It's All About the Endpoint: Protecting and Enabling End Users with Least Privilege

By Dr. Eric Cole

Sponsored by BeyondTrust

ecole@secureanchor.com www.secureanchor.com

Secure Anchor is All Cyber Defense, All the Time

PREVENT | DETECT | RESPOND

Table of Contents

It's All About the Endpoint: Protecting and Enabling End Users with Least Privilege

Eric Cole

Introduction

In today's threat environment, breaches are inevitable. So, while trying to prevent breaches is important, we need to accept the reality that breaches will happen, and implement tools and processes that limit the impact or meet the appropriate risk appetite.

The reason why organizations headline the news after an incident is not necessarily just because they had a breach of systems, but likely because they failed to adequately control and contain the damage caused by the breach. It is the damage that is what ultimately impacts an organization--and damage is directly tied back to exposure of critical information and / or disruption of systems.

In today's cloud-first, mobile-first world, sensitive and business critical information is increasingly accessible via mobile endpoints. In most organizations, the endpoint is the exposure point that too often is a low priority. If you look at the specifications for typical endpoints (i.e. laptops, notebooks, and tablets), today they are not fixed location devices; they are tantamount to portable servers. The laptop that I am using to write this paper has more storage and computational power than a top-of-the-line server from only 15 years ago. The amount of information available and stored on one laptop can represent a significant loss to an organization if it was stolen or compromised. In addition, most laptops are directly accessible to the Internet via both public (Wi-Fi) and private networks in order to access various cloud based services, which makes it a viable attack vector for adversaries.

Many organizations will claim, "we have full disk encryption; therefore, our endpoints are protected." The problem with this logic is once a user logs in, or their credentials are stolen, endpoint encryption provides minimal protection for data on the endpoint. If a user logs in and is connected to the Internet and the device subsequently gets compromised, the exploit (malware or hacker) gains full access and full disk encryption is essentially moot at this point. The primary measure required to properly protect an organization is to control and manage access to the critical information that is both stored on the laptop and accessible to the various user accounts on the system.

The primary measure required to properly protect an organization is to control and manage access to the critical information that is both stored on the laptop and accessible to the various user accounts on the system.

This white paper will explore the four pillars of protecting the endpoint – least privilege, application control, password management, and user behavioral analytics. When used in concert, these capabilities will better secure access to critical enterprise data.

Four Pillars of Protecting the Endpoint

In any area of security, there is no single, silver bullet technology that will protect and secure a system. However, by taking an integrated, defense-in-depth approach to endpoints, proper security can be implemented. In building a robust foundation for securing the endpoint, there are four key components that need to be addressed:

- *Least Privilege* – One of the fundamental rules of security is that any entity, or user, must be given the least amount of access they need to do their job. If in doubt, do not provide access. The main issue with least privilege is maintenance of the access. Just because someone needs access today does not mean they need access in the future. Removing access is key to maintaining an appropriate level of least privilege.
- *Application Control* – Adversaries will typically target and exploit applications to allow long-term access to a system. By compromising key applications, malicious code can be injected or tied to the applications. Email and web based applications are often targeted in this manner. By carefully controlling and managing applications, security teams can not only bolster security of the system, but make it much more difficult for an adversary to cause harm.
- *Password Management* – In the case of traveling laptops that are directly accessible from the Internet, in many cases the first and only line of defense is authentication. Regardless of all of the security software installed on the system, if an adversary can gain access to your password or an enterprise credential, they will have access to the system. Least privilege will help minimize the damage--but ultimately, controlling and managing the authentication credentials will keep an adversary out of the system.
- *Behavioral and Threat Analytics* – You may be familiar with the security mantra, *prevention is ideal, but detection is a must.* Ultimately, we have to recognize that systems will be compromised and, thus, timely detection is critical to finding and stopping the exploit. Advanced hunting mechanisms that utilize behavioral and threat analytics can be deployed to quickly identify and track down adversaries. Visibility into the activity in all four of these recommended controls will ensure that any behavior analytic tools has sufficient information to analyze and identify when threats are likely occurring. It is not enough to have least privilege or application control alone if the events related to each action are not centrally collected, processed, and monitored in a manner that allows IT to take timely and appropriate action.

The goal of security and protecting the endpoint is focused on managing risk which is all about managing access to the system and related information.

