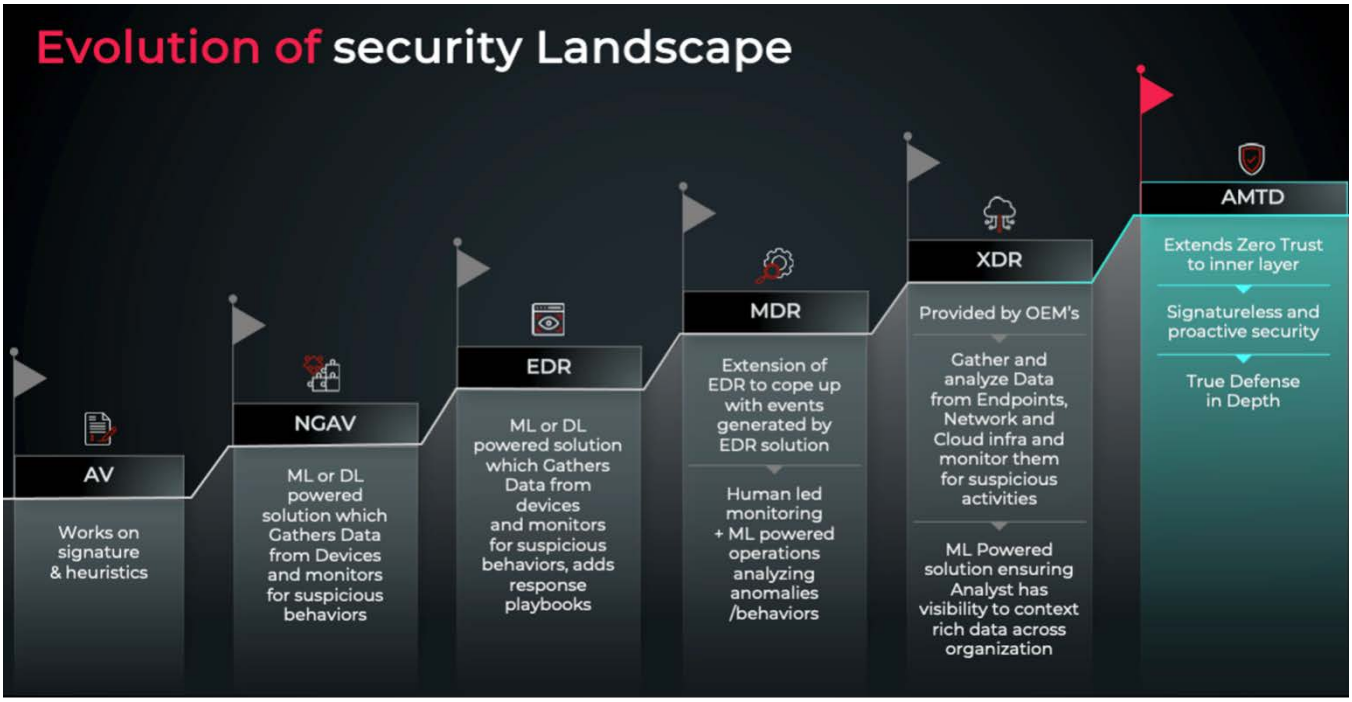
While implementing AMTD might seem resource-intensive initially, over time it proves cost-effective. By reducing the frequency and impact of security breaches, organizations can save on the costs associated with mitigating attacks and data breaches.

Compliance and Regulatory Alignment

As regulatory bodies increasingly recognize the importance of dynamic and proactive security measures, implementing AMTD can also help organizations stay ahead in compliance and regulatory matters, protecting not just their data but also their reputation.

Security Technology Innovation

The evolution of the security landscape illustrates the progressive stages in cybersecurity technologies and strategies.



Each progressive evolutionary section is described below, which collectively illustrates the evolution from traditional, signature-based antivirus software to more sophisticated, layered, and intelligent cybersecurity systems that aim to proactively defend against modern threats:

AV (Antivirus) – Antivirus solutions are the foundational elements of cybersecurity defenses. They primarily work on signature-based detection, which involves matching known malware signatures to files, and heuristic analysis, which looks for behavior or characteristics that are typical of malicious software.

Key Aspects:

- Signature-based detection
- Heuristic analysis

NGAV (Next-Generation Antivirus) – Next-Generation Antivirus uses machine learning (ML) or deep learning (DL) to improve upon traditional antivirus solutions. NGAV systems gather data from devices and monitor for suspicious behaviors, often with the capability to respond to threats in real-time.

Key Aspects:

- Machine or Deep Learning powered
- Data gathering and behavior monitoring

EDR (Endpoint Detection and Response) – EDR represents a step up in cybersecurity technology. It is also powered by ML or DL and focuses on gathering comprehensive data from endpoint devices. EDR systems not only monitor for suspicious activities but also add response mechanisms, often in the form of playbooks for addressing detected threats.

