Avecto

defendpoint

Prevention
is possible

Defendpoint by Avecto is a security software solution that makes prevention possible. It uniquely integrates three proactive technologies to stop malware at the endpoint.

The combination of Privilege Management, Application Control and Sandboxing in a single suite solution finally allows global organizations to improve security while ensuring a positive user experience across Windows and OS X.

Introducing Defendpoint

Three simple steps to defense in depth

$$\boxed{1} + \boxed{2} + \boxed{3} = \text{defendpoint} \blacktriangledown$$

Stop malware at the endpoint.

2 Application Control

Second, grant users the flexibility to access the applications, tasks, scripts and content they need to remain productive with pragmatic yet effective whitelisting.

1 Privilege Management

First, remove admin rights from all users - cutting out the risk associated with over 90% of Critical vulnerabilities reported by Microsoft.

3 Sandboxing

Finally, add a last line of defense with Sandboxing to protect your users and data from threats that originate online.

Privilege Management

▶ Eliminate admin rights

▶ Assign privileges directly to applications

▶ Protect the endpoint from insider threats

By assigning privileges to applications and tasks, not users, you remove the admin rights that are often targeted by hackers and malware that rely on elevated privileges to gain entry into your corporate network.

This provides a solid security foundation, allowing all users to run with standard accounts, while at the same time ensuring they have the freedom to remain productive.

Defendpoint provides a fully customizable end user experience, with a 'workstyle' based approach that ensures you cater for the specific access needs of individual users and groups, with advanced exception handling capabilities.

Key technical benefits

▶ **Privileges are applied directly to approved apps, tasks and scripts, not users**

▶ **Works seamlessly with Windows User Account Control to suppress or replace UAC prompts**

▶ **Map policies to specific job roles, even developers and sysadmins in the data center**

▶ **Simple configuration with clear process flows**

> The single most important way to improve endpoint security is to run more of your Windows users without administrator rights
>
> **Neil MacDonald, Gartner**

Application Control

▶ Block unauthorized applications

▶ Handle diverse user needs flexibly

▶ Defend against zero day and targeted attacks

Defendpoint's Application Control module adds a crucial second layer to the security stack, solving the traditionally difficult challenge of managing business applications.

By taking control of your software environment and applying simple rules to manage trusted applications, you automatically reduce risk by blocking the unknown. With its advanced capabilities, you can take a more pragmatic approach to whitelisting without locking down the endpoint, so that your users retain the flexibility they need to be productive.

Application Control is so effective that experts analyzing real-world threats, including the Council on Cyber Security (in association with SANS), name it the most essential strategy for mitigating cyber threats.

Key technical benefits

▶ **Advanced exception handling with customizable messages and prompts**

▶ **Tight integration with Privilege Management and Sandboxing**

▶ **Simple to use and manage with broad rule criteria and application support**

▶ **Gain visibility and identify all applications in use across your business**

> Rated number one mitigation strategy for overcoming real world threats
>
> **Council on Cyber Security**

Sandboxing

▶ Contain web-borne threats

▶ Isolate untrusted activity

▶ Protect your data from malware

With internet browsing a business necessity, the risk of users introducing malware through document downloads or infected websites has increased exponentially.

Sandboxing complements your patching and anti-malware strategies, adding a vital last line of defense against attacks that originate online while keeping users free to safely use the internet.
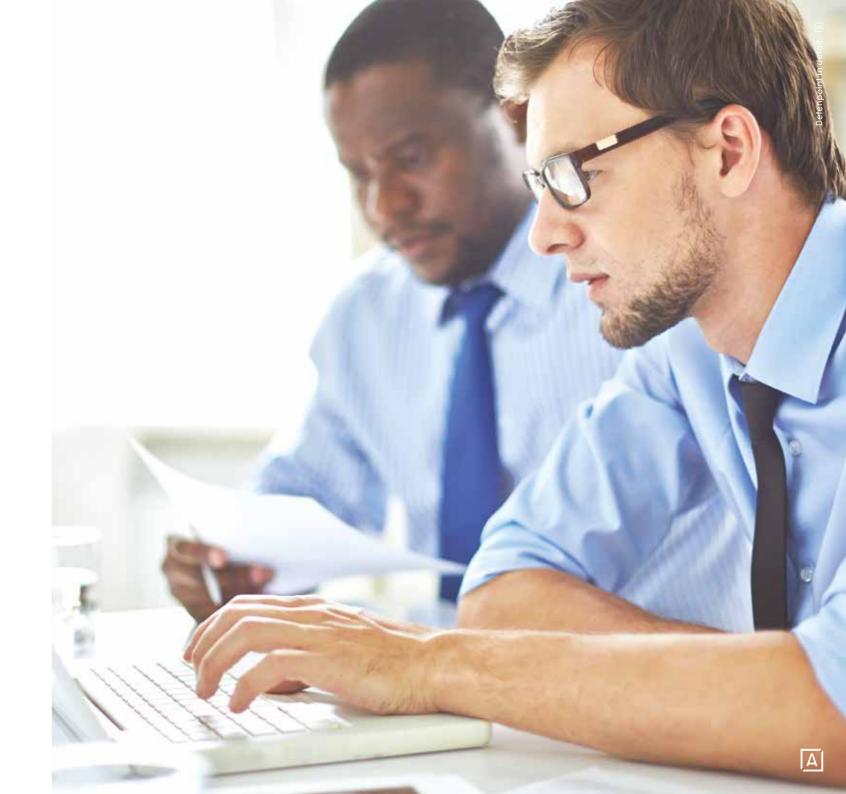
Unlike traditional Sandboxing solutions that isolate content by building barricades, Defendpoint takes a unique approach. Leveraging the native Windows security model that traditionally separates one user account from another, all untrusted activity runs inside a secure container so that any potential threats are contained. A seamless end user experience is assured, with no impact on web performance.