Each of the above four components will be discussed below in more detail, but remember, the goal of security and protecting the endpoint is focused on managing risk which is all about managing access to the system and related information.

Least Privilege

There are three core areas of focus when managing and controlling access: Authentication, Authorization and Accountability. We call it 3As. Authentication is focused on verifying the identity of an individual and proving that someone is who they claim to be. Authentication will be covered in more detail under the Password Management section.

Authorization is controlling and managing what access an individual has and is the focus of this section. Accountability is tracking and monitoring what a user account is doing, looking for and finding indications of a compromise. Accountability is covered in more detail under the Threat and Behavioral Analytics section.

The key component of authorization is least privilege: giving someone the least amount of access they need to do their job, and properly maintaining that access. The two big problems with least privilege are **minimal access** and **expiration of access**. When assigning or providing access, in many cases an admin is not sure whether or not someone needs access. In the past, if an admin was not sure if a user needed access, the default rule was to go ahead and provide the user with access. While this potentially minimized support desk calls and user frustration, it introduced considerable risk.

If you provide additional access and it is not needed, no one ever notifies the help desk. Ultimately, providing access to a user beyond what he or she needs to perform his/her role leads to a massively increased attack surface that leaves organizations wide open to damage from hackers and insiders.

However, if we have a paradigm shift and not provide access unless we are 100% sure of a user's need, the system will stay in a secure state. Now, if the access is not provided and it is needed, the user can notify the help desk, get appropriate approval, and then get the access added. In light of many disastrous real world examples of privileged access gone wild, this is a much safer and smarter approach to managing access. If it is intelligently implemented, the initial user frustration and help desk calls can be mitigated with granular policies, versus broad strokes of privileged denials.

The second big problem with data access is expiration. In most organizations, once access is provided to a piece of information, it is never removed. This leads to what I call *the sticky principle*. Over the course of employment at an organization, as a user's role and responsibilities change (or the technologies they need to access grow), more access is granted to the user. However, rarely is the previous access, when no longer relevant to a user's role, removed. I have seen this in many organizations where someone who has worked for the company for 20 years in various different roles and, thus, has accumulated access to almost every piece of information and system. Thus, a best practice is to set expiration dates for access. Therefore, after a certain period of time, if the access is not renewed or extended, it will expire and proper access will be maintained on the system. This is analogous to the expiration of your password and requires a simple periodic reset.

Discovery is key

A key component of controlling access and maintaining least privilege is data discovery. Access is all about managing, controlling, and protecting critical information. However, if you don't know what your critical information is and where it is located, how can you properly protect the information?

With endpoints, it's all too easy to copy critical information, and consequently, key pieces of information will often exist in a large number of locations, which is unwieldy to control and manage. If a manager

sends a critical customer proposal with sensitive information to their team to review, most people will save a local copy on their system. Now that information exists in many locations and control of the information has been lost. Fortunately, there are still several ways of managing this information sprawl, but it requires a change in mindset.

The first approach is to limit the information that is allowed to be stored on endpoints. Either by buying systems with small hard drives, or by utilizing thin clients to reduce the amount of information and exposure that exists for a single system. While this approach does work in some cases, it is not always scalable with regards to mobile laptops and the ability to be able to work and access information without an Internet connection. In those cases, endpoint-based access control software is critical to manage and control what information can be accessed and when it can be accessed. Just because information resides on a laptop does not mean it should be accessible at all times and in all locations.

Frequently, when a system gets compromised, there is a lot of extraneous data that the user has access to that was not required for them to do their job. This means that, for a large percentage of the information stolen, the user did not require it. If it had been properly maintained, the amount of damage from the attack would have been greatly reduced. See figure 1.

Figure 1 – When accounts get compromised, the data stolen is not aligned with the data that was required for that user

While performing data discovery, it is important to:

1. Understand where critical information is located,
2. Determine who needs access to the information, and
3. Control access to minimize potential damage.

Controlling and managing access is how you win in security.

The easiest way to think about data access is to consider that the more access a given user has, the more exposure is created when their account and/or credentials are compromised. In any given system, it's only a matter of time before a certain number of user credentials become compromised. While multi-factor authentication can help, to a point, to prevent this from happening, controlling damage by minimizing exposure provides an optimal level of protection. Controlling and managing access is how you win in security.