Key Aspects:

- Data collection from devices
- Real-time monitoring and response playbooks
- Machine or Deep Learning enhanced detection

MDR (Managed Detection and Response) –MDR is an extension of EDR solutions designed to manage the high volume of events generated by EDR systems. It combines human-led monitoring with ML-powered analytics to sift through and analyze the anomalies and behaviors flagged by EDR systems, providing a managed service layer on top of technology.

Key Aspects:

- Human and ML-powered analysis
- Management of events from EDR
- Focus on anomalies and behavior

XDR (Extended Detection and Response) – XDR extends the capabilities of EDR by incorporating data from not just endpoint devices but also from network and cloud infrastructures. This holistic approach allows for a wider net of surveillance for suspicious activities across an organization's entire digital footprint.

Key Aspects:

- Data integration from endpoints, network, and cloud
- OEM (Original Equipment Manufacturer) provided solutions
- Machine Learning powered for comprehensive visibility

Automated Moving Target Defense – Automated Moving Target Defense stands at the forefront of cybersecurity innovation, dynamically altering system configurations to increase complexity for attackers. This proactive strategy does not depend on recognizing known threat signatures, thereby offering a preemptive approach to security that mitigates risks before attacks can stabilize.

Key Aspects:

- Zero Trust extended to the inner layer
- Signatureless technology for proactive defense
- Multi-layered security approach
- True defense in depth

Introducing Morphisec Blast Radius Resiliency

Much like an earthquake event, damage severity radiates from a breach event's hypocenter. Morphisec fortifies your organization by diminishing the blast radius of attacks, by preemptively reducing your organization's exposure to cyber risk, proactively preventing advanced threats, and ensuring optimal anti-ransomware defense.

Powered by AMTD, Morphisec's streamlined solution effortlessly integrates with your current endpoint protection array, enhancing existing protection capabilities or operating independently when necessary.

Adaptive Exposure Management

Elevating your security posture with Adaptive Exposure Management that prioritizes vulnerabilities, automates the assessment of your security controls, identifies high-risk software, and addresses security misconfigurations.

Infiltration Protection

Enhancing your cybersecurity resilience with Morphisec's prevention-first technology that continually changes the attack surface, rendering the target unpredictable, making it harder for attackers to exploit vulnerabilities.

Impact Protection

Augmenting your cybersecurity with dedicated Anti-Ransomware protection that proactively defends critical assets and data with a prevention-first strategy, minimizing recovery times and strengthening your anti-ransomware stance.

Read more about Morphisec's Anti-Ransomware Assurance

Learn More

Key benefits include

Assurance – Gain peace of mind, knowing you're protected even when other safeguards fail, ensuring uninterrupted cyber defense.

Total Cost of Ownership (TCO) – By preventing threats as early as possible and classifying them accurately, Morphisec significantly reduces the time and costs for tech resources as well as the financial impact.

Enhanced Visibility – Morphisec sheds light on shadow IT, misconfigurations, and high-risk software, revealing critical issues that may have gone undetected, thus mitigating potential impacts on your organization.

Defense-in-Depth – The implementation of AMTD provides a multi layered defensive approach that enhances cyber-resilience against unknown evasive threats.

Improved Cybersecurity Posture – Morphisec boosts audit scores and helps in achieving compliance, which can contribute to reduced cyber insurance premiums, thus enhancing the overall cybersecurity posture.

Operational Readiness – Morphisec enhances team efficiency and effectiveness by eliminating attack dwell time and recovery efforts through proactive prevention. System hardening and virtual patching free up resources, allowing teams to concentrate on critical tasks instead of routine patching.

Additional professional services

Morphisec offers multiple professional services to support the success of its customers, together with incident response services by Morphisec's security team.

Professional services include:

Deployment & Onboarding – Quick, efficient setup for reduced risk to advanced attacks.

Concierge Services – Dedicated concierge that guarantees ideal performance and maximized platform benefits through best practices.

Incident Response – Fast, expert threat mitigation in Morphisec; minimizes cost by containing attacks and advising on prevention.

Revolutionizing Threat Exposure with Adaptive Exposure Management

Adaptive Exposure Management provides multiple layers of analytics, providing visibility, actionable insights, and recommendations to reduce your risk and fortify defenses - all tailored to your business context and unique environment.

Overview of Morphisec's Adaptive Exposure Management Features

	Description	Benefits
Software Asset Inventory	Maintains an inventory of all installed and running applications on assets.	Validates compliance and provides centralized visibility of all installed applications and hosts, ensuring visibility and control over software assets.
Vulnerability Prioritization	Offers continuous, risk-driven remediation recommendations tailored to your business context. Provides visibility to gaps in the patching process of third-party applications.	Streamlines patch management efforts and focuses resources on the greatest threats using advanced metrics including EPSS and CISA KEV listing. Quickly highlights gaps to reduce attack surface exposure, ensuring that vulnerabilities are promptly addressed.
Security Control Validation	Ensures operational and functional end-point protection solutions are in place and alerting on any deviations.	Enhances total cost of ownership (TCO) by assuring security software deployment and configuration, enabling swift response to reduce cyber risk associated with security tools, while ensuring compliance with internal policies.
High Risk Software	Identifies and prioritizes high-risk and active software on endpoints that if misused, can compromise security.	Prioritizes remediation and provides cyber risk scores to address security risks, maintaining vigilance over software that could be exploited by adversaries.
Security Misconfigurations	Regularly checks for misconfigurations within endpoint protection solutions and prioritizes configurations not compliant with security policies.	Provides greater level of cyber risk insights and recommended actions, enhancing compliance and reducing attack surface exposure through the enforcement of hardened rules and policies.

