

The Need for Additional Deception Protection on the Endpoint

Prevention-First, Defense-in-Depth Approach

NETWORK & ACCESS LAYER



Firewall



SASE / VPN



IDS / IPS



Mail Gateway



DLP

Controls access and traffic – but can't stop post-entry execution

MORPHISEC (PREVENTION)



Prevention-first



≠ EDR



Stops attacks before they execute on the endpoint

EDR / XDR



Detect



Investigate



Respond

Detects and responds after execution begins

BACKUP & RECOVERY



backup is not security



recovery is not prevention



Immutable Backup



Decryption



Forensics

Restores systems after impact