BeyondTrust

Implement least privilege to take control of your macOS endpoint estate

Securing Mac Endpoints

5 PAM Use Cases

EXECUTIVE SUMMARY

Security for Mac endpoints is an increasingly critical, yet often overlooked need for enterprises.

Organizations once stood firm against the ever-growing employee demand for macOS devices. However, the momentum for Mac usage only continues to grow across enterprise, non-profit, and public agency environments, with some research firms estimating it will increase by as much as 20% in 2024.[1]

Today, organizations of all sizes and across all verticals – including today's largest enterprises – provide macOS devices to their employees. IBM, one of the first large enterprises to offer macOS devices, has been a major proponent of Apple in the Desktop estate.

The likelihood of receiving a silver, unibody laptop on your first day at work is higher today than ever before. In fact, a Parallels survey reported that 55.7% of small to medium-sized enterprises (SMEs) now use or permit the use of Macs.[2] Consequently, the attention of IT organizations, long focused on managing Windows devices, now must extend to also prioritize macOS devices.

One of the simplest, yet most impactful, ways to take control of your macOS endpoints and prevent breaches is to implement least privilege by removing excessive standing privileges from your users. However, without the right endpoint privilege management solution in place, removing excessive privileges can create roadblocks to productivity.

BeyondTrust Endpoint Privilege Management for Windows and Mac enables organizations to remove local admin rights and enforce least privilege across their macOS and Windows estates fast, without sacrificing end-user productivity.

[1]Online Article. Computerworld. Aug 28, 2023.
[2]Parallels survey

As a core component of BeyondTrust Privileged Access Management (PAM) solutions, Endpoint Privilege Management for Windows and Mac offers the following capabilities to help organizations harden their security posture seamlessly across their Windows and macOS estates:

True Least Privilege
Give just enough access for only the finite moments needed, and only to the appropriate application or process, so users never have access to risky privileges.

Granular Application Control
Gain control over what applications users can install or run — without impacting productivity or creating management overhead.

Reporting & Visibility
Monitor user activity through customizable dashboards and reports; seamlessly update policy based on user activity to continuously bolster your security posture.

Rapid Deployment & Streamlined Management
Deliver fast time-to-value, alleviate the IT service desk workload, and minimize business disruption with prebuilt QuickStart policy templates and robust support.

This guide shares common privilege management use cases for macOS and demonstrates how **BeyondTrust Endpoint Privilege Management for Windows and Mac** addresses them.

5 Common Use Cases *for* Securing Mac Endpoints with Endpoint Privilege Management for Windows and Mac

USE CASE

1

Removing admin privileges from a developer team— *without compromising productivity*

Developers are required to complete complex and dynamic tasks as a part of their day-to-day jobs. Many of these tasks require admin privileges to complete, leading organizations to grant standing privileges, which are persistent and "always-on", to their developers to give them the flexibility needed to do their jobs. These standing privileges create a large security risk, exposing the organization to both external and internal threats.

SOLUTION

Endpoint Privilege Management for Windows and Mac enables organizations to quickly remove standing admin privileges and allow their developers to log in with standard user accounts, without compromising their productivity or performance.

Pre-built QuickStart policy templates featuring low, medium, and high flexibility workstyles are available out of the box, allowing you to customize the level of flexibility needed by different teams and individual users throughout the organization. These templates enable you to rapidly operationalize least privilege and make quick leaps in risk reduction.

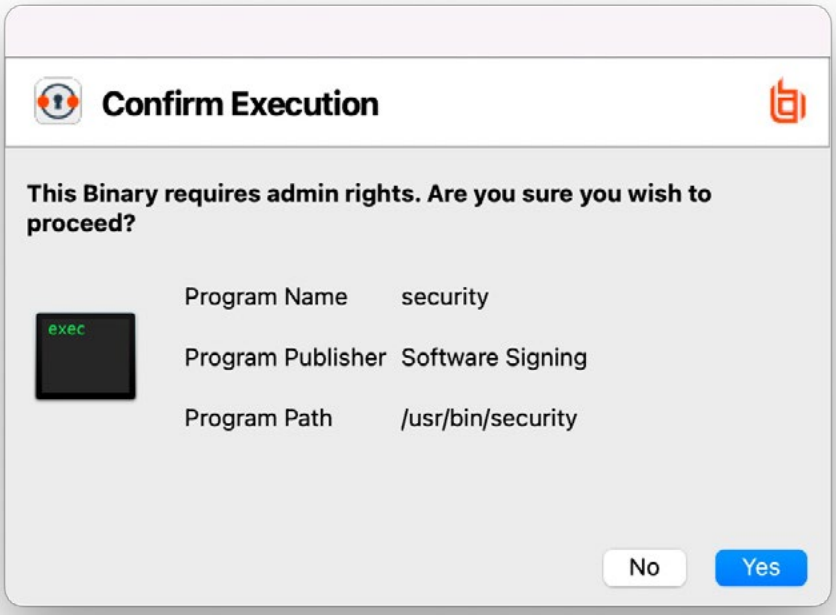
Since developers are required to complete more complex and dynamic tasks than most users, they are a great fit for the high flexibility workstyle. This is the most flexible workstyle offering and is highly configurable to allow you to offer a tailored end-user experience.

