SOLUTION BRIEF

5 Ways to Optimize Your Endpoint Protection Strategy With BeyondTrust & McAfee

BeyondTrust

Faced with today's advanced threats, such as zeroday, phishing, and drive-by downloads, endpoint protection suites bolstering security on Windows are required.

Below are 5 tips for optimizing your endpoint protection strategy with BeyondTrust's Endpoint Privileged Management solutions integrated with McAfee.

1. Get Proactive with Security

BeyondTrust Endpoint Privilege Management complements detection-based technologies with a proactive approach containing the impact of attacks that go undetected. Employing a layered approach to endpoint security, our solution enables you to implement least privilege by eliminating the need for local administrator accounts. Building on McAfee's granular application control capabilities, our Privileged Management solution adds extra defense for trusted software.

2. 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 94% 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.

3. Gain Flexibility with Privilege Management

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.

BeyondTrust Privileged Management 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. Our Privileged Management platform empowers IT teams to secure endpoints whilst providing a positive user experience and freeing the helpdesk from access requests.

4. 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, signature-based 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 up to date versions of approved programs are allowed to run.

5. BeyondTrust and McAfee

Our software provides security strength and depth, offering robust protection against advanced threats on the endpoint. With a unique approach that complements McAfee's Endpoint Protection solutions, BeyondTrust adds Privilege Management 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.

BeyondTrust Privilege Management 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.

McAfee's Security Connected vision now being implemented in McAfee products and offered to BeyondTrust and other partners will further enable real-time communication among products to coordinate response. We are actively developing this greater level of integration.