MORPHISEC

Whitepaper

Achieving Adaptive Cyber Resiliency With Automated Moving Target Defense

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.

Attackers continuously iterate and innovate attack techniques to stay one step ahead of defensive tools and technologies. Many techniques aren't new – rather attackers, always seeking the fastest path to access, are finding success in iterating on classic methods.

For example, the Verizon 2024 Data Breach Investigations Report (DBIR) found that vulnerability exploitation for initial breach entry nearly tripled in 2023, increasing 108%. In many cases attackers can exploit breaches faster than teams can patch them. According to the DBIR it takes organizations approximately 55 days to address vulnerabilities, while large-scale scanning for those same vulnerabilities by threat actors starts within five days.

Once initial access is established, attackers can initiate dangerous and undetectable attacks like ransomware and pure extortion attacks – the DBIR found the latter grew year-over-year, representing 9% of breaches in 2023.

A current state of omni-present risk means that security leaders must shift from a reactionary mindset to a preventative one. Adopting an adaptive cyber resiliency strategy mitigates the danger of cybersecurity complacency, helping leaders and their teams speed breach event response, contain breach damages and return to business as usual faster.

This white paper:

- Explores the changing threat landscape and top-of-mind use cases
- Introduces adaptive cyber resiliency strategy and how adaptive exposure management can support it
- Provides a technical overview of Morphisec's pioneering Automated Moving Target Defense (AMTD) technology, its application, capabilities and performative cyber resiliency outcomes

Introduction

The DBIR breach data reinforces that popular attack techniques are increasingly initiated through vulnerability exploitation. “Set and forget” detection and response strategies and technologies are failing to stop the attacks that ensue.

Security leaders, acutely aware of increasing risk, are re-assessing their organization’s overall security posture. And regardless of size, scope or industry, three central and supporting use cases have emerged:

1. Ransomware Ransomware looms large for organizations due to its multifaceted threats. These attacks hold critical data and systems hostage, causing severe disruptions and financial losses. Beyond operational standstills, ransomware tarnishes reputations, erodes customer trust and risks business losses. Modern ransomware tactics use increasingly sophisticated fileless and in-memory techniques that can evade industry-standard detection and response technologies.

2. An expanding attack surface Many factors are continually warping and expanding every organization’s attack surface. The adoption of cloud services and Software-as-a Service (SaaS) solutions diversifies potential entry points for attackers. The surge in remote and hybrid work models introduces vulnerabilities as employees access systems from varied networks and devices while the proliferation of Internet of Things (IoT) devices on corporate networks amplifies risks of compromise and lateral movement. Additionally, extensive reliance on third-party integrations raises concerns over security inconsistencies and overlooked vulnerabilities.

3. Security control gaps Outdated and unpatched systems harbor vulnerabilities ripe for exploitation by attackers. Insufficient access controls, marked by weak authentication and authorization measures, open the door to unauthorized access to critical systems and data. Any lack of robust endpoint protection leaves user devices vulnerable to malware infections, while ineffective detection and response mechanisms permit breaches to linger undetected, granting attackers prolonged access. Additionally, inadequate employee training heightens risks, as uninformed staff become susceptible to phishing attacks and mishandle sensitive information.

Overall reliance on digital systems is fueling the cybersecurity landscape’s rapid evolution and its ability to outpace traditional security measures. Today’s cyber threats, while rooted in classic methods, are highly sophisticated and adept at exploiting weaknesses in static and reactive security protocols that rely on signature-based detection and sporadic updates.

The inadequacy of perimeter-focused cybersecurity models, combined with the complexity of threats, demands a shift towards adaptive and proactive strategies capable of evolving alongside the ever-changing threat landscape.

Exploring Adaptive Cyber Resiliency

For security leaders, refining cybersecurity strategies in response to the escalating sophistication of adversaries' tactics is key to defending against them. Traditional strategies tend to adopt a reactive stance, emphasizing threat intelligence to inform conventional defense mechanisms like signatures, heuristics, behavior analysis, and Indicators of Attack (IOA) and Indicators of Compromise (IOC).

Yet to effectively counter advancing threats, a proactive and perpetually evolving adaptive cyber resiliency strategy is imperative. Such an approach fortifies an organization's overall security (and defense) posture against cyber-attacks.