Under the high flexibility workstyle, when developers go to complete a task that requires admin rights, they will be met with a message dialog that requires them to complete an action before proceeding. This action is configurable based on the task the end-user is trying to complete.

Here are two examples of message dialogs that a high flexibility end-user might see:

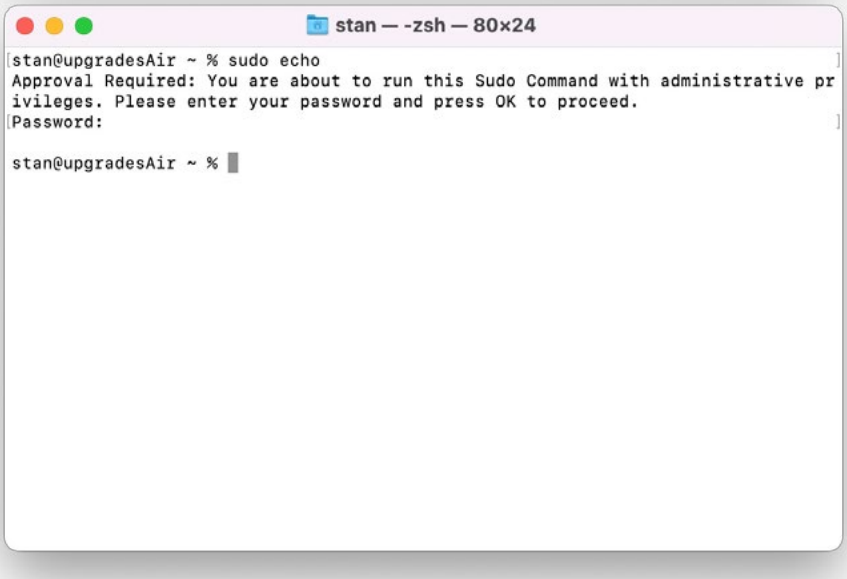
Example 1

Requires the end-user to acknowledge that the task they're trying to complete requires admin rights before proceeding.



Example 2

Requires the end-user to authenticate by entering their password before proceeding.



2

USE CASE

Removing admin privileges from a marketing team— *without compromising productivity*

Marketing teams typically do not perform many tasks requiring them to have admin privileges, but they do still require some flexibility in their day-to-day work. Some of these privileged tasks may include installing and running applications, changing settings, connecting to printers, and more.

SOLUTION

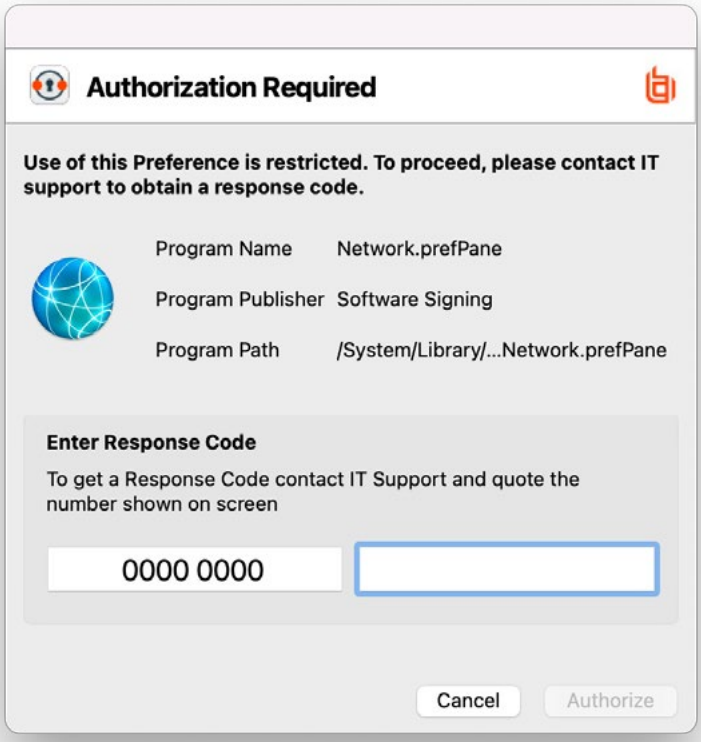
Because of this, marketing teams are typically best suited to the low flexibility workstyle within **Endpoint Privilege Management** for Windows and Mac.