If controlling and managing access is the first step, then monitoring and revoking access is a close second. When an account becomes compromised, there is a distinct difference in behavior patterns that can be observed – assuming this information is being logged and monitored. While monitoring is discussed below, it is important to bring it up under least privilege to emphasize that with careful analysis, data breaches can be detected early, which aids in containing the damage. Ultimately, the best way to stop access is by revoking access when it is no longer required. For example, if a user has privileged access to a system that has not been used in "n" days, why are they still granted access to that privilege? It is analogous, to setting the archive bit on a file and after a period of time, allowing the backup solution to archive the file since it is stale.

This step sounds so simple, yet it is often overlooked. I have seen cases where employees have left the organization and their accounts remain active. In addition to revoking access of employees who left the organization, managing access for dormant accounts is just as important. Often, when organizations implement systems or new processes, they will set up accounts for everyone in the organization with a default account, requiring users to change the password after the first time they login. However, in many cases employees never login in and/or never use the system. Yet, those accounts remain active and are sitting targets for hackers. The reason why hackers love dormant accounts is because, all too often, no one will notice if the account is being use for anomalous purposes. Therefore, all accounts must be carefully monitored, any employees or contractors who left the organization must be removed, and any dormant accounts that have not been logged into for a certain period of time must be disabled. This is true for any local accounts, applications, cloud resources, and even partner systems that are outside of the management policies an organization maintains.

Use case: Elevate rights to applications, not users

It's difficult to strike the right balance between security and enabling end users to do their jobs unencumbered by constant IT roadblocks. Enforcement of least privilege in an adaptive model – applying situational policies and elevating by application– is essential. This approach transparently grants the rights users need to do their jobs without exposing the organization to unnecessary risk.

The best practice here is to eliminate admin rights and grant privileges to applications and tasks – not users – without providing administrator credentials, helping to achieve privilege and closing potential security gaps.

When evaluating least privilege solutions, consider the following must-have capabilities:

- Elevate rights to an application, not the user
- Report on privileged access to file systems for all users
- Document system changes during privileged sessions
- Monitor sessions, capture screens, and log keystrokes during privileged access
- Provide a technique for using real domain or local privileges when required
- Integrate with other privilege solutions to achieve comprehensive privileged account management

Application Control

In the late 90's and early 2000's when adversaries were mainly targeting visible servers to break in over the Internet, the main method for combatting this threat was locking down the servers. This could include removing any components that were not needed, closing down ports, and removing services. Now, with everything moving to the endpoint, the same logic applies to protecting the endpoint – lock down the system. The good news is that endpoints, including laptops, should not have any open ports visible, so one level of the hardening process becomes easier.

> ***In talking about hardening and securing the endpoint, it is all endpoints, not just Windows systems.***

On the other hand, the main vector of attack for endpoints is tricking the user to cause harm and infect his/her system. IT organizations will often claim that they have hardened, locked down configurations for their endpoint, but in digging deeper, this only refers to secure configurations for their Windows endpoints (because Windows has typically been the target of attack). However, exploits increasingly target Linux and Mac, which IT should be weary of, because more and more endpoints are running Linux and Mac. Therefore, when I talk about hardening and securing the endpoint, it is all endpoints, not just Windows systems.

From an endpoint security perspective, the two most dangerous applications on the planet are: email and web browsers. In securing applications, email and web have to be at the top of the list to verify they are running at a minimal level of access, fully patched, and carefully controlled and monitored. One of the tricks that I perform with my clients is to run the mail client and web browser in separate virtual machines. What is nice about this trick is that it is completely transparent to the user; they have no idea that this is happening, but it makes it very difficult for the adversary to cause harm. By running dangerous applications in a virtual machine, if the user opens an attachment or clicks on a link, the virtual operating system will be infected, not the host. When they close down the application, the virtual operating system goes away, and with it, all of the malware. In this case, a system is still being infected, but the damage is contained and controlled for a short period of time with no lasting effects.

Whitelisting

One of the best and most effective ways of controlling and managing applications is to implement application whitelisting. With application whitelisting, all applications that are installed on the system are verified/validated and all components that are used by the application are cryptographically hashed, digitally signed, and/or verified. With application whitelisting, no new software can be installed and nothing that runs can be altered, changed, or modified that has not been approved. From a security perspective, this provides a robust level of security that makes it difficult for the adversary to cause any damage to the system. On the downside, application whitelisting is very restrictive and typically works best in environments that are simple, static, and homogenous.

