KuppingerCole Report

EXECUTIVE VIEW

By Paul Fisher

February 04, 2021

BeyondTrust Endpoint Privilege Management

Privileged Access Management (PAM), of which Endpoint Privilege Management (EPM) is a part, is an essential component in protecting organizations against cyber-attacks, ransomware, malware, phishing, and data leaks. No longer a tool for protecting admin accounts, privilege management now extends across the entire organization, from on-premises and cloud infrastructure to every user, no matter where are working from, or what they are accessing. A critical role of PAM is controlling the use of privileges, increasingly these days in remote and work-from-home environments.

By **Paul Fisher**
pf@kuppingercole.com

Content

1 Introduction

Digital transformation is no longer optional for businesses and organizations if they wish to stay competitive and deliver greater value to customers. But as they seek to embrace the advantages of Cloud, IoT, AI and Big Data projects across extended infrastructures, organizations need to be aware of the cyber security, compliance, and identity risks that digital transformation also creates.

While these risks are serious, they can be significantly reduced through intelligent, fit for purpose and structured deployment of security solutions. As agile access and identity requests are a prime characteristic of a successful digital environment it follows that one of the most important suites of products to manage this securely is PAM. PAM solutions are critical cybersecurity controls that address the security risks associated with the use of privileged access in organizations and companies. Among the key challenges that drive the need for PAM are:

- Abuse of shared credentials
- Abuse of elevated privileges by unauthorized users
- Hijacking of privileged credentials by cyber-criminals
- Abuse of privileges on third-party systems
- Accidental misuse of elevated privileges by user
- The requirement to perform attestations on privileged users and admin accounts
- Vulnerability of endpoints that provide access to privileged accounts

Furthermore, there are several other operational, governance and regulatory requirements associated with privileged access:

- Discovery of shared accounts, software, and service accounts across the IT infrastructure
- Identifying and tracking of ownership of privileged accounts throughout their lifecycle
- Establishing Single Sign-on sessions to target systems for better operational efficiency of administrators
- Auditing, recording, and monitoring of privileged activities for regulatory compliance
- Managing, restricting, and monitoring administrative access of IT outsourcing vendors and MSPs to internal IT systems
- Managing, restricting, and monitoring administrative access of internal users to cloud services

Users also need fast and easy access to applications, files, databases, and servers which calls for greater attention paid to the design of the security and productivity balance within PAM tools. In recent years, PAM solutions have become more sophisticated making them robust security management tools. While credential vaulting, password rotation, privilege delegation and activity monitoring are common, more advanced capabilities such as privileged user analytics, risk-based session monitoring, advanced threat protection, and the ability to embrace PAM into an enterprise governance program are the new standard to protect against today's threats in complex environments.

The endpoint challenge for privileged access management

Privileged access is required from the millions of endpoints that form part of extended enterprises, traditionally on machines running Windows or macOS operating systems. The importance of Endpoint Privilege Management (EPM) increased as the COVID-19 crisis took hold across the world in 2020 and organizations were forced to rely on operations and tasks executed by employees at home. Often, these were on devices outside of the network and even included personal devices shared by family members, leaving organizations more vulnerable.

The COVID-19 crisis also unleashed an avalanche of malware as criminals looked to take advantage of the situation. A stunning 30,000% increase in malware volume in the first months of the pandemic was recorded by security researchers, acutely underlining the risk posed by uncontrolled use of privileged accounts from unprotected endpoints.

Therefore, Endpoint Privilege Management (EPM) has gained renewed currency among IT and security managers but to implement it well there are several challenges. The EPM solution chosen should ensure that it prevents intrusion into servers from malware as well as protecting the endpoint itself. End users do not need any more barriers to "getting the job done" so avoiding another set of credentials at the endpoint is recommended.

In addition, organizations are faced with tighter budget controls after the COVID-19 crisis. They need to carefully balance cost, time to value as well as security for any new investment into endpoint security. In this Executive View we assess how BeyondTrust's EPM solution stacks up to meet the challenges of privilege management at the endpoint inside, and outside of, the network with the large shift to remote working.