Under the low flexibility workstyle, when an end-user needs to complete a task that requires admin rights, they will be met with a message dialog presenting them with a "challenge-response". This means that the end-user must enter an IT-generated PIN code to proceed. This allows a relevant and knowledgeable IT professional to verify any software installation or system change as low risk before being completed.

Here are two examples of message dialogs that a low flexibility end-user might see:

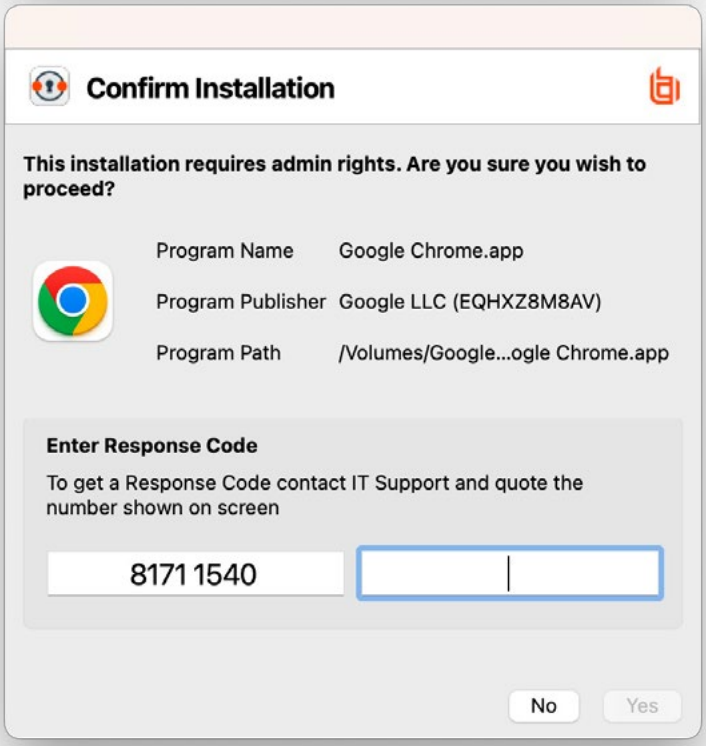
Example 1

Requires the end-user to enter an IT-generated PIN code to proceed in updating a preference



Example 2

Requires an end-user to enter an IT-generated PIN code to proceed in installing an application



3

USE CASE

Preventing users from running or installing unwanted applications

Not all endpoint attacks need to leverage privileges to compromise a machine. That's where Application Control steps in.

Application control stops users, threat actors, and other applications from installing or running any inappropriate commands or applications on an endpoint. This allows you to decide what applications a user can run, regardless of privileges, and allows you to define good and bad applications based on business needs and reputation-based models.

SOLUTION

With other endpoint privilege management solutions, application control is often a highly manual process, and can be extremely resource-intensive to maintain. **Endpoint Privilege Management** for Windows and Mac makes implementing and maintaining application control simple and straightforward.

When you first deploy Endpoint Privilege Management for Windows and Mac to the endpoints in your estate, the recommended approach is to initially set all users to the High Flexibility workstyle within the QuickStart policy template. This means that all users will immediately start operating with standard user accounts but will still be able to execute any tasks they need to.

Once the High Flexibility workstyle has been implemented, Endpoint Privilege Management for Windows and Mac will start monitoring and collecting data on all privileged activities your users are executing. Through the reporting and analytics functionality, you can utilize that data to build tailored application allow and block lists, which will define which applications your users can install or run on their machines. Allow and block lists are built using specific binaries, packages, and bundles to best configure the end-user experience.

Once you have built your allow and block lists and are ready to initiate application control, you can begin transitioning end-user groups to medium and low flexibility workstyles based on the characteristics and needs of your organization.

