Avecto Datasheet

defendpoint

▽ Protect

Eliminate admin rights, achieve least privilege

▽ Control

Whitelist trusted apps and block malware

▽ Isolate

Content isolation for email attachments and websites

Defendpoint by Avecto creates the foundation of your security architecture. It's a multi-layered prevention engine that stops cyber attacks at the endpoint. By uniquely combining the technology capabilities of privilege management, application control and content isolation, Defendpoint protects your users, your data and the rest of your security stack from external and internal threats.

How does it work?

This innovative solution allows organizations to balance security and usability, ensuring user experience is never compromised.

Content isolation
Isolation of the most common attack vectors, the web browser and email, prevents attackers accessing user data, launching payloads or persisting.

Defendpoint uniquely uses native Windows security to provide a lightweight isolation model without the expense and complexity of virtualization. Isolation protects vulnerable applications and the endpoint from the threat of zero day or unpatched exploits.

Application control
Defendpoint allows you to take a more pragmatic approach to whitelisting, so that users retain the flexibility they need to be productive. Simple yet highly effective rules make it possible to maintain application control across even the largest enterprises without relying on signatures or hashes.

A trust-based model working seamlessly with privilege management stops malware payloads from running or gaining a foothold on the endpoint. Plus, integration with content isolation means contextual whitelisting rules can be applied within the isolated sandbox environment.

Privilege management
With privileges assigned to applications, not users, Defendpoint allows you to successfully remove admin rights and protect the operating system. Individuals can still access the applications and tasks they need to perform their job role, so they can be productive without security compromise. Least privilege mitigates the risk of privilege escalation and removes the potential for rootkit infections, protecting the integrity of the OS.

Technical benefits

Proactive security
Gone are the days when you could rely on detecting threats and blocking malicious websites. Defendpoint is a non-signature based solution that hardens the endpoint to prevent attacks before they happen.

Combined benefits
By combining multiple capabilities in a single lightweight agent, Defendpoint offers unrivaled coverage of attack vectors. Users benefit from least privilege, whitelisting and content isolation all from a single pane of glass.

Protection from the unknown
Defendpoint stops malware and attacks at the endpoint using a unique approach that goes beyond targeting specific threats. It is highly effective against known malware as well as zero day threats.

Combat ransomware

By isolating untrusted content, including email attachments and web browsers, Defendpoint stops ransomware from launching payloads and accessing user data.

Simple and smarter security

Out of the box configurations and instant protection combine with a user-friendly experience to make a positive impact on security from day one. Pragmatic rules and a flexible policy engine let you easily manage complex user requirements.

Multi-platform support

With Windows desktop, Windows server and Mac editions including support for the latest operating systems, Defendpoint secures endpoints across your entire organization.

Enterprise management

Defendpoint integrates with Active Directory, McAfee ePO and Cloud platforms including Azure for rapid and scalable deployment with centralized reporting.

Compatibility

Defendpoint is designed from the ground up to work with your existing environment and operating system, providing maximum compatibility with your applications and the other layers in your security stack.

Positive end user experience

Replace native Windows User Account Control prompts with customized messages, with a variety of options for users to request access to 'greylist' applications. Challenge/response codes, dual authentication or on demand elevation ensures users remain productive, with activity logged in reporting dashboards to allow for policy refinement.

Actionable intelligence via advanced reports

With Defendpoint's enterprise reporting solution, you can easily identify privileged users and activity with usable data that enables you to keep admin rights to a minimum. Graphical dashboards and reports with drill-down options provide fast access to as much detail as you need. Reports are built on familiar and trusted SQL Server and SQL Reporting Services.

Supported platforms

- Windows XP – Windows 10
- Windows Server 2003 – Windows Server 2016
- macOS 10.10 Yosemite – macOS 10.12 Sierra

32-bit and 64-bit versions are available for all supported platforms.

About Avecto

Avecto is a global security software company. Its innovative endpoint security solution, Defendpoint, is a multi-layered prevention engine that stops cyber attacks. It takes a proactive approach to preventing malware, uniquely combining three core capabilities of privilege management, application whitelisting and content isolation. Defendpoint protects over 8 million endpoints at many of the world's biggest brands, ensuring that strong security never comes at the expense of usability.