2 Product Description

US-based company BeyondTrust is one of the world's leading providers of PAM solutions for digital organizations. Its Endpoint Privilege Management (EPM) solution is compatible with Windows, macOS, Unix and Linux operating systems.

The solution has been engineered to stop most zero-day attacks by eliminating excessive end user privileges and implementing advanced application control and command filtering. Additionally, it solves a pressing problem for organizations wishing to grant privileged access to users working across all endpoints. That is: how to maintain user productivity. End users need privileges to perform everyday tasks such as self-serve installation of applications, updates, system settings, and printers and other hardware drivers – without relying on the service desk, expensive repackaging, or 3rd-party ITSM tools.

In the datacentre, privileges present a more significant challenge, where sysadmins will routinely require administrative access to Windows, Unix and Linux infrastructure operating critical services. It's essential these environments are matched with strong controls and visibility of activities, without hindering productivity. BeyondTrust check those boxes too, with EPM solutions tailored for deployment across all server OS's, both on-premise and in the cloud.

Currently, many organizations give users permanent, or even temporary access to admin accounts to get around this. But with that comes the risk that excessive privileges maybe be abused or hacked, or users introduce malware to the wider organization. A workaround would be to legislate users to request privilege access for each and every occasion they need it. But this is time consuming, unwieldly, reduces digital productivity, and typically ends up with privilege creep. According to BeyondTrust's Microsoft Vulnerabilities Report, 77% of critical Microsoft vulnerabilities would be mitigated by removing admin rights – proving that giving back admin rights, in any form, is a big risk to organizations.

BeyondTrust EPM uses a Just-in-Time (JIT) process that elevates the application, script, or command and not the user, without the need for passwords. In this scenario, the user is never privileged, and the application request is checked against a security policy which allows for a targeted user experience based on the end user. This includes elevating the application seamlessly to blocking completely, with numerous options in between such as challenge/response. BeyondTrust describes this as Passwordless Administration (not to be confused with Passwordless Authentication).

The company says that customers can still add MFA to the process if they wish for an extra layer of protection. But by default, the platform does not need a password from the user, utilizing JIT access. An example is compatibility with BeyondTrust's password management tool, BeyondTrust Password Safe. For Windows endpoints not connected to the corporate network, BeyondTrust EPM can apply local account password rotations on behalf of Password Safe. Organizations can manage credentials on endpoints in remote locations, and passwords can be rotated automatically – again with the end user never having to see

or be involved in the process.

Deploying BeyondTrust EPM out-of-the box should be relatively easy for many customers. BeyondTrust QuickStart policies provide templates for a claimed 80% of known uses cases. These out-of-the box policies are based on implementations across over 50 million endpoints recorded by BeyondTrust. The company also says that by using their QuickStart polices, long periods of discovery and monitoring is negated and local admin rights can be removed from users overnight, without a productivity impact. Additionally, all audit data can be recorded in detail to make further policy improvements for privileged access.