Technical Review: Automated Moving Target Defense Explained

Despite massively expanding investment in cybersecurity, damage from cyber-attacks continues to rise at an unprecedented rate. Industry standard solutions are not countering today's increasingly advanced attacks.

Morphisec identified – as early as in 2014 – the limitation of then evolving solutions against advanced fileless malwares which mimic legitimate activities to confuse the defense mechanism of the incumbent solutions and execute their code to infiltrate the organizations and create a point of persistence. Many modern cyber-attacks are highly targeted and tailored to evade and bypass specific defense layers as denoted by the following technology capabilities matrix and respective limitations.

Technology comparison

Technology	AV	EDR	XDR	AMTD
Strategy	Prevention	Detection and Response	Detection and Response	Prevention
Techniques	Signatures and Heuristics	ML or DL powered solution collect data from system and monitors for malicious or suspicious patterns	ML or DL powered solution collect data from multiple devices and monitors for malicious or suspicious patterns	AMTD
Limitations	Focused on Files introduced onto system	Alert Fatigue (review the alerts triggered by EDR)	Alert Fatigue (review the alerts triggered by EDR)	N/A
	Fileless malware/ evasive malwares	Fileless malware/ evasive malwares	Fileless malware/ evasive malwares	N/A
Offline Protection	No (Limited to available signatures)	No (Limited to available IOA/IOC's)	No (Limited to available IOA/IOC's and signatures)	Yes
Skillsets Requirement	Medium	High (Skilled researchers)	High (Skilled researchers)	Negligible

Morphisec's pioneering AMTD technology dynamically changes the attack surface to reduce attack surface exposure. This approach augments the endpoint cybersecurity stack by complementing a traditionally reactive approach with a proactive defense shield which alters the attack surface dynamically.

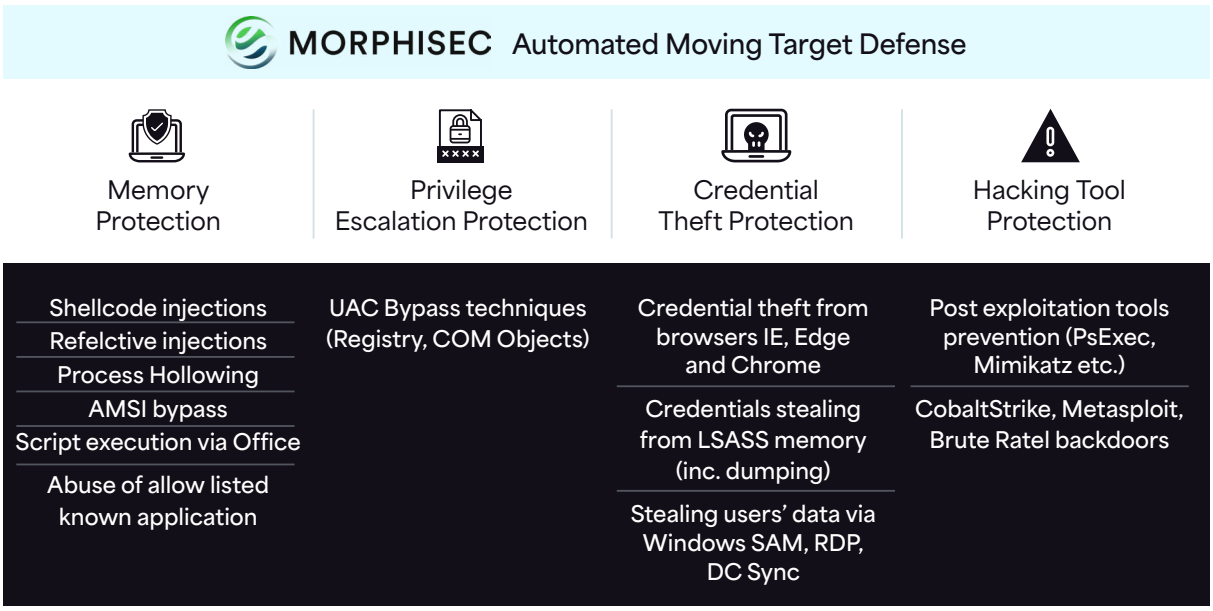
AMTD's preventive approach is particularly important given the investment attackers put into attack reconnaissance to discover vulnerabilities and the right way to exploit a victim's systems.