4

USE CASE

Achieving compliance and simplifying forensics, with auditing and reporting

Understanding your users' activity is not only important for the day-to-day management of your estate, but is also vital to achieving compliance, qualifying for cyber insurance, and streamlining forensic investigations. You need to maintain full visibility of all privileged activity being executed on every endpoint across your (multi) cloud and on-premises estate.

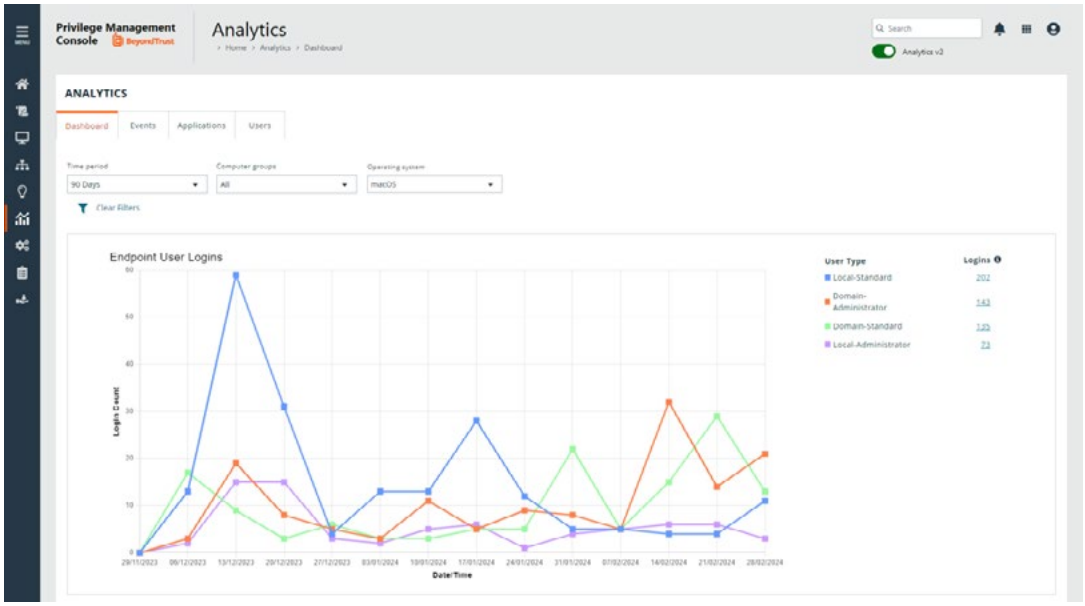
SOLUTION

Endpoint Privilege Management for Windows and Mac provides a single audit trail of all privileged user activity in addition to comprehensive reporting functionalities.

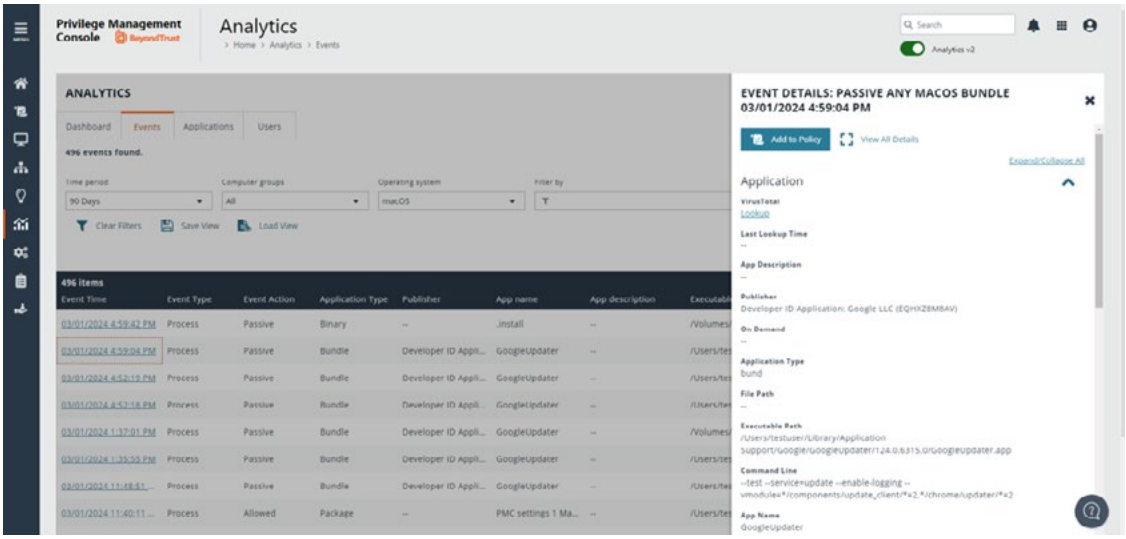
Streamlined, actionable insights make it easy to cut through the noise, and granular data options allow you to see as much detail as desired. Customizable reports and dashboards allow you to build the analytics needed to meet your unique requirements. These capabilities empower you to achieve compliance, qualify for cyber insurance, quickly facilitate forensic investigations, and continuously refine and improve your security policies.