The more complex and dynamic the environment, the harder it is to implement application whitelisting. To overcome application whitelisting challenges, we perform an opt-in rollout with many of our customers. Based on the impact it has on being able to update and install applications, application whitelisting is not installed by default. However, if a user gets their system infected because they made

a bad decision by clicking on a link or opening an attachment, they have opted in to the program in full force. When they receive their computer back from being rebuilt, application whitelisting is now active, versus potentially a listen-only mode used to drive behavior analytics. The beauty of this solution is that most compromises of the endpoint originate from a small number of users who have routinely made poor decisions. If via self-selection you can identify those users and lock them down, you can significantly reduce the likelihood of compromise.

Endpoints and the Cloud

Many cloud based applications are available via web-based portals and web-based tools, which dramatically simplifies the configuration and number of applications that reside on the desktop. The more cloud- based integration that can be performed, the less applications that have to be actively managed. While a browser is still required, locking down and securing one application (the browser) is easier than trying to manage and secure a large number of complex applications. As your organization migrates more to the cloud, determine the extent to which your providers have cloud based applications. If all of the core applications you need are cloud-based, both configuration and application management become straightforward because you have a simple, static environment.

Use case: Vulnerability-based Application Management

In maintaining which applications can and cannot run, you have to eliminate risks associated with malicious and vulnerable software. What happens when we allow, or in some cases, have to elevate, applications that carry risk of exploitation? Aren't we potentially allowing hackers in at a risk commensurate to letting our users run with Admin rights? Vulnerability-based application management (VBAM) is a concept that helps organizations immediately evaluate the risk threshold of an application at the time of elevation. The risk threshold is unique to your organization's risk requirements, and if that threshold is hit or exceeded, the application can be stripped of Admin rights or denied.

When evaluating application control, consider the following must-have capabilities:

- Vulnerability-based application management – make least privilege decisions for applications based on that application's vulnerability, risk, and compliance profile
- Quarantine files if there are suspicious vulnerabilities
- Leverage an integrated data warehouse and analytics across the privilege landscape

Password Management

Authentication is the entry point into a system, and with portable laptops, it is often the first and only line of defense. If someone can hijack, crack, or intercept your password they can often gain access to all of the information that is stored on your system. Man in the Middle (MTM) attacks are notorious for executing this type of breach. With the cloud, these attacks become even more detrimental since, in many cases, people use the same password for multiple accounts. Therefore, if one cloud-based account becomes compromised, an adversary would often have access to multiple accounts and a trove of information. This is why utilizing a multi-factor authentication method, especially for cloud, is highly recommended. The simple multi-factor methods involve texting the user a one-time password after they authenticate with a userid and password. This provides an extra level of protection to ensure that it is the proper user of the account, and only works for one service at a time.

> ***Since most users do a poor job at monitoring and tracking passwords, password vaulting takes it out of the user's hands and creates a secure way to efficiently manage and protect a large number of credentials.***

When multi-factor authentication is not an option, it is important to utilize robust passwords that are carefully managed with proper complexity controls in place, and never duplicated between resources. Hackers will target passwords, so it's important that they are long, hard to guess, and changed periodically. The problem with these requirements is that, while these restrictions often make it hard for an adversary, it induces users to either write down the password in an unsecure manner or use the same password for multiple accounts. Neither one of those options is acceptable. Therefore, we encourage organizations to move from passwords to passphrases, or highly complex passwords, that are under management. Passphrases are generally easier for the user to remember and more difficult for the adversary to guess, so in these cases, we now achieve a scalable solution. Highly complex passwords that are under management are not human-friendly for documenting and are best used for machine to machine communications and impractical for humans to say, type, or even write down. This approach falls under password safe or password vaulting solutions.

Another problem with passwords is that users often have many of them. It's not uncommon for a user to have at least a dozen applications that each require authentication, and this only increases with the use of the cloud. Even though users are instructed to not use the same password for multiple applications and/or not write them down in an unsecure manner, faced with the option of a dozen passwords, one or both of those options are going to happen. In order to stop users from practicing bad security, it is important to provide them appropriate options. One such option is single sign on (SSO). SSO solution are highly scalable. By leveraging SSO, a user has one set of credentials that can be used to access several applications within the organization. The problem with SSO is if that one set of credentials becomes compromised, an adversary would have access to all of a user's associated accounts. To overcome this problem, SSO solutions need to utilize multiple factor authentication, which would include a one-time password to make it very difficult for their credentials to be compromised.