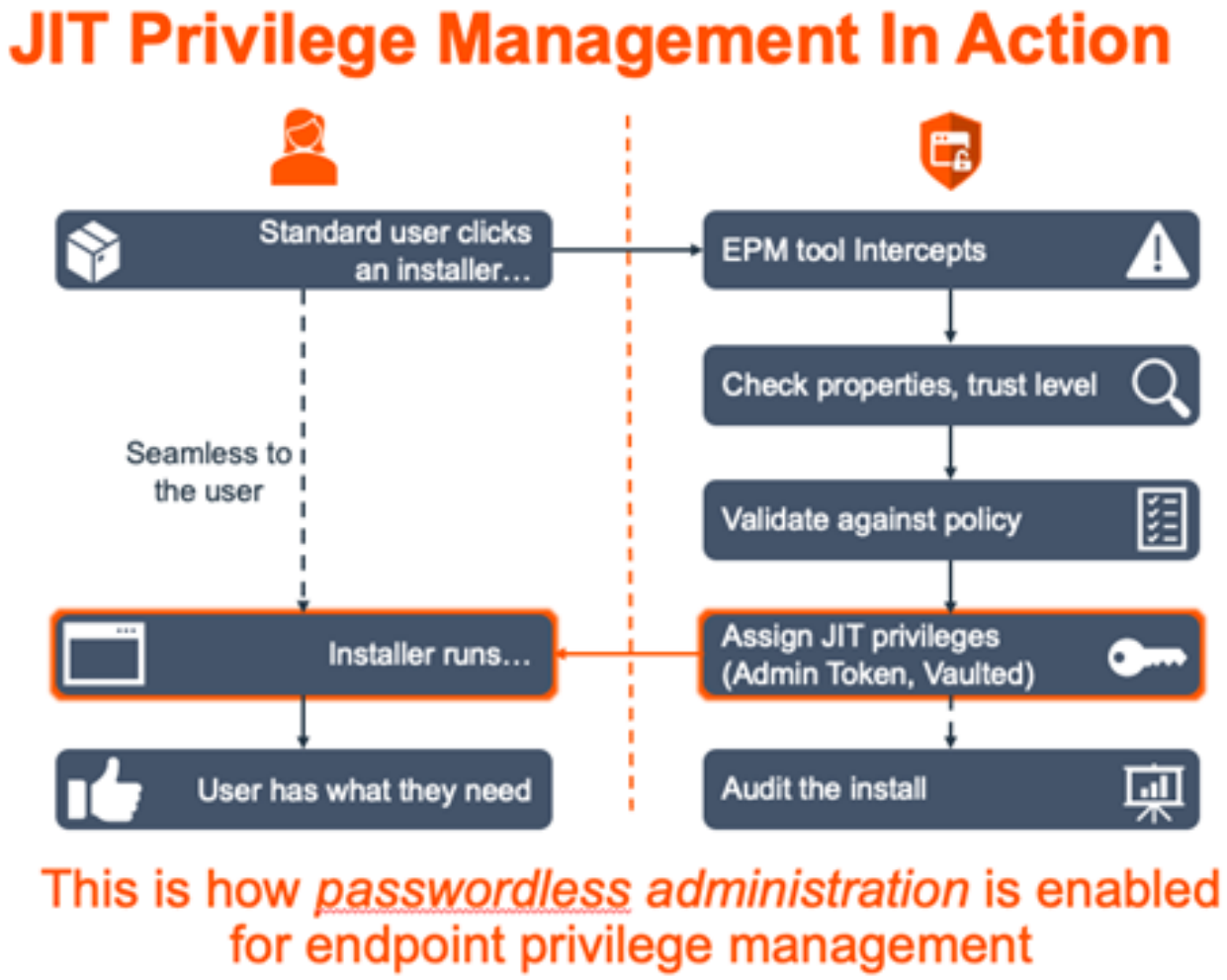

Figure 1: BeyondTrust EPM uses JIT to allow privilege access to resources (Source: BeyondTrust)

Deployment models cover a range of options. Privilege Management Cloud as a SaaS solution, BeyondInsight platform as an appliance (virtual or physical), and McAfee ePolicy Orchestrator (ePO). The solution is also compatible with Microsoft Group Policy Object (GPO) although only for Windows endpoints connected directly to corporate networks, meaning remote users need to continually connect via VPN to receive GPO updates.

Third party Integrations are strong, as you would expect from BeyondTrust. Major SIEM platform, Splunk, among others supported. And integration with digital workflow tools from ServiceNow should provide more complete support for remote end users.

The platform is also compatible with the Open Integration Framework which uses APIs to automate management of rules and application lists from ITSM solutions, audit scripting, and third party and bespoke data warehouses. Support for ITSM and digital workplace delivery tools is important if PAM is to cope with the new challenges of remote and home working and it is good to see this support from BeyondTrust here.

Figure 2: Five critical steps of endpoint security (Source: BeyondTrust)

EPM fills the gap between traditional AV tools and Endpoint Detection and Response and this is exactly where BeyondTrust EPM sits to stop zero-day attacks and block malicious code from entering the wider organization.