The Morphisec platform was initially designed to close gaps and protect against fileless attacks. Since its release, additional features have been added to the platform with the introduction of new capabilities designed to close additional gaps and fortify the security stack against evasive malware.

AMTD is an ideal defense-in-depth solution for organizations, particularly as protection from fileless attacks – this remains a weakness in existing security strategies, which rely on endpoint security solutions working on runtime.

Morphisec AMTD does not require constant updates or connectivity to cloud to provide protection, making it an ideal last line of defense.

Morphisec's Automated MTD Prevention Stack



Morphisec presents an advanced cybersecurity suite designed to protect against a multitude of threats through its AMTD technology. The stack is divided into four key protection domains: Memory Protection, Privilege Escalation Protection, Credential Theft Protection, and Hacking Tool Protection. Each domain targets specific threat vectors and tactics employed by attackers, ensuring comprehensive defense across various attack surfaces.

Memory Protection

Morphisec's AMTD technology offers robust Memory Protection by defending against:

- Shellcode Injections: Prevents the execution of malicious code injected into memory.
- Reflective Injections: Blocks the technique of injecting code that reflects the executable image from disk into the memory space.
- Process Hollowing: Stops the tactic of replacing an existing process's code with malicious code.
- AMSI Bypass: Protects against attempts to evade the Anti-Malware Scan Interface, which malware often targets for uninterrupted execution.
- Script Execution via Office: Secures against the execution of harmful scripts that can be initiated through Office applications.
- Abuse of Allow-Listed Known Application: Shields against the misuse of trusted applications to perform malicious activities.

Privilege Escalation Protection

This domain focuses on preventing unauthorized elevation of privileges:

- UAC Bypass Techniques: Thwarts attempts to bypass User Account Control (UAC) using registry and Component Object Model (COM) object manipulation, which can lead to elevated system access.

Credential Theft Protection

Credential Theft Protection safeguards sensitive user credentials by:

- Protecting Browsers: Ensures credential safety within popular browsers like Internet Explorer, Edge, and Chrome.
- Securing LSA: Shields the Local Security Authority Subsystem Service (LSASS) memory to prevent credential dumping.
- Guarding Windows Services: Defends against the theft of user data via critical Windows services such as Security Accounts Manager (SAM), Remote Desktop Protocol (RDP), and Domain Controller Synchronization (DC Sync).

Hacking Tool Protection

Morphisec combats tools commonly used in post-exploitation phases:

- Post-Exploitation Tools Prevention: Blocks tools like PsExec and Mimikatz that are known for aiding attackers in lateral movement and further exploitation after the initial breach.
- Mitigating Advanced Backdoors: Neutralizes sophisticated backdoors and penetration tools like Cobalt Strike, Metasploit, and Brute Ratel, which are often used for establishing persistent access and control over compromised systems.

Morphisec's AMTD Prevention Stack offers a comprehensive security solution that addresses critical threat vectors through advanced, proactive defenses. By focusing on the prevention of sophisticated attacks at the memory, privilege, credential, and tool levels, Morphisec ensures a high level of security for organizations against the ever-evolving landscape of cyber threats.

Closing the Gap

Morphisec's AMTD technology effectively addresses a critical security gap – often estimated at 30% – that traditional security measures fail to cover.

AMTD closes the cybersecurity gap with:

1. Prevention without Prior Knowledge – Morphisec AMTD operates independently of traditional detection methods such as signatures, rules, or Indicators of Compromise/Attack (IoCs/IOAs). This allows it to prevent attacks without needing prior knowledge of specific threats, making it highly effective against zero-day exploits and advanced persistent threats that have not yet been cataloged.

2. Proactive Automatic Protection – The solution offers proactive, automatic protection against a variety of threats, including:
   - Runtime Memory Attacks: AMTD can detect and neutralize threats that attempt to manipulate or exploit applications in memory.
   - Defense Evasion: By altering memory allocations dynamically, AMTD prevents attackers from bypassing security measures.
   - Credential Theft: It protects sensitive data such as passwords and keys from being stolen, even if attackers breach other security layers.
   - Ransomware: AMTD immediately neutralizes ransomware upon execution, preventing it from encrypting files or spreading within the network.

3. Immediate Malware Neutralization – Upon detection of malicious activity, AMTD instantly kills malware at the point of execution. This immediate response limits the potential damage and spread of the infection, safeguarding critical systems and data.

4. Minimal Impact on Performance –One of the standout features of Morphisec AMTD is its negligible impact on system resources, such as CPU and RAM. This ensures that security does not come at the expense of system performance, allowing business operations to continue smoothly without noticeable slowdowns.

5. High-Fidelity Alerts and SOC Efficiency – AMTD generates high-fidelity alerts that significantly reduce the number of false positives, which in turn decreases the workload and fatigue experienced by security analysts and Security Operations Centers (SOCs). By prioritizing responses to genuine threats, AMTD enhances the efficiency and effectiveness of incident response efforts.

