5 ways to optimize your endpoint protection strategy with Avecto & Intel Security

Gone are the days where desktop security was limited to just antivirus software. Faced with combatting todays advanced threats — including targeted, zero-day attacks, phishing, drive-by downloads and advanced persistent threats — endpoint protection suites that bolster security on Windows are required.

In this short article, we share 5 tips for optimizing your endpoint protection strategy with Avecto's Defendpoint technology integrated with McAfee ePO™.

01 Get proactive with security

Defendpoint complements detection based technologies with a proactive approach that contains the impact of attacks that go undetected. Employing a layered approach to endpoint security, Defendpoint enables you to implement least privilege by eliminating the need for local administrator accounts. Building on McAfee's granular application control capabilities, Defendpoint adds extra defense for trusted software. When trusted software opens untrusted content, Defendpoint confines the application in an endpoint sandbox.

02 Remove admin rights from users

To fully capitalize on the investment in their security solutions, organizations must first remove administrative privileges from end users. Layered endpoint security controls should build on a solid foundation of least privilege.

As hackers employ more sophisticated means to infiltrate corporate IT systems the evolving mindset of "assume compromise" underlines the need to restrict privileges and protect against lateral attack propagation.

If employees are only granted standard user rights, the risk associated with 97% of Critical Microsoft vulnerabilities can be mitigated, considerably decreasing the risk compared to when patches, antivirus and application control are deployed alone. Without the admin access it seeks, malware targeting elevated privileges cannot reach the core network, where they cause the most damage.

03 Gain flexibility with privilege panagement

Any approach to removing admin rights should be planned carefully. Removing administrative privileges has become more realistic in recent versions of Windows with the introduction of User Account Control (UAC). Moving users to a standard user account, i.e. not a member of the local administrators group, cuts off access to all system changes that require greater privilege, as well as installing or updating authorized software.

Some user roles such as IT admins and developers can't function without additional system access. Without appropriate technology in place, users find themselves restricted and unable to access files and applications they need on a daily basis. Additionally, without considering the end user experience, admin rights are often granted back to enable emergency access but never removed. Even a small number of admin users create significant internal and external vulnerabilities.

The built-in Windows tools and UAC features lack the flexibility required in managed corporate IT deployments. Defendpoint features policy-based rules that allow application privileges to be elevated without elevating the user to an administrator. When users encounter exception scenarios, customizable messaging and advanced features such as two-factor authentication and challenge/response authorization allow users to remain productive with minimal impact on helpdesk staff.

Without flexible privilege management rules, least privilege implementations often fail because of compatibility issues with legacy applications, changing business needs or lack of user acceptance.

Defendpoint empowers IT teams to secure endpoints while providing a positive user experience and freeing the helpdesk from access requests.

04 Leverage application control

Endpoint protection has been focused on malware detection and blocking using signature-based approaches. Although a mainstay of endpoint security for many years, signaturebased antivirus has struggles to provide effective protection, failing to detect more than 50% of attacks today.

Application control adds an additional layer of protection by blocking applications that are not specifically approved by your IT team. McAfee's Application Control solution ties into a comprehensive application and URL reputation database and provides granular rules and finite control. This layer of security can considerably reduce risk as most vulnerabilities are not in the operating system, but in applications. By gaining control of application use across your business, you can prevent users from inadvertently downloading and running malware, and ensure that only fully up to date versions of approved programs are allowed to run.

05 Add a last line of proactive defense with content isolation on the endpoint

Endpoint content isolation adds a final line of defense against undetected threats delivered in content files like PDF, Office and web page content such as Java libraries. Consider an example where a user opens an infected document downloaded from the internet, or the website itself is compromised. The attack isn't detected as malicious and is loaded in an approved IT application such as Internet Explorer, Adobe Reader, Microsoft Office or the Java runtime. Neither antivirus nor application control block the content file or its handler, resulting in malware running with access to user's files and applications.

Defendpoint content isolation with privilege management isolates untrusted content and the related application to protect user's data and the system itself. From an end user perspective content isolation is transparent – protecting the user from threats without affecting their experience working with their files.

Why Avecto and Intel Security?

Defendpoint offers robust protection against advanced threats on the endpoint. With a unique approach that complements McAfee's Endpoint Protection solutions, Defendpoint adds privilege management and content isolation capabilities to provide simple and holistic defense in depth.

As the foundation of the McAfee Security Management Platform, The McAfee ePolicy Orchestrator (ePO) framework makes risk and compliance management simple, allowing organizations to connect industry-leading security solutions to their enterprise infrastructure to increase visibility, gain efficiencies and strengthen protection.

As attackers become more proficient in working around detection techniques and focusing on specific organizations as targets, the ability to coordinate security solutions becomes important. Responding to an emerging threat may require changes at one or more layers in your security stack. This can be difficult to enact quickly if disparate management solutions are in use.

Defendpoint ePO Edition uniquely provides full management of the solution from within the ePO console for consistency and familiarity and includes client deployment, policy management and reporting. Application rules can be automatically generated from the endpoint audit data collected in ePO which is presented in actionable application and process report views. The reporting module is comprehensive, satisfying the needs of the most demanding regulated industries.

Avecto is a member of the Intel Security Innovation Alliance and Defendpoint is fully integrated with Intel Security's McAfee Threat Intelligence Exchange (TIE) via the McAfee Data Exchange Layer (DXL). Building deeper integration among security products, McAfee DXL empowers organizations with a clear view and a more intelligent understanding of their security environment.

With Defendpoint offered as a McAfee DXL-ready solution, the integration allows application reputation data to be used to drive configuration changes and make risk-based policy adjustments powered by third party data.

As part of this industry disrupting integration with McAfee ePolicy Orchestrator (ePO), Defendpoint offers simplified management, further solidifying the technology partnership.