Here are some examples of the dashboards and reports that you could access in Endpoint Privilege Management for Windows and Mac:

Example 1
The Analytics functionality enables organizations to easily gather insights from their user behavior data, either at a high-level or in granular detail



Example 2
Shows the details of a single privilege elevation event on a Mac endpoint



5

USE CASE

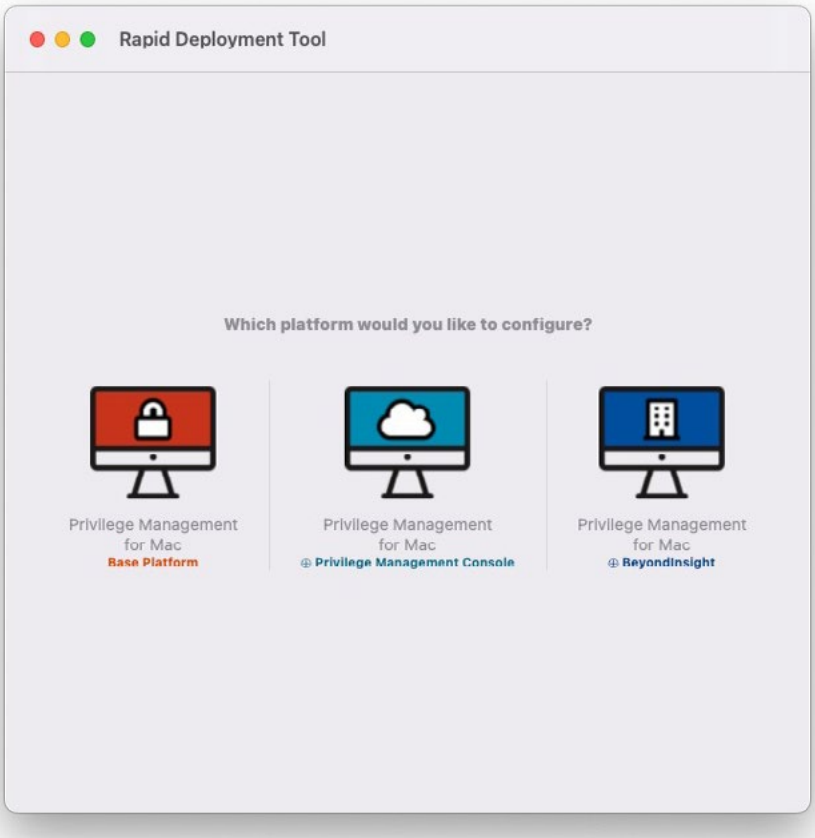
Deploying an endpoint privilege management solution easily and efficiently