6. Full Protection for Legacy Operating System– Legacy operating systems, which are often vulnerable to a wide array of exploits due to lack of updates or inherent security weaknesses, receive comprehensive protection with Morphisec AMTD. This feature is particularly valuable for organizations that, due to operational or financial reasons, must continue to rely on older technology.

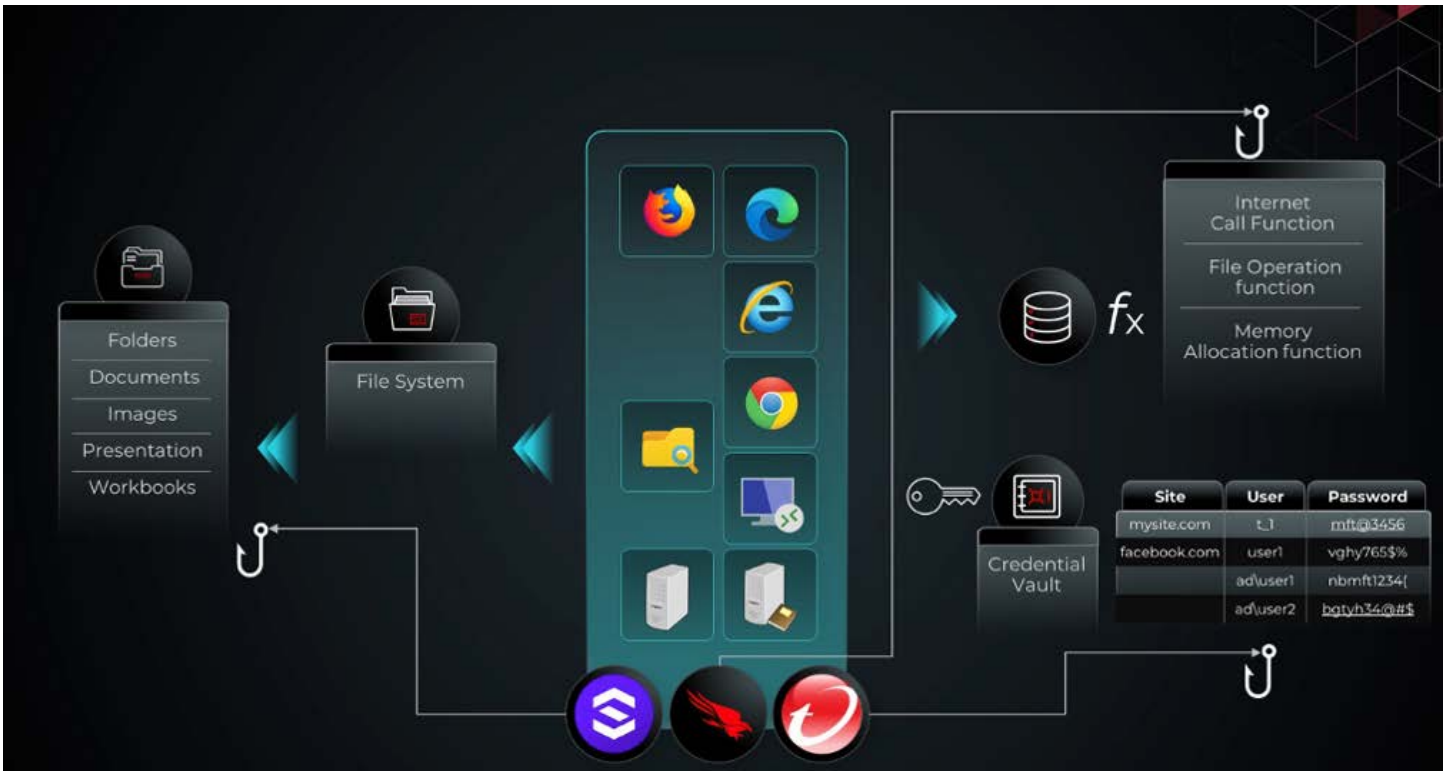
By closing the 30% gap in traditional security measures, Morphisec AMTD offers a robust and efficient solution tailored to meet the challenges of modern cyber threats. Its ability to operate without prior threat knowledge, combined with its proactive protection capabilities and minimal impact on performance, makes it an indispensable tool for safeguarding critical IT assets in a dynamic threat landscape.

Technical Application of AMTD by Morphisec

AMTD principle introduces dynamism into the static environment – which Morphisec has implemented in the runtime memory in user mode.

The guiding philosophy of this approach is to reduce business interruptions and avoid compatibility issues. This strategy has proven highly effective, as evidenced by the minimal compatibility problems encountered over a decade, during which the solution was deployed across approximately 9 million endpoints worldwide.

Logical Representation of Current Protection



The diagram above presents a logical representation of how memory, credential vault, and file-based protections are applied to an application during load time, alongside the protection offered by existing security solutions.

