Avecto Datasheet

defendpoint

# Deep dive: Content isolation

Defendpoint by Avecto creates the foundation of your endpoint 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's proactive security protects your endpoints, your users and your data no matter where they are, from the office to the coffee shop.

## Deep dive: Content isolation

Avecto content isolation offers a unique approach to endpoint protection. The core idea is simple, launch content originating online, such as email attachments and web browsers, under a separate temporary account to protect the users' data. This has several key advantages over other approaches:

- **Endpoint-based security –** With an increasingly mobile workforce it's important to isolate content on the endpoint, as this is not only where data is accessed from, but where the attack starts. Network-based isolation can be evaded and fails to protect the endpoint.
- **Protection –** In the event content is malicious, it will be unable to access the user's data or profile. This boundary is implemented by the Windows operating system, which prevents one user from accessing the files of another.
- **Performance –** Traditional sandboxing products have been built around hardware or software virtualization. This makes them very resource heavy and requires a lot of configuration to setup and maintain. Defendpoint is a single lightweight agent, requiring no additional hardware.
- **Compatibility –** Defendpoint maximizes compatibility by working with the operating system, rather than having to virtualize or emulate. This allows other components in your security stack, such as AV and forensics tools, to work alongside Defendpoint without conflict.
- **Context –** Content isolation is just one part of the Defendpoint solution, with privilege management and whitelisting capabilities adding security benefits far beyond isolation alone. Content isolation provides context, allowing organizations to easily define controls that prevent isolated content from accessing privileges or launching payloads without limiting the normal user activity. A good example of this is preventing phishing attacks leveraging built in tools, such as PowerShell, without blocking the user's access.

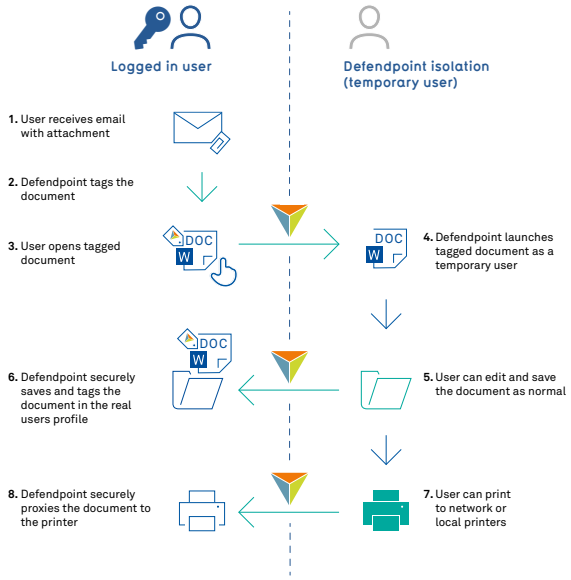
## How does content isolation work?

Defendpoint content isolation is built on the native Windows NTFS security model and uses a Windows user account. When enabled, it automatically generates a temporary local user profile that is used as a secure container to launch content in. As it utilises a standard user account the design is secure by default, as the Windows Kernel prevents access to the logged in user's data.

To ensure a positive user experience, key user settings are applied to the applications running in the isolated environment. The user is also able to save and print files as usual, with Defendpoint securely mapping the user's folders and printers without allowing direct access to files and resources that could be attacked.

All content is still saved locally, and appears as the user expects in their profile with Alternate Data Stream (ADS) tags used to identify content that has been downloaded and requires isolation. These tags are applied automatically to email attachments and downloaded documents. When the user clicks a link, or opens a tagged document, Defendpoint seamlessly launches the content in the isolated environment.

## Example 1 – Unknown email attachment:

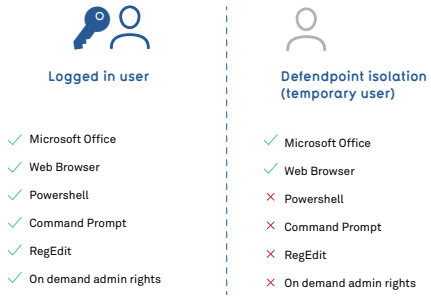



In this example, we see that Defendpoint has automatically isolated the email attachment while still allowing the user to edit, save and print. The document is tagged, so if it is reopened in the future it will again be launched into the isolated environment.

## Combined capabilities

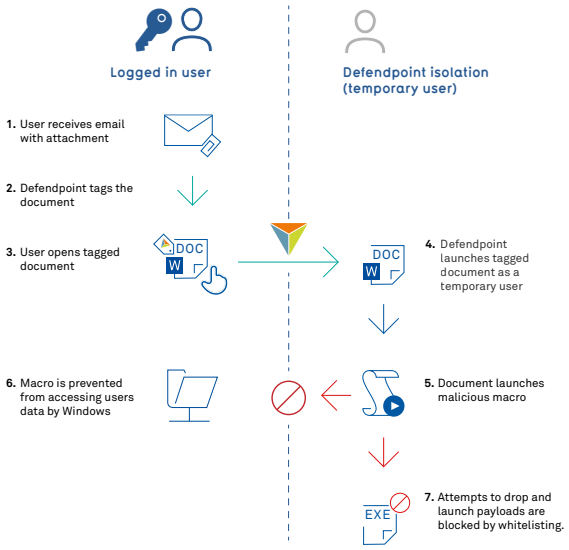
The full benefits of Defendpoint are unlocked when you combine its three capabilities. Isolation provides context for whitelisting and privilege management. This allows you to apply separate rules and control to downloaded content. This powerful combination enables you to prevent malware using built in tools such as PowerShell and CMD. exe, which would ordinarily be whitelisted.

## Example 2 – Isolation aware control policy




In example 2 we see how the benefits of Defendpoint go beyond isolation alone with policy that can use targeted restrictions to prevent attacks without impacting on the user experience. This key differentiator is unique to Defendpoint allowing users to be productive and endpoints to be secure by using context aware layers of security that work together.

## Example 3 – A phishing email attachment




As with the previous example, we see that Defendpoint automatically isolates the email attachment. However, this document is infected and contains malware. As the attack is launched within a separate user account, the attacker is unable to access the logged in user's data. This is key to stopping ransomware as it prevents access to the data.

Whitelisting and privilege management capabilities offer further protection by blocking the payload dropped to disk and preventing admin rights being exposed to the attacker. Even “fileless malware” attacks, which rely on hiding PowerShell scripts in the registry, are prevented as the registry is not that of the logged in user and PowerShell cannot be launched in the temporary profile.

This all occurs without any form of detection, representing an entirely proactive approach. Defendpoint is just as effective across all variants of malware, as it breaks the attack chain. Without access to data, privilege and no ability to drop and launch a payload, threats are mitigated from day one.

## Summary

Relying on detection alone is not enough to prevent cyber attacks. Defendpoint leverages the Windows security model to achieve content isolation that is secure and highly effective. When combined with the other capabilities of Defendpoint, it provides robust proactive security that can handle even the most advanced cyber threats. With ever-increasing ransomware and attacks targeting data, it has never been more important to isolate content that originates online.

## Supported platforms

- Windows XP – Windows 10
- Windows Server 2003 – Windows Server 2016

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.