SOLUTION

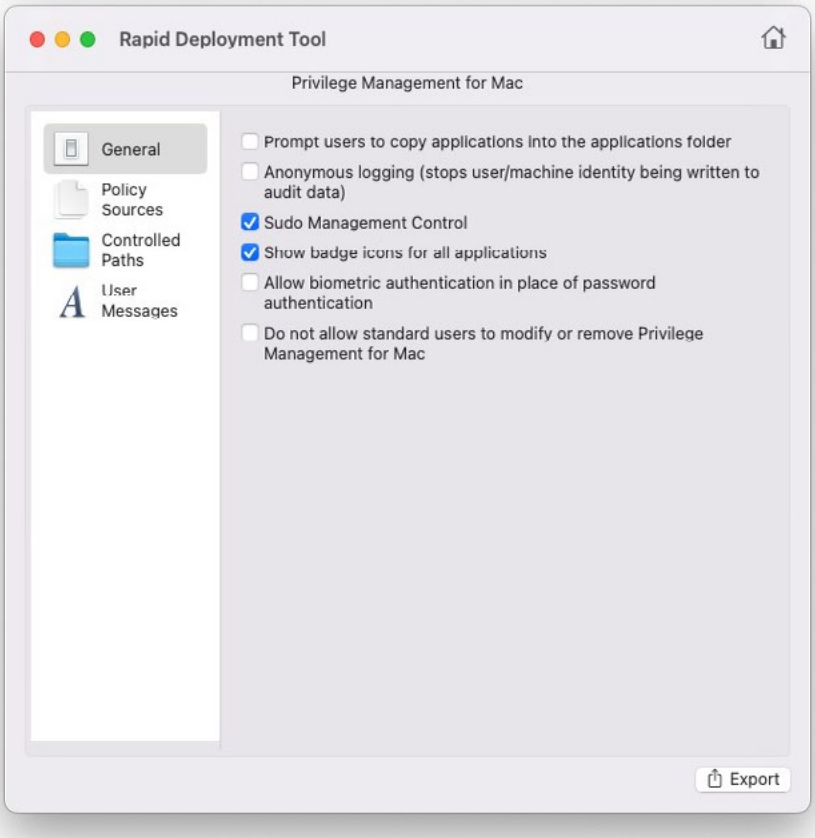
Leveraging years of deployment scenarios across thousands of complex organizations, BeyondTrust has streamlined the Endpoint Privilege Management deployment process, allowing you to rapidly protect your estate.

The Rapid Deployment Tool was designed by BeyondTrust to assist organizations in quickly and easily onboarding an estate of Mac endpoints without the need for their IT, or other responsible departments, to manually configure each endpoint.

The Rapid Deployment Tool



The Rapid Deployment Tool allows you to configure the settings that will be rolled out to your macOS estate



The tool creates distributable packages (PKG files), which deploy configurations for Endpoint Privilege Management for Windows and Mac. Organizations typically use a mobile device management tool such as Jamf to deploy the PKG files to endpoints.

Endpoint Privilege Management Reviewed by Our Customers

"Competitor solutions were bulky and had difficult processes to set up and apply. BeyondTrust Endpoint Privilege Management seamlessly integrated with our internal process and created an exceptional outcome."
– Vikas Vijaywargiya, CIO, Zensar

"Everybody tries to sell you the world and then gives you a little bit. BeyondTrust is different. They have given us more than we even knew was possible."
– Tommy Green, VP Information Systems & Technology, Amoco

"We've got a team of six engineers who manage the entire desktop and mobile estate, so we needed something that was really going to empower them to get the job done in as quick and efficient way as we can. Using [Endpoint] Privilege Management for Windows and Mac really opened doors to allow us to do that."
– Ryan Powell, Operations & Response Centre Manager, University of Derby

"If you are looking for a solution that allows you to quickly and easily eliminate admin rights, I have no hesitation recommending [Endpoint Privilege Management for Windows & Mac] to any organization."
– Application Support Manager, Seyfarth Shaw

"BeyondTrust provides a powerful platform that allows us to streamline and standardize application control and privileged management across our entire organization. Our people are smarter and better protected, and that's great news for our business."
– Dan Bartlett, Senior Consultant, Ramboll

"BeyondTrust pushes us to be better... From sales to support to engineering, BeyondTrust has always extended dedicated care and attention to our projects."
– David Lokke, Senior Systems Administrator, PREMIER Bankcard

Privilege Management Across Your Entire Estate

More about BeyondTrust Endpoint Privilege Management

BeyondTrust Endpoint Privilege Management enables organizations to enforce least privilege dynamically to prevent malware, ransomware, and identity-based attacks and achieve compliance across Windows, macOS, and Linux desktops and servers. The unmatched support provided by BeyondTrust, including white glove technical validation, streamlined professional service engagements, and robust ongoing technical support, ensures easy deployment and ongoing management.

Next Steps & Resources

Contact BeyondTrust today to schedule a demo of Endpoint Privilege Management for Windows and Mac and view these additional resources.

Gartner Magic Quadrant for Privileged Access Management

A Guide to Endpoint Privilege Management

Buyer's Guide for Complete Privileged Access Management (PAM)

Cyber Insurance Checklist

Endpoint Privilege Management Case Study: Ramboll

BeyondTrust

BeyondTrust is the worldwide leader in intelligent identity and access security, enabling organizations to protect identities, stop threats, and deliver dynamic access. We are leading the charge in innovating identity-first security and are trusted by 20,000 customers, including 75 of the Fortune 100, plus a global ecosystem of partners.

Learn more at beyondtrust.com