While SSO is a scalable option within an organization, it does not work well with cloud-based applications. In these cases, distributed SSO solutions are available for use on the endpoint which is often called password vaulting. The way these solutions work is that each application has a different, complex password that is stored securely on the system. The user would authenticate once and the password manager would automatically manage all of the various complex passwords and authentication. Again, this solution is acceptable if the authentication to the password manager is based on robust multi-factor authentication. In addition, since the user does not have to remember the various passwords for the applications, it is ideal for these passwords to be complex and to change frequently to minimize the risk of compromise.

Password vaulting solutions can also take password management to the next level. With password vaulting, passwords can be kept secure, rotated and tied directly into to access control mechanisms. Since most users do a poor job at monitoring and tracking passwords, password vaulting takes it out of the user's hands and creates a secure way to efficiently manage and protect a large number of credentials.

Use Case: Using real credentials for application access

Users need to run applications that interact with other machines. More specifically, users sometimes require administrative access to one or more remote hosts. A good example of this would be running Event Viewer to view remote logs, or AD Users and Computers from an administrative, (Non DC) workstation. A least privilege product would not allow for remote elevation. However, least privilege paired with password management enables a user to call an application using approved alternate credentials, without having to know the password for that account. This provides a secure and efficient method to maintain a least privilege model.

When evaluating enterprise password management solutions, consider the following must-have capabilities:

- Automatically rotate enterprise credentials and SSH keys according to a defined schedule, enforcing granular access control, workflow, and auditing over their use
- No requirement for additional third-party tools or Java for session management – utilize native tools (e.g. MSTSC, PuTTY) instead
- Provide context to workflow requests, considering multiple factors to determine access
- Full network scanning, discovery, and profiling with auto-onboarding
- Build permission sets dynamically according to data from scans
- Get control over scripts, files, code, and embedded keys
- Enable true dual control with the ability to lock, terminate, or cancel a session
- Leverage an integrated data warehouse and advanced threat analytics across the privilege landscape
- A clean, uncluttered user interface (HTML5) for end users that speeds adoption

Threat and Behavioral Analytics

Regardless of the motives of a hacker, the main component of damage is often associated with compromising, altering, or destroying critical information that is needed in order to run the business. It is an unfortunate reality, but organizations are going to get compromised.

In designing security, especially for the endpoint, robust measures are deployed to prevent compromise, layered with defenses to minimize the damage that is caused by a compromise, but ultimately, we need to be able to detect the compromise within a timely manner. Since, on average, organizations are often compromised for close to a year before being detected (according to the Verizon Data Breach Report), IT organizations have concluded that finding a compromised system is very difficult. Fortunately, that is not the case. Revealing compromised systems is straightforward when the right tools and processes are implemented. Too many organizations still fall into the trap of putting all of their security eggs in the prevention basket, so when that fails, they have scant resources dedicate toward detecting and tracking an exploit that is in progress.

> ***By carefully monitoring, watching and tracking any changes in behavior, which include data access, applications, services and network activity, distinct differences can be detected to indicate that a compromise has occurred.***

When an endpoint becomes compromised, there are distinct differences in what activity a normal user performs and what activity an adversary would perform. By carefully monitoring, watching and tracking any changes in behavior, which include data access, applications, services and network activity, distinct differences can be detected to indicate that a compromise has occurred. This data can be derived from all of the disciplines discussed in this whitepaper.

From a host-based activity perspective, software can carefully monitor what is happening on the system and detect subtle differences in behavior. A critical area to monitor on the host are files and applications that run when the system boots. One of the goals of an adversary is to maintain persistence, and this is achieved by running malicious code when the system starts. Since there is only a finite number of ways that programs can run during boot up, this is an easy area to monitor and track.

From a network perspective, a compromised system will often make a C2 (command & control) session back to the adversary so they can continue to monitor the system and cause additional harm. These connections are often fully encrypted and go to IP addresses that are not associated with legitimate or normal sites. Therefore, by carefully monitoring network connections including DNS lookups, suspicious activity can be detected. This general activity of looking for compromised systems is referred to as hunting. Threat hunting is the act of aggressively tracking and eliminating cyber adversaries as early as possible and is a key component of mitigating damage.

There is no such thing as an invisible adversary. By carefully monitoring and tracking the system, the dwell time, or amount of time an adversary is on a system, can be reduced, helping to limit any damage.

