OnSystem Defender Is the Best Endpoint and Application Security Solution For Your Organization

Seeking a modern and adaptive cybersecurity approach? ***OnSystem Defender*** provides the most comprehensive and flexible solution when compared to others' rigid, whitelist-focused models.

OnSystemLogic™

Endpoint and Application Security

OnSystem Defender (OSD) Brings Two Solutions in One Easy Deployment

Two Solutions, One Deployment

OSD application whitelisting provides an easy to deploy and manage service that allows only pre-approved applications to run on your system.

OSD memory protection techniques safeguard your system's applications' memory from unauthorized access or malicious code execution; effectively preventing malware and other unauthorized software from running by strictly controlling which applications can access memory and what operations they can perform within it.

Unmatched Benefits

Proactive defense: Blocks unknown malware by preventing execution of unauthorized applications.

Reduced attack surface: Limits the potential entry points for malicious code by restricting application execution.

Enhanced resilience against exploits: Memory protection techniques can mitigate vulnerabilities even if a system is not fully patched.

Traditional Solutions' Ten Significant Limitations Compared to OSD

1 High Maintenance Over Time

Traditional solutions require a "learning period" to gather every application, script, DLL, and file that runs. While this is a critical step to avoid blocking legitimate processes, it introduces complexity for IT teams in managing these profiles.

OnSystem Defender eliminates the need for such extensive profiling by leveraging **"pre-configured application control policies"** and **"adaptive learning of application behaviors"**, reducing administrative overhead.

2 Static Whitelisting Model

Traditional solutions rely heavily on "static whitelisting" to approve applications and their updates. While this simplifies management for recognized apps (e.g., Microsoft Office, Chrome), it may struggle with "dynamic environments" where new applications or untracked dependencies are introduced frequently.

OnSystem Defender's dynamic behavior-based approach actively **enforces legitimate "runtime" behaviors**, which adapts more fluidly to such changes without requiring constant administrative adjustments to the whitelist.

3 Inability to Address Memory Exploits

Traditional solutions do not provide capabilities for protecting an application's "runtime memory." Whitelisted applications, even if legitimate, can still be exploited by attackers through fileless malware, memory injections, or zero-day vulnerabilities.

OnSystem Defender actively **monitors and controls application memory in real time,** preventing malicious instructions from executing even within trusted apps.

4 Operational Delays for End-User Requests

While other solutions allow end-users to request new software and provide an approval process, this still introduces delays and requires additional IT intervention. In environments requiring agility, such as software development or other fast-paced industries, this approval model can hinder productivity.

OnSystem Defender **uses learned application governance**, meaning IT teams are less frequently involved in micromanaging new software requests, as legitimate behaviors are automatically adapted.

5 Potential for False Positives

Other solutions provide tools for examining applications and processes during the learning phase and later approvals. However, the static whitelist model can lead to “false positives”, where legitimate software may be incorrectly flagged and blocked due to strict policies.

Repeated false positives could frustrate end-users and lead to productivity bottlenecks.

OnSystem Defender’s **behavior-based enforcement** reduces false positives by focusing on legitimate memory and runtime actions rather than static lists.

6 Vulnerabilities in Supply Chain Attacks

Other solutions may track applications and their updates, ensuring they are authenticated before being allowed. However, this does not prevent “supply chain attacks”, where a trusted application update is compromised (e.g., SolarWinds attack).

Other solutions cannot detect malicious modifications in trusted applications if the compromise occurs after the whitelist approval.

OnSystem Defender mitigates this risk by **enforcing legitimate application behaviors even after updates**, ensuring that compromised software cannot execute malicious code.

7 Resource Requirements for Deployment and Maintenance

Deploying other solutions, performing the learning mode to identify applications, and managing the approval process for each request can quickly become resource-intensive, especially for large organizations or rapidly changing IT environments.

OnSystem Defender's **pre-configured policies and minimal** setup provide faster deployment and lower management requirements.

8 Focus on Known Threats

Other solutions claim to excel at blocking "known bad applications", malware, and unauthorized tools. However, itheir reactive models don't inherently protect against "unknown or zero-day exploits" that abuse novel techniques or memory-based attacks.

OnSystem Defender **uses deterministic filtering and runtime memory control to stop unknown threats** before they execute, regardless of whether they've been previously identified as malicious.

9 Reliance on Sandboxing and Virus Checking

Other solutions' use of sandboxing (to test suspicious applications) and tools to check against known malware databases are useful, when available. However, they require "manual intervention from administrators", which can slow response times and leaves room for human error.

OnSystem Defender **automates advanced threat prevention**, leveraging real-time behavior enforcement rather than relying on external tools or manual processes.

10 Lack of Real-Time Adaptation

Other solutions may allow automatic updates for certain applications (e.g., Microsoft Office) but don't dynamically adapt to runtime changes or evolving software dependencies outside its pre-approved definitions.

OnSystem Defender **handles runtime changes dynamically**, learning and adapting to legitimate behaviors without requiring constant manual updates.

OnSystemLogic™