In this framework, the depicted hooks are conceptual tools that reroute function calls to the databases of signatures or Indicators of Attack (IOAs) that the security systems reference. These calls are then checked against known behaviors or indicators, and if a match is identified, the system takes the necessary action.

Limitations

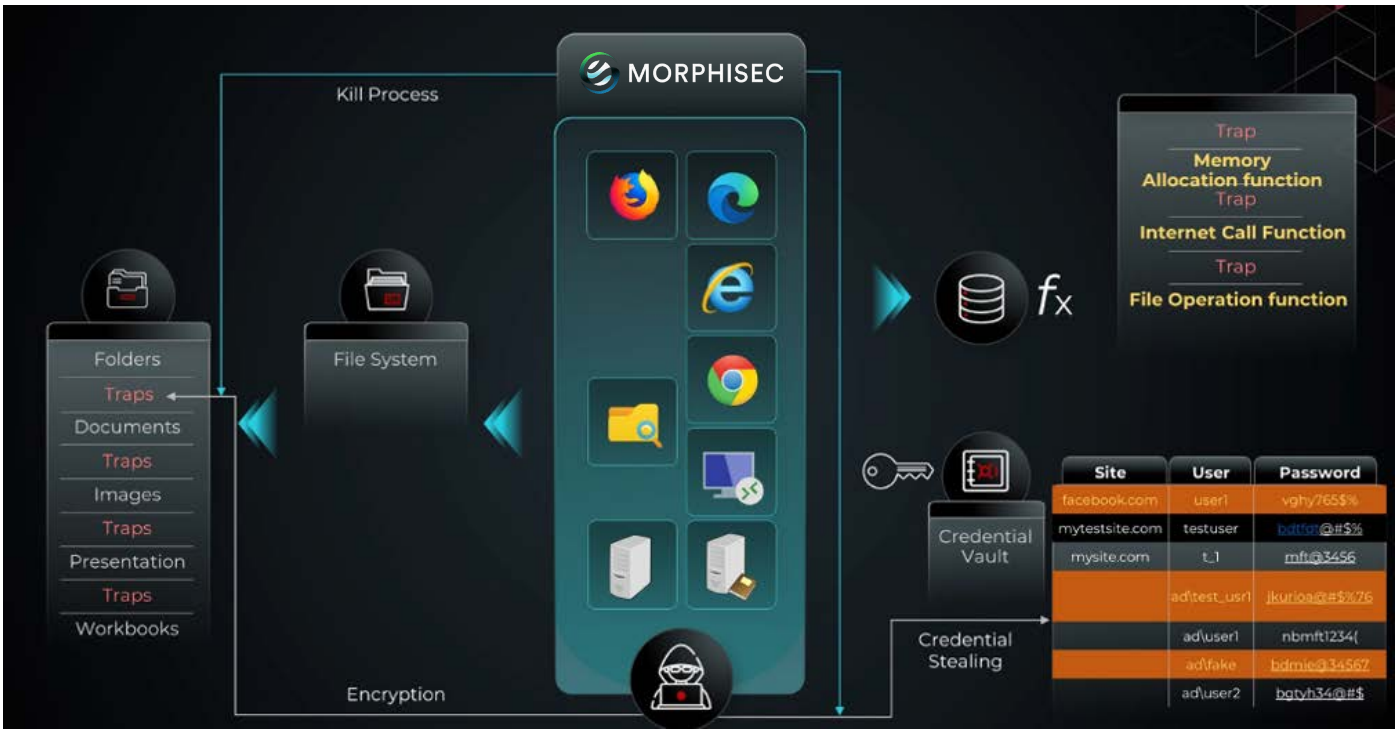
This approach faces a significant challenge in balancing effective security with maintaining business continuity:

- The inspection of calls can severely impact the application's performance and consume substantial CPU resources.
- To mitigate this, security providers typically restrict inspections to areas commonly targeted by attackers under default settings.
- Stricter security policies often result in a high rate of false positives or negatively affect application performance.
- The security measures require continual updates to keep pace with evolving attack methods.

How Attackers Bypass These Defenses

Attackers have developed methods to circumvent these defenses by using techniques that evade the hooks. For instance, they might directly reference a specific memory region to execute code, effectively bypassing the hook-based security mechanisms. Additionally, some attackers may tamper with the security solutions themselves, disabling the hooking mechanism (e.g., AMSI bypass) to execute their malicious code unimpeded.

AMTD-powered Cyber Defense



AMTD integration provides several cyber defense benefits including:

Enhanced AMTD Implementation for Cybersecurity – Morphisec's AMTD technology is a sophisticated cybersecurity measure that dynamically modifies the memory allocation of processes during load time. This state-of-the-art approach leverages a proprietary and patented technique that has earned certification from Microsoft. For a visual representation, please refer to the diagram provided above.