Use case: Seemingly isolated events lost amidst the noise

An application is launched for the first time. An administrator logs in at 2 a.m. A server has unpatched vulnerabilities. Seen individually, these events may be written-off as low-risk blips. When combined on a single system, in a single time period, they add up to a red alert.

It's no secret that IT and security professionals are overloaded with privilege, vulnerability, and attack information. Unfortunately, advanced persistent threats (APTs) often go undetected because traditional security analytics solutions are unable to correlate diverse data to discern hidden risks. Seemingly isolated events are dismissed as exceptions, filtered out, or lost altogether in a sea of data. The intruder continues to traverse the network, and the damage continues to multiply.

An advanced threat analytics solution can effectively detect and highlight critical IT security threats that were previously buried amidst volumes of data. Such analytics tools enable you to identify users and assets displaying patterns of risky activity by:

- Gathering, centralizing, and baselining all asset and user activity in one place
- Connecting disparate evidence to reveal hidden risks
- Checking environmental data against global threat databases
- Detecting abnormal changes that signal in-progress threats
- Spotlighting users and assets posing the greatest risk

Analytic tools must do this through a combination of multiple inputs and sources, and a powerful correlation engine to check against standard user behavior.

When evaluating threat and behavioral analytics solutions, consider the following must-have capabilities:

- Aggregate users and asset data to centrally baseline and track behavior
- Correlate diverse asset, user, and threat activity – from vulnerability management products, firewalls, malware databases, and more – to reveal critical risks
- Identify potential malware threats buried in asset activity data
- Measure the velocity of asset changes to flag in-progress threats
- Isolate users and assets exhibiting deviant behavior
- Generate reports to inform and align security decisions

Conclusion

All indications of technology point to a future of portable, lightweight endpoints with all services in the cloud. The idea of complex secure network architectures is quickly fading away, along with organizations running complex data centers, when that is not their primary business. It is more scalable to let cloud providers who specialize in delivering applications provide secure server solutions and have organizations focus on their endpoints. While implementation of this scenario a ways into the future, most organizations are starting to experience this trend in some manner.

The four critical capabilities to better control the endpoint are:

- Least privilege
- Application control
- Password management
- User behavior and threat analytics

The most dangerous components in any architecture are a) the piece that is managed and controlled by the end user, and b) the piece that contains sensitive information or access to sensitive information. Convergence has occurred and today that is all one component, the endpoint. Therefore, the more an organization can do to protect, secure, and lockdown the endpoint, the more protected their organization will be and the less chance of damage when a compromise occurs.

Appendix: How BeyondTrust Helps with Least Privilege on Endpoints

Eliminating excessive rights on user endpoints is a common starting point for many organizations to close avoidable security gaps, but legacy approaches to solving this problem are insufficient. Existing tools lack visibility into the security profile of applications targeted for elevation, and the risk-reducing effects of eliminating over-privileged users are negated if a vulnerable or exploited application is elevated for use. The traditional approach to solving these endpoint least privilege problems requires security and IT teams to cobble together point tools from multiple vendors resulting in unnecessary complexity and cost, and no visibility into user behavior throughout the enterprise.

BeyondTrust solves this problem by:

- Removing excessive rights on all endpoints, reducing risk, and simplifying least privilege enforcement
- Providing visibility into target system and asset security, reducing risk from elevated application vulnerabilities
- Providing application control on the endpoint, blacklisting hacking tools, whitelisting approved applications, and greylisting applications
- Analyzing and reporting on privileged user and account behavior, reducing risk from anomalies
- Delivering a modular, integrated platform, speeding implementations and reducing costs

Enforce Complete Endpoint Least Privilege

PowerBroker enables IT to grant privileges to applications and tasks – not users - without providing administrator credentials, helping IT to achieve the best practice of least privilege and closing potential security gaps. Policies can be applied across both Windows and Mac endpoints, providing flexibility. As a pioneer in the market, BeyondTrust holds the patent for privilege elevation.

Gain Visibility into Privileged Application and Asset Security

PowerBroker leverages vulnerability data from BeyondTrust Retina and other leading solutions to provide a complete picture of privileged application and asset security – including for network, cloud, and virtual assets. Having this zero-gap coverage reduces risk by ensuring that no assets are left unprotected, while privilege decisions are made with insight into the risk profile of the system or asset.

Ensure Complete Application Control