Endpoints should have AV and firewalls installed, as they are typically out-of-the box solutions and can mitigate many known attacks. However, according to Ponemon, 60% of attacks are missed, consisting of mostly zero-day attacks, which is a significant problem considering the number of new malware per day is estimated at 350,000 according to AVtest.org. BeyondTrust EPM uses the Trusted Application Protection feature to prevent malware from executing through popular applications such as Word, PowerPoint, Excel, Adobe Reader and common web browsers, by controlling the application Dynamic Link Libraries (DLL). Application Control tools block or allow applications for each group of users, and enable tracking of processes, installations, and attempted installations and allow admins to add applications to policies with easy-to-use import capabilities from audit data.

Some very capable analytics are supplied with BeyondTrust EPM out of the box. Graphical dashboards provide insights into all users, with drill down, custom filtering and SIEM integrations. Additionally, the solution provides full keystroke logging and recording and File and Integrity Monitoring (FIM) on Linux and Unix servers. In addition to providing an audit trail, reports also make it easy to refine and improve security policies. BeyondTrust EPM allows users to gain deeper visibility into user behaviour, using threat data from a variety of BeyondTrust and third-party solutions.

3 Strengths and Challenges

Given the recent shift to remote working brought on by the pandemic and other factors, customers are likely looking for products that will help them more easily manage elevation of privilege for users working at home, or elsewhere beyond the corporate network. Changing times makes us focus more on providing elevated access to standard users as and when they need it.

In this sense, BeyondTrust Endpoint Privilege Management offers a great deal of functionality, ease of use and ease of deployment to enable end users to do their jobs while protecting the corporate network and wider organization from threats.

By separating end users from applications and enabling the application to be elevated to perform a task, when combined with application control, the product effectively blocks the execution of malware and stops end users from performing unauthorized actions which could lead to a breach of the organization. At the same time, the default passwordless setting and opaque nature of the process saves users from extra tasks and hides the authentication process from them. This also happens very quickly enabling users to get on with their jobs.

This would be admirable even if it only improved productivity and efficiency. But the product is also backed by excellent analytics tools and integration with SIEM tools to ensure that organizations have a complete record of privilege access on the endpoint. This facilitates the discovery of malicious behavior patterns and ability to meet compliance demands. The integration with ServiceNow is another plus point, providing end users with an industry standard tool to get PAM support tickets while working remotely.

Endpoint privilege management will only increase in importance. This is a good product from an established and respected PAM vendor that should be seriously considered by any organization looking to secure and empower their employees working on endpoints, wherever they may be.

Strengths

- Works well within the BeyondTrust ecosystem but equally at home as EPM standalone solution
- Excellent analytics out of the box, helped further by integration with SIEM platforms
- Easy to configure and get started out of the box thanks to QuickStart templates
- Proven enterprise-class solution that is scalable and available on-premises or in the cloud
- Benefits from BeyondTrust experience in PAM solutions
- No admin or root accounts for end users or server admins

Challenges

- Further third-party SIEM integration would be useful addition
- We would like to see support extended to iPads, iPhone, Chrome and Android devices
- Pricing not publicly available

4 Related Research

Advisory Note: Trends in Privileged Access Management for the Digital Enterprise –71273
Architecture Blueprint: Access Governance and Privilege Management – 79045
Blog: PAM Can Reduce Risk of Compliance Failure but is Part of a Bigger Picture
Blog: Privileged Access Management Can Take on AI-Powered Malware to Protect
Blog: Taking One Step Back: The Road to Real IDaaS and What IAM is Really About
Leadership Brief: Privileged Account Management Considerations – 72016
Leadership Compass: Identity Provisioning – 70949
Leadership Compass: Identity Governance & Administration – 71135
Leadership Compass: Privilege Management - 72330
Whitepaper: AI, Machine Learning and Privilege Access Management – 80120
Whitepaper: Privileged Access Requirements for Small to Medium Size Businesses (SMB) – 80123
Whitepaper: Understanding Privilege Access Management – 80302

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded back in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.