Key aspects of an Adaptive Cyber Resiliency strategy include:

Continuous Monitoring	Ongoing surveillance of both internal and external attack surfaces is crucial for quickly identifying and mitigating threats.
Agility	Flexibility, allowing for rapid adaptation to changing threat landscapes using agile processes and tools.
Adaptive Security Controls	Incorporation of emerging technologies to enhance current security measures. These technologies should complement the existing tools to build a comprehensive defense-in-depth framework.
Risk Assessments	Incorporation of emerging technologies to enhance current security measures. These technologies should complement the existing tools to build a comprehensive defense-in-depth framework.
Continuous Validation	Regular validation of security controls and processes to maintain and improve cyber resilience.

An Adaptive Cyber Resiliency 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 Resiliency architecture cover:

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

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.
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.
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.
Secure 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.
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.

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.
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.
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.

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.
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 Resiliency 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 and continuous security and trust.

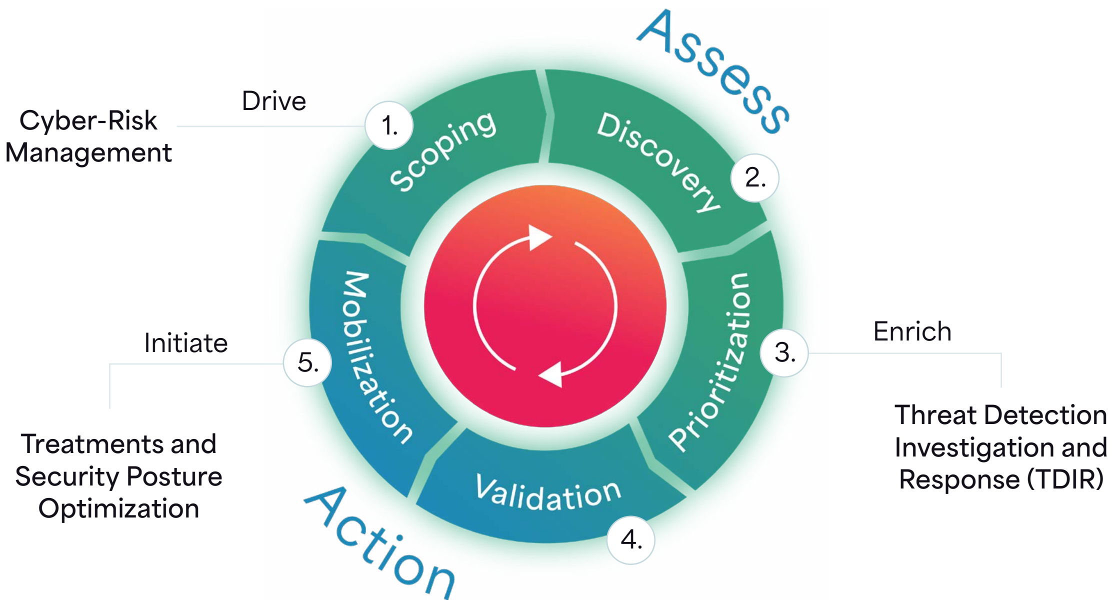
Continuous Threat Exposure Management

Managing and mitigating an organization's exposure to threats in real-time and on a continuous basis is a key component of adaptive cyber resiliency. Exposure management – mitigating risk related to digital assets, data access and vulnerabilities – directly impacts an organization's attack surface. Continuous Threat Exposure Management (CTEM), a term coined by Gartner, is an approach aimed at identifying, assessing, and remedying attack paths and security risks associated with digital assets. In application, CTEM helps cybersecurity practitioners minimize vulnerability risk by identifying vulnerable systems, ensuring security controls are working properly and understanding which remediation actions to prioritize.

A full CTEM cycle defines five key stages:

- Scoping – Aligning assessments to key business priorities and risk.
- Discovery – Identifying various elements within and beyond the business infrastructure that could pose risks in a comprehensive way.
- Prioritization – Identifying threats with the highest likelihood of exploitation and flagging which could have the most significant impact on the organization.
- Validation – Validating how potential attackers could exploit identified vulnerabilities or exposures.
- Mobilization – Ensuring all stakeholders are informed and aligned toward risk remediation and measurement goals.

Continuous Threat Exposure Management



Gartner says: “Continuous threat exposure management (CTEM) is an umbrella program for forward-looking and sustainable approaches to exposure reduction. Implementing CTEM enables closer alignment to business needs and risk impact. CTEM involves business leadership in identifying key assets and processes to defend against cyberattacks/business disruption.”[1]

Positioned as a top 2024 cybersecurity priority, CTEM adoption is underscored by Gartner’s assertion that “organizations prioritizing security investments through a continuous exposure management program are three times less likely to suffer from a breach.”[2]

However, for IT and security teams managing limited resources, inefficient processes, and copious data influxes, pinpointing and prioritizing the most vulnerable digital assets is a challenge. This is evident, and reflected in recent breach data that attributes delayed patching and remediation as a conduit for vulnerability exploitation.

While teams rely on vulnerability scanners, penetration testing, patch management systems, threat intelligence feeds, and asset inventory and management solutions for exposure management, they lack the proactive and preventative capabilities necessary to comprehensively assess their unique attack surface and efficiently prioritize vulnerability remediation efforts.

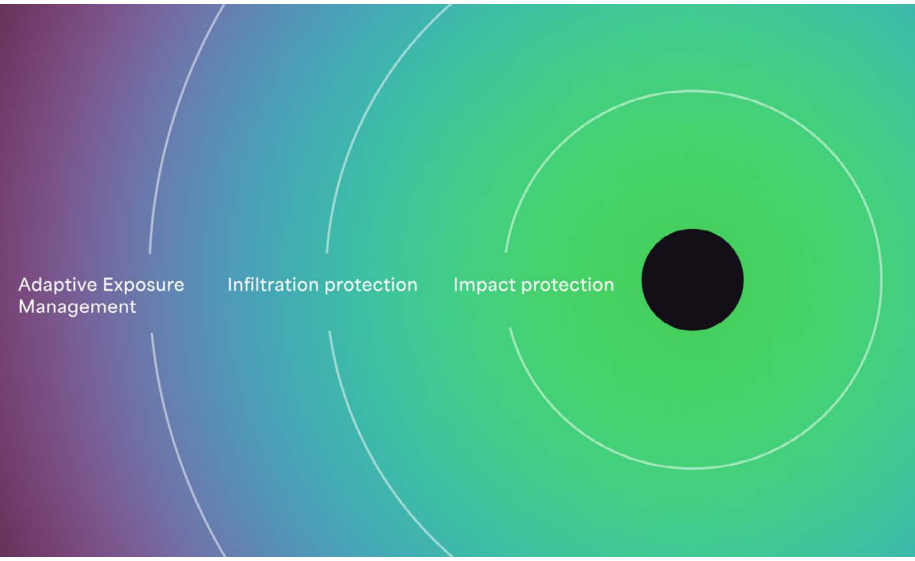
[1] Gartner: Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management, Published 16 October 2023, Jeremy D’Hoinne, Pete Shoard, [2] Gartner: Implement a Continuous Threat Exposure Management (CTEM) Program, Published 11 October 2023

Introducing Adaptive Exposure Management Powered by AMTD

An adaptive approach to exposure management elevates an organization’s overall security posture and pre-emptively defends against attacks. Tactically, Morphisec’s Adaptive Exposure Management prioritizes vulnerabilities, automates the assessment and validation of an organization’s security controls, identifies high-risk software, and addresses security misconfigurations.

Adaptive Exposure Management uncovers blind spots lurking in enterprise environments. Powered by Automated Moving Target Defense (AMTD), it provides multiple layers of analytics, providing visibility, actionable insights and recommendations to reduce risk and fortify defenses – all tailored to an enterprise’s business context and unique environment.

- Vulnerability Prioritization
- Security Controls Validation
- High Risk Software
- Security Misconfigurations



Evasive threats like fileless, in-memory and ransomware attacks are becoming increasingly complex; 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.

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.

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.

Despite continued investments in cybersecurity tooling, 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	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.

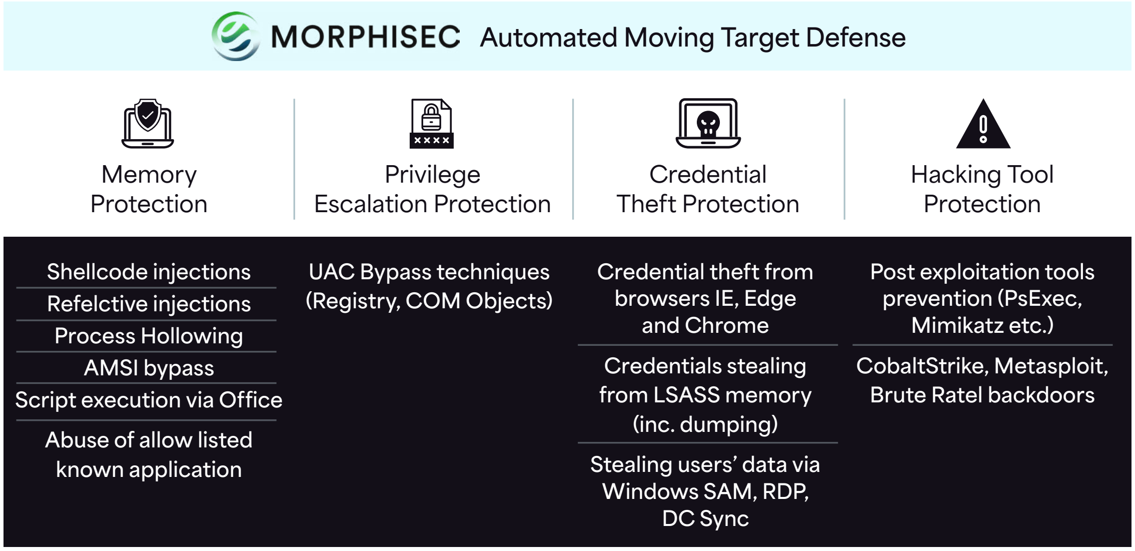
AMTD's preventive approach is particularly important given the investment attackers put into attack reconnaissance to discover vulnerabilities and the right way to exploit a victim's systems.

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 Automated Moving Target Defense

Memory Protection	Privilege Escalation Protection	Credential Theft Protection	Hacking Tool Protection
Shellcode injections Refelctive injections Process Hollowing AMSI bypass Script execution via Office Abuse of allow listed known application	UAC Bypass techniques (Registry, COM Objects)	Credential theft from browsers IE, Edge and Chrome Credentials stealing from LSASS memory (inc. dumping) Stealing users' data via Windows SAM, RDP, DC Sync	Post exploitation tools prevention (PsExec, Mimikatz etc.) CobaltStrike, Metasploit, Brute Ratel backdoors

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.

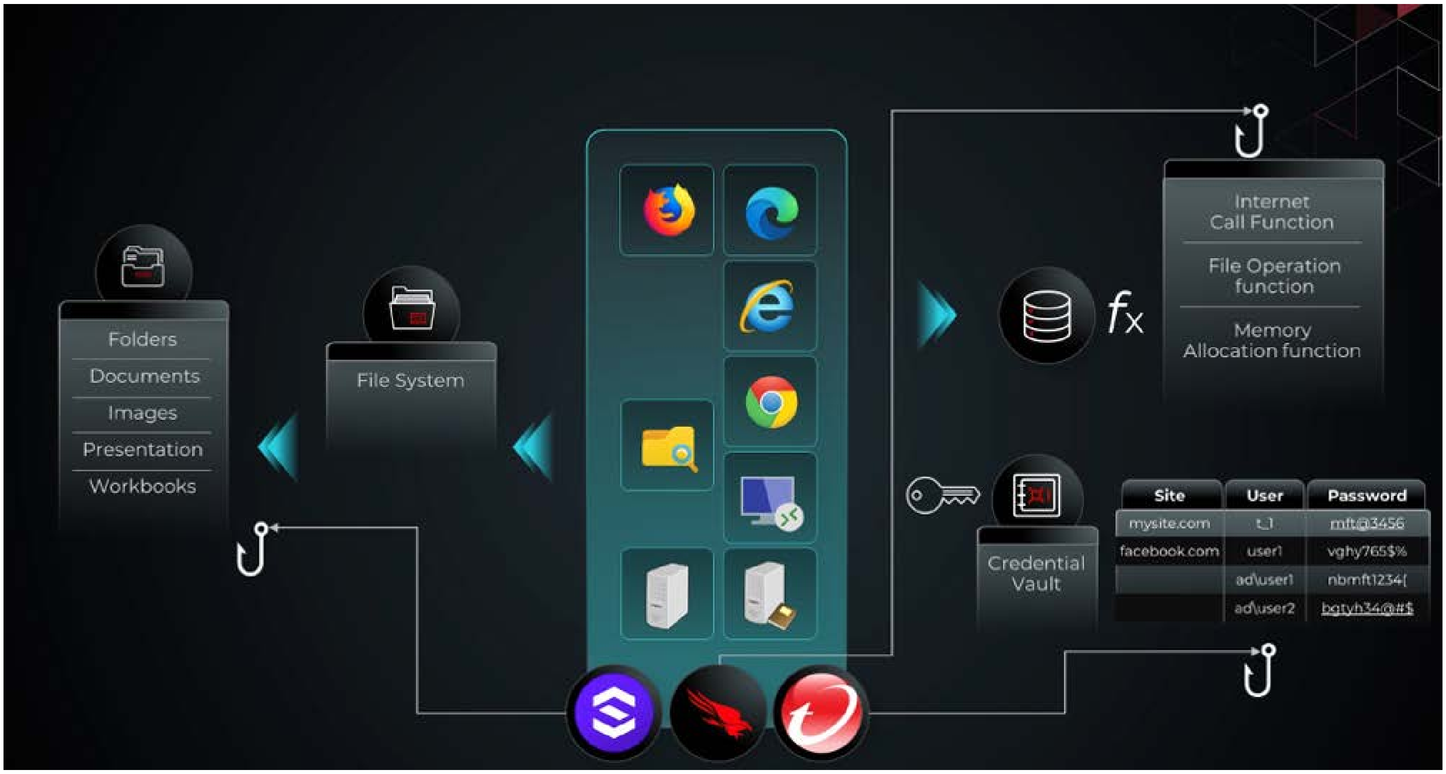
Morphisec's AMTD Prevention Stack offers a comprehensive security solution that addresses critical threat vectors through advanced, proactive defenses. By focusing on the prevention of sophisticated attacks at the memory, privilege, credential, and tool levels, Morphisec ensures a high level of security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

AMTD Technical Application Review

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



Site	User	Password
mysite.com	t_1	mft@3456
facebook.com	user1	vghy765$%
	ad\user1	nbmft1234[
	ad\user2	bgtyh34@#$

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

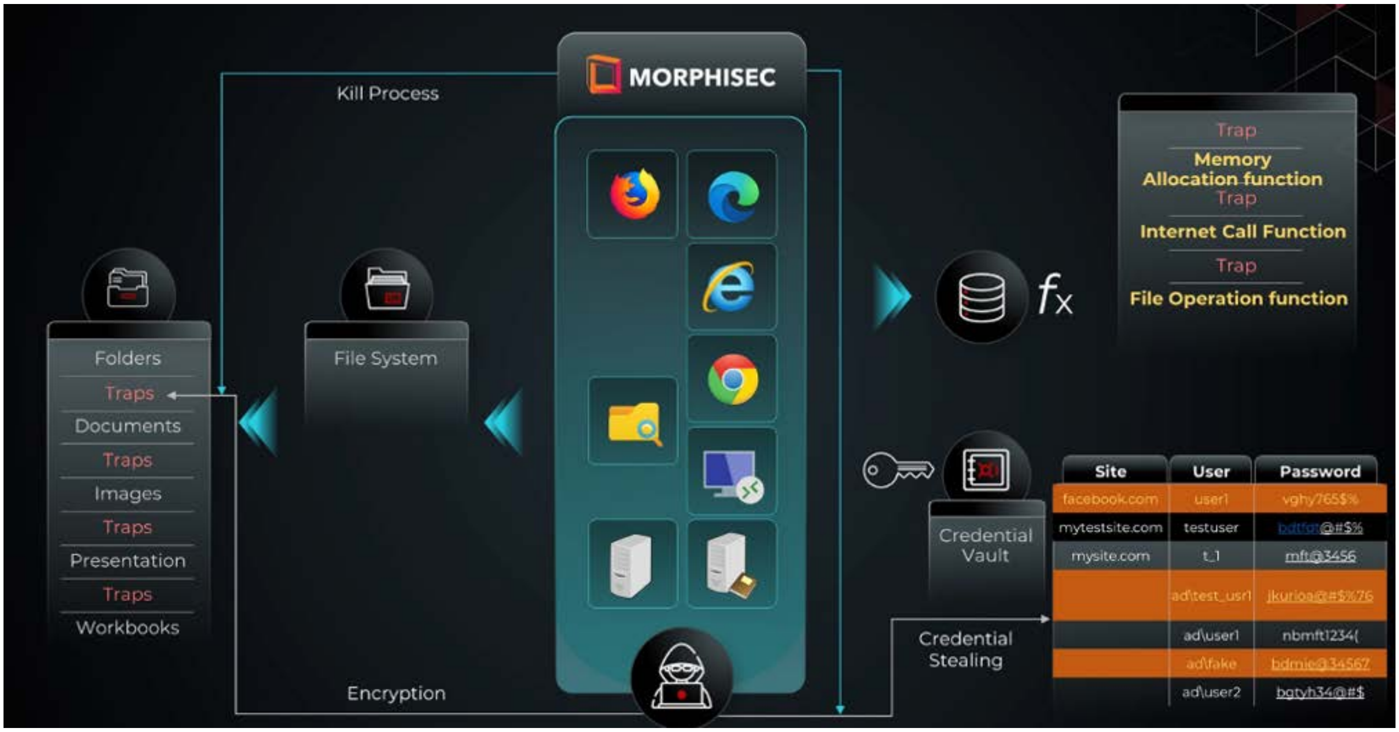
This approach faces a significant challenge in balancing effective security with maintaining business continuity:

- 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



Site	User	Password
facebook.com	user1	vghy765$%
mytestsite.com	testuser	bdtfot@#$%
mysite.com	t_1	mft@3456
	ad\test_usr1	jkurioa@#$%76
	ad\user1	nbmft1234(
	ad\fake	bdmie@34567
	ad\user2	bgtyh34@#$

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

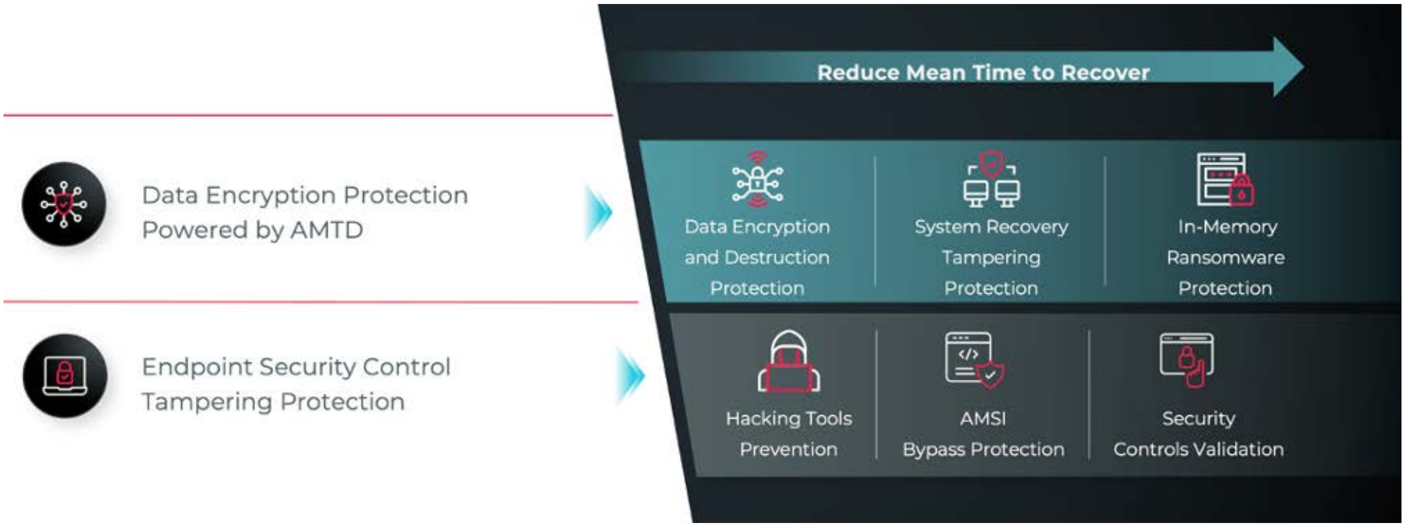
Morphisec's AMTD provides a proactive, sophisticated layer of security designed to preemptively neutralize threats, enhance system resilience, and offer invaluable insights into adversarial tactics, all while seamlessly complementing and strengthening existing security protocols.

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.


Reduce Mean Time to Recover
Data Encryption Protection Powered by AMTD
Data Encryption and Destruction Protection
System Recovery Tampering Protection
In-Memory Ransomware Protection
Endpoint Security Control Tampering Protection
Hacking Tools Prevention
AMSI Bypass Protection
Security Controls Validation

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.

Conclusion

As cyber threats continue to evolve in complexity and frequency, organizations must adopt a cybersecurity strategy 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.

By integrating cutting-edge technologies such as 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 cyber resiliency framework that adapts to emerging threats and evolving business needs.

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. It addresses key 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. Supported by Morphisec's pioneering AMTD technology, this strategy ensures a continually evolving defense system, providing strong protection for traditional computing platforms against an ever-changing threat landscape.

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. See Morphisec in action – book a personalized demo today.

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.

See how Morphisec can complement your Microsoft Defender for Endpoint investment – book a demo today.

MORPHISEC

See Morphisec in action

Stop ransomware with our
Preemptive Cyber Defense Platform

Get a demo

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

To learn more, visit morphisec.com/demo