Dynamic Memory Allocation and Trap Deployment – At the core of AMTD's functionality is the continuous relocation of functions during the process load time. This movement is complemented by the strategic placement of traps, which substitute the original memory locations. These traps act as sentinels, deterring unauthorized access or tampering.

Broad-Spectrum Defense – Expanding its protective reach, the AMTD mechanism also fortifies sensitive areas such as credential vaults and data repositories. By doing so, it offers a robust defense against credential theft and shields data from destruction or encryption by ransomware.

Unlike traditional security measures that rely on symmetric or asymmetric cryptographic keys, AMTD employs a unique one-time randomization technique. This randomization occurs every time a process is loaded, which significantly complicates any adversarial attempt to tamper with or evade the system's defenses.

Independent and Efficient Security – Key to Morphisec's approach is the independence of AMTD from conventional hook-based systems or the requirement for an Indicator of Attack (IOA) or signature database. This self-sufficient mechanism focuses solely on dynamic structural alteration at load time, positioning it as an exemplary defense-in-depth solution.

By disrupting the very framework attackers rely upon for evasive tactics, AMTD effectively raises the cost and complexity of launching a successful attack.

Complementary to Existing Security Measures – Morphisec's protection is designed to augment current security systems, ensuring that they continue to operate effectively without interference. This integration enhances the overall resilience of an organization's cybersecurity infrastructure.

Advantages of AMTD include:

- A proactive, preventive approach to endpoint cyber defense
- Early-stage attack prevention, enhancing system resiliency
- Signature-less operation, eliminating reliance on known threat databases
- Virtual patching capabilities to address in-memory vulnerabilities
- Zero-day defense against previously unknown threats
- A robust Anti-Ransomware Shield to prevent data encryption and loss

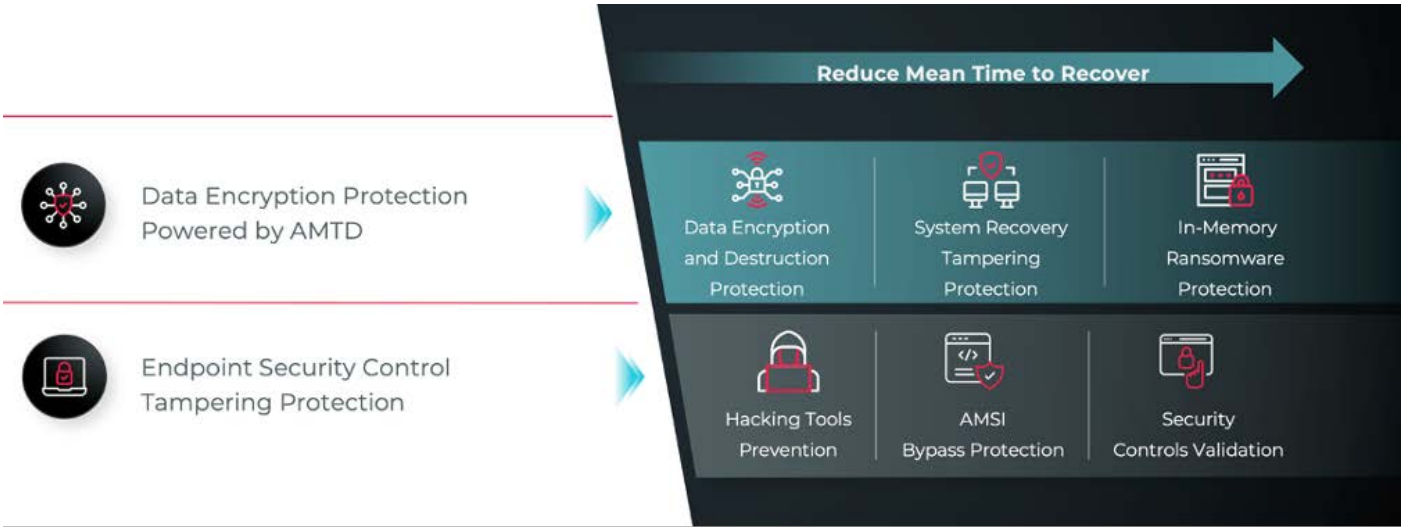
Morphisec's AMTD provides a proactive, sophisticated layer of security designed to preemptively neutralize threats, enhance system resilience, and offer invaluable insights into adversarial tactics, all while seamlessly complementing and strengthening existing security protocols.

Impact Protection

AMTD-powered Impact Protection offers organizations a credible shield against ransomware defense. The solution is designed to mitigate the destruction of data by preventing the encryption process at a very early stage thereby reducing the mean time to recovery.

The solution offers tampering protection of endpoint security controls which further enhances the resiliency of the cybersecurity stack.

At the heart of the solution is Morphisec's patented technology that deploys decoy files which when triggered will kill the encryption process. This approach is found to be highly effective against the most dangerous ransomware in the wild.



The impact protection framework consists of several defensive layers, each contributing to a robust security posture:

Data Encryption Protection Powered by AMTD – The foundational layer focuses on protecting data through encryption, ensuring that even if data is accessed unauthorizedly, it is unreadable and secure.

