MORPHISEC

Data Sheet

Anti-Ransomware Assurance Suite

Network Service Discovery

Expose and Prioritize Hidden Network Risks Before Ransomware Can Exploit Them

Ransomware groups don't break in through the front door—they exploit hidden cracks in the network. Unmonitored services, exposed ports, and overlooked connections give attackers the footholds they need to gain initial access, move laterally, and escalate their reach undetected. Yet most organizations lack visibility into these exposures from the endpoint perspective, leaving blind spots where ransomware can quietly map, probe, and exploit critical services. Without the ability to identify and prioritize these risks, IT and security teams are left reacting after attackers are already inside.

Introducing Morphisec Network Service Discovery

Morphisec's Network Service Discovery is a pivotal capability Adaptive Exposure Management capability, available as part of Morphisec's Anti-Ransomware Assurance Suite.

This advanced capability delivers deep visibility into network exposures from the endpoint perspective, enabling organizations to identify and prioritize vulnerabilities that ransomware attackers commonly exploit for initial access, propagation and reconnaissance. By mapping and prioritizing established connections and listening ports, Morphisec helps prevent unauthorized entry, lateral movement, and service exploitation—key stages in ransomware campaigns.

Deep Endpoint-Based Visibility

Maps established connections and listening ports from the endpoint perspective, uncovering network exposures often invisible to traditional security stacks.

Port-to-Application Mapping

Correlates listening ports with applications and devices, tying them directly to running processes for clear context on what's exposed.

Prioritized Risk Assessment

Evaluates exposures by severity and relevance to ransomware techniques, highlighting the most critical risks to address first.

Standard Port Detection

Identifies commonly exploited ports such as SSH (22), FTP (21), SMB (445), HTTP (80/8080), HTTPS (443), and SQL Server (1433), and provides visibility into their associated applications and services.

Non-Standard Port Discovery

Detects critical services running on non-standard ports, where attackers use enumeration to uncover hidden high-value targets.

Exposure Mapping Across Devices

Links exposures across applications, endpoints, and devices to reveal potential lateral movement paths and high-value assets.

Key Benefits of Network Service Discovery

Close Critical Blind Spots

Shine a light on network exposures that attackers exploit for reconnaissance, lateral movement, and service exploitation.

Reduce Ransomware Entry Vectors

Eliminate low-hanging fruit like exposed servers and unsecured ports, limiting adversaries' ability to gain initial access.

Strengthen Ransomware Resilience

Proactively reduce the overall attack surface, making it harder for adversaries to propagate and achieve their objectives

Protect Critical Services

Identify and harden both standard and non-standard ports tied to sensitive or legacy applications that ransomware groups aggressively target.

Prioritize What Matters Most

Move beyond static monitoring with prioritized risk insights that direct IT and security teams to the exposures with the highest impact.

Accelerate Response and Hardening

Enable faster mitigation of exploitable services by correlating ports with processes, applications, and devices in real time.

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 maps established connections for every process running on servers, sampling data frequently throughout the day. Prioritization focuses on persistent and consistently open connections which would allow higher success for an actor to exploit the connections, in comparison to periodic or short-term open connections.

2. **Mapping and Identification:** Starting with standard ports frequently targeted by attackers, the agent correlates listening ports to applications and devices. This includes known ports like 22, 21, 445, 80, 8080, 443, and others, while extending to non-standard ports tied to critical services such as SQL.

3. **Prioritization and Dashboard Presentation:** Exposures are prioritized based on port and service criticality, focusing on the potential impact of exploitation of critical services such as SMB, SQL, or web applications. The user-friendly dashboard presents actionable insights, including exposed devices, correlated processes, with prioritized criticality, allowing security teams to investigate and mitigate promptly.

Morphisec's Network Discovery equips your team with the tools to uncover and address network exposure risks on the endpoints effectively, strengthening your defenses against targeted 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