Over 288,000 new cyber threats are reported every day

McAfee

Key technical benefits

▶ **Protect private and corporate data by isolating all web-based activity**

▶ **Leverages native Windows security to offer native performance and compatibility**

▶ **Users are able to download content to their standard document folders and print as usual**

▶ **Tracking of saved content to ensure downloads are always opened securely**
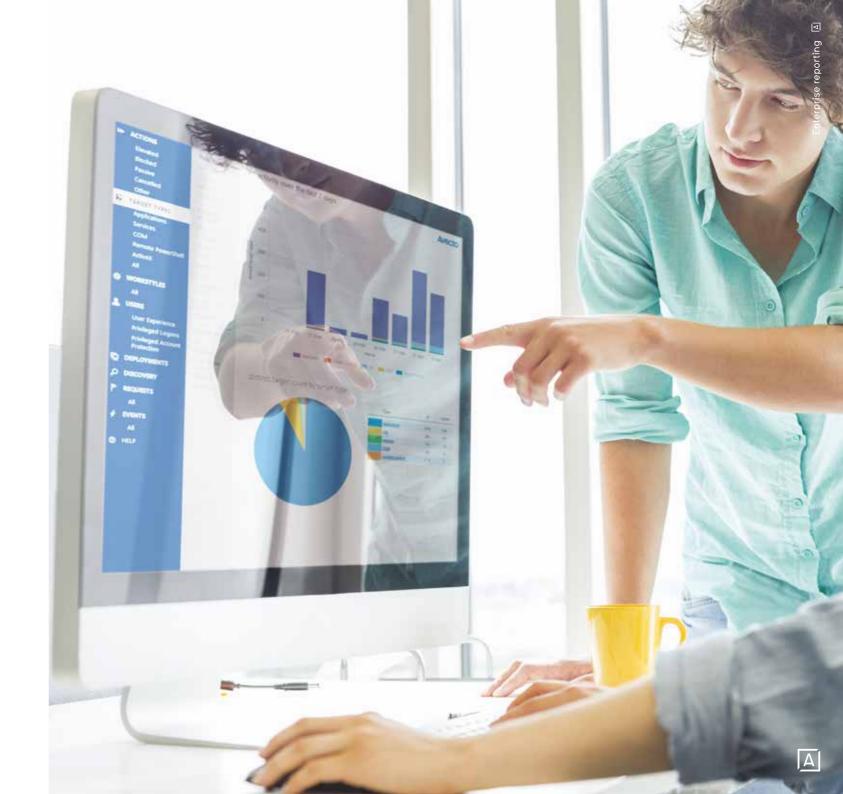
Enterprise Reporting

▶ Gain real-time insight
▶ Dig deeper with granular reports
▶ Refine your Defendpoint policy

Gain comprehensive visibility across your Defendpoint suite with integrated Enterprise Reporting that comes as standard. Discover, monitor and manage activity across your entire business, generating actionable intelligence to make informed decisions about your policy.

Defendpoint's broad range of web-based reports provide trend analysis and more, delivering unique insight that aids troubleshooting. This depth of information enables you to take a more proactive approach to implementing and maintaining your endpoint security.

Key technical benefits

▶ **Graphical dashboards provide real-time insight**

▶ **Schedule automated distribution and build custom reports**

▶ **Pinpoint where your Defendpoint policy is impacting user productivity and refine over time**

▶ **Secure access via Microsoft SQL Reporting Services or McAfee ePO**

Architecture that fits your business

▶ Enterprise-class architecture
▶ Highly scalable
▶ No additional investment

Building on trusted infrastructures, you benefit from choice and flexibility with your Defendpoint deployment.

A single agent is installed on the endpoint, powering all three technologies. Simple, streamlined management is provided through a single console that is tightly integrated with either Microsoft Active Directory Group Policy or McAfee ePolicy Orchestrator (ePO), making it scalable across any size of organization.

Defendpoint's integration abilities, utilizing in-built delegation models and digital policy signing, ensures your policies can be designed and transferred securely to those responsible for deployment.

McAfee®   ■■ Microsoft

Extending protection to servers

▶ Gain real-time insight
▶ Dig deeper with granular reports
▶ Refine your Defendpoint policy

To achieve holistic endpoint security, the same approach to user privileges, applications and online activity should be applied inside the data center.

With Defendpoint, you can extend your security protection to sysadmins in the server room without locking down essential functionality.

Specific Defendpoint features have been developed to meet the advanced requirements of sysadmin users. This means you gain full transparency and control in the data center without compromising productivity.

Key technical benefits

▶ **On-demand elevation for gated access control with authentication, justification and challenge/response codes**

▶ **Full audit trails of all privileged activity with detailed application forensics**

▶ **Remote PowerShell control for the management of remote servers using standard accounts**

▶ **Over-the-shoulder authentication control to meet the dual authorization requirements of compliance mandates**

▶ **Secure elevation of scripts, services, driver operations and individual management consoles**

▶ **Content control to allow privileged access (or the application of restrictions) to server configuration files**

About Avecto

Avecto is an innovator in endpoint security. Founded in 2008, the company was established to challenge the status quo that effective security leads to user lockdown. This philosophy of security + freedom promotes a positive user experience across every software implementation, allowing organizations to strike just the right balance.

Its unique Defendpoint software makes prevention possible, integrating three proactive technologies to stop malware at the endpoint. This innovative software protects over five million endpoints across the world's most recognizable brands in some of the most highly regulated industries.

Attention to detail is paramount, with a team of qualified and experienced technology consultants to guide clients through a robust implementation methodology. This consultative approach provides clients with a clearly mapped journey against measurable objectives to ensure project success.

Avecto