Endpoint Security Control Tampering Protection – This layer safeguards the security controls on endpoints, preventing malicious actors from disabling or altering the security measures that are in place.

System Recovery Tampering Protection – This critical layer ensures that recovery systems cannot be tampered with, which is vital for restoring operations after an incident without interference from attackers.

Hacking Tools Prevention – Proactively prevents the use of common hacking tools that could be used to exploit vulnerabilities, thus reducing the risk of a successful breach.

AMSI Bypass Protection – Protects against attempts to bypass the Anti-Malware Scan Interface (AMSI), a Windows security feature that allows applications to integrate with antivirus software.

Security Controls Validation – The final layer before in-memory ransomware protection, this ensures that all security controls are functioning correctly and are in compliance with policy requirements.

The entire system is designed to decrease the mean time to recover from an incident, ensuring that the impacts of any breaches are minimized and normal operations can be resumed quickly.

In Conclusion

As cyber threats continue to evolve in complexity and frequency, it is imperative for organizations to adopt a cybersecurity strategy that is as dynamic as the threats it aims to combat.

Morphisec's Adaptive Cyber Resiliency approach provides a comprehensive solution that not only defends against current cyber threats but also adapts to future challenges. This strategy empowers organizations to not just survive but thrive in the digital era, maintaining trust among stakeholders and ensuring compliance across regulatory frameworks.

As organizations increasingly depend on digital infrastructures, the cybersecurity landscape becomes not just a technical battleground, but a critical business continuity concern. Traditional security measures, while foundational, are no longer sufficient in isolation due to their reactive nature and limitations in dealing with sophisticated, evolving cyber threats. Morphisec's Adaptive Cyber Resiliency framework marks a paradigm shift in how cybersecurity is approached and implemented in corporate environments.

This technical white paper thoroughly reviewed the limitations of conventional cybersecurity strategies, emphasizing the necessity for a system that is not only robust but also flexible and forward-thinking. Morphisec's Adaptive Cyber Resiliency approach, with its core components like AMTD and Anti-Ransomware Assurance, represents an advanced cybersecurity architecture. This architecture is designed to dynamically adapt to new threats, thereby not just responding to incidents but actively preventing them.

This approach is built on several pillars essential for a comprehensive cybersecurity strategy: continuous monitoring for real-time threat detection, agility in deploying adaptive security measures, and comprehensive risk assessments that inform proactive defenses. Additionally, the integration of advanced technologies such as behavior analytics and automated response mechanisms ensures that the security posture of an organization evolves continuously to outpace potential attackers. Moreover, implementing Morphisec's strategy enhances an organization's resilience, enabling it to withstand and quickly recover from cyber incidents while minimizing operational disruptions and financial losses. This resilience is crucial for maintaining stakeholder trust and protecting the brand reputation in a digital-first world.

The current era equates the cost of cyber breaches through financial and larger reaching business impacts. As such, it is imperative that adaptive strategies be adopted. Adopting Morphisec's Adaptive Cyber Resiliency not only prepares organizations to defend against current cyber threats but also equips businesses with the agility to adapt to future challenges. This shift from a static, reactive posture to a dynamic, proactive stance is essential for any modern enterprise aiming to thrive in an increasingly complex digital landscape.

How Morphisec Can Help

Decision-makers and IT leaders are urged to recognize the strategic importance of cybersecurity and to view it as a dynamic and integral part of their overall business strategy.

Contact Morphisec today to discuss how our Adaptive Cyber Resiliency approach can be integrated into your security architecture. Let Morphisec help you transform your cybersecurity defenses from a cost center into a strategic asset that not only protects but also adds value to your organization.

Embrace the future of cybersecurity with Morphisec and ensure your organization is equipped to navigate the digital threats of tomorrow. Secure your operations, protect your assets, and ensure your competitive edge in the digital age.

Morphisec AMTD protects more than 9 million devices across more than 7,000 organizations, routinely preventing ransomware and highly evasive attacks that bypass leading endpoint protection solutions, including EDR/XDRs.

Connect with Morphisec's panel of experts to see how you can tailor a cybersecurity solution that fits your unique organizational needs today, and as you embark on your journey towards a secure and resilient digital infrastructure.

Gartner Disclaimer

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About Morphisec

Founded in 2014, Morphisec, a pioneer in blast radius resiliency, keeps your business safe by intelligently anticipating and neutralizing threats - minimizing the impact and blast radius of cyber incidents and ensuring uninterrupted business operations without the need for constant tech team intervention or impact to performance.

Powered by Automated Moving Target Defense (AMTD) technology, the next evolution of cybersecurity, Morphisec protects over 7,000 organizations across nine million Windows and Linux endpoints, servers and workloads. Morphisec stops thousands of advanced attacks daily at Lenovo/Motorola, TruGreen, Cipla, Citizens Medical Center, and many more. Learn more at www.morphisec.com