MORPHISEC

Data Sheet

Anti-Ransomware Assurance Suite

Identity Risk Exposure

Expose and Prioritize Identity-Based Risks Before Ransomware Turns Trusted Accounts into Attack Vectors

Ransomware actors increasingly exploit identities—not just endpoints—to infiltrate, escalate, and persist within enterprise environments. Dormant accounts, misconfigured privileges and overlooked local admin credentials create invisible attack paths that traditional security stacks often miss.

These identity exposures allow adversaries to blend in as trusted users, hijacking privileges to access file servers, SQL databases, and even domain controllers. Without clear visibility into identity risks and anomalous access patterns, organizations are left vulnerable to stealthy lateral movement and privilege escalation—the very tactics that power today's most damaging ransomware campaigns.

Introducing Morphisec Identity Risk Exposure

Available as part of Morphisec's Anti-Ransomware Assurance Suite, the Identity Risk Exposure module provides unparalleled visibility into identity-based vulnerabilities, empowering organizations to proactively detect and mitigate risks that ransomware threat actors and groups exploit.

By monitoring anomalies in account behavior and access patterns, the module helps prevent identity theft, privilege escalation, and lateral movement—common tactics in ransomware attacks.

Anomaly Detection in Account Behavior

Continuously monitors logged-in accounts, access sessions and privilege usage to uncover risks invisible to standard identity tools.

Dormant Logon Account Identification

Detects accounts active for days without logoff, correlating them with executed processes to highlight potential hijacked identities.

Domain Account Reconnaissance Protection

Identifies and prioritizes domain accounts with broad server access, often targeted by attackers for elevated privileges and lateral movement.

Local Admin Account Monitoring

Provides visibility into non-domain local admin accounts, including reused credentials across servers, to prevent credential spraying and NTLM token theft.

Backdoor Account Detection

Flags recently generated or enabled local admin accounts to quickly expose threat actor persistence mechanisms.

Critical Application Account Mapping

Maps accounts executing high-privilege applications (e.g., SQL, deployment accounts) for proactive anomaly detection and prioritized risk assessment.

Critical Device Access Monitoring

Tracks high-privilege accounts accessing sensitive devices such as Domain Controllers, SQL databases, and IIS servers, exposing risky patterns attackers' exploit.

Key Benefits of Network Service Discovery

Eliminate Identity Blind Spots

Gain visibility into identity risks and anomalous behavior often overlooked by traditional monitoring solutions.

Prevent Privilege Escalation

Stop attackers from exploiting dormant or misconfigured accounts to gain elevated access to critical systems.

Reduce Lateral Movement Paths

Identify accounts with broad or risky access before attackers can use them to move deeper into the network.

Detect Hidden Backdoors

Uncover unauthorized local admin accounts created by threat actors for persistence and re-entry.

Safeguard Critical Applications and Devices

Protect the "crown jewels" of your environment–databases, file servers, and domain controllers–from account-based compromise.

Strengthen Ransomware Resilience

Proactively address identity exposures, closing one of the most common pathways for ransomware propagation and escalation.

How It Works

Morphisec's Network Service Discovery utilizes our efficient agent to provide thorough network visibility with minimal impact. Here's the step-by-step process:

1. **Telemetry Collection:** The Morphisec Agent gathers data from logon events and every application executed on servers. This includes accounts without Service Principal Names (SPNs) and non-domain accounts with high privileges, ensuring no blind spots in local or domain environments.
2. **Mapping and Analysis:** Using the collected telemetry, the agent creates a detailed map of account activities, access patterns, and privileges. Identifying anomalies such as dormant sessions, broad access, recent creations, and high-risk executions tied to critical applications or devices. .
3. **Prioritization and Dashboard Presentation:** Risks are prioritized based on severity, representative of the potential for lateral movement or privilege escalation. The intuitive dashboard displays actionable insights, including correlated processes, server access, enabling security teams to investigate and remediate quickly.

Identity Risk Exposure from Morphisec empowers your team to monitor and mitigate identity risks in real-time, fortifying your defenses against sophisticated ransomware attacks.

“Morphisec prevents attacks from actually happening. It gives us an early warning sign...and that lets me make informed, intelligent decisions.”

Richard Rushing, CISO at Motorola

Morphisec offers the only solution that combines future-ready AEM and AMTD to deliver a prevention-first strategy against ransomware that’s backed by a

100% Ransomware-Free Guarantee.

Adaptability is key to resilience – **schedule a demo** to see how AEM and AMTD can help your business stay one step ahead of diverse and unpredictable cyber threats.

Get a demo

About Morphisec

Morphisec is the trusted global leader in prevention-first Anti-Ransomware protection, redefining cybersecurity with our industry-leading Automated Moving Target Defense (AMTD) technology. Our solutions are trusted by over 7,000 organizations to protect more than 9 million endpoints worldwide, stopping 100% of ransomware attacks at the endpoint and safeguarding businesses against the most advanced and dangerous threats, including zero-day exploits and ransomware. Shrink your attack surface faster to prevent ransomware entry. Eliminate blind spots across complex environments that attackers exploit for ransomware campaigns.

At Morphisec, we don’t just fortify defenses – we proactively prevent attacks before they happen, delivering unmatched protection and peace of mind to our customers. With our Ransomware-Free Guarantee and commitment to Preemptive Cyber Defense, we set the standard for accountability and innovation in the fight against modern cybercrime.

To learn more, visit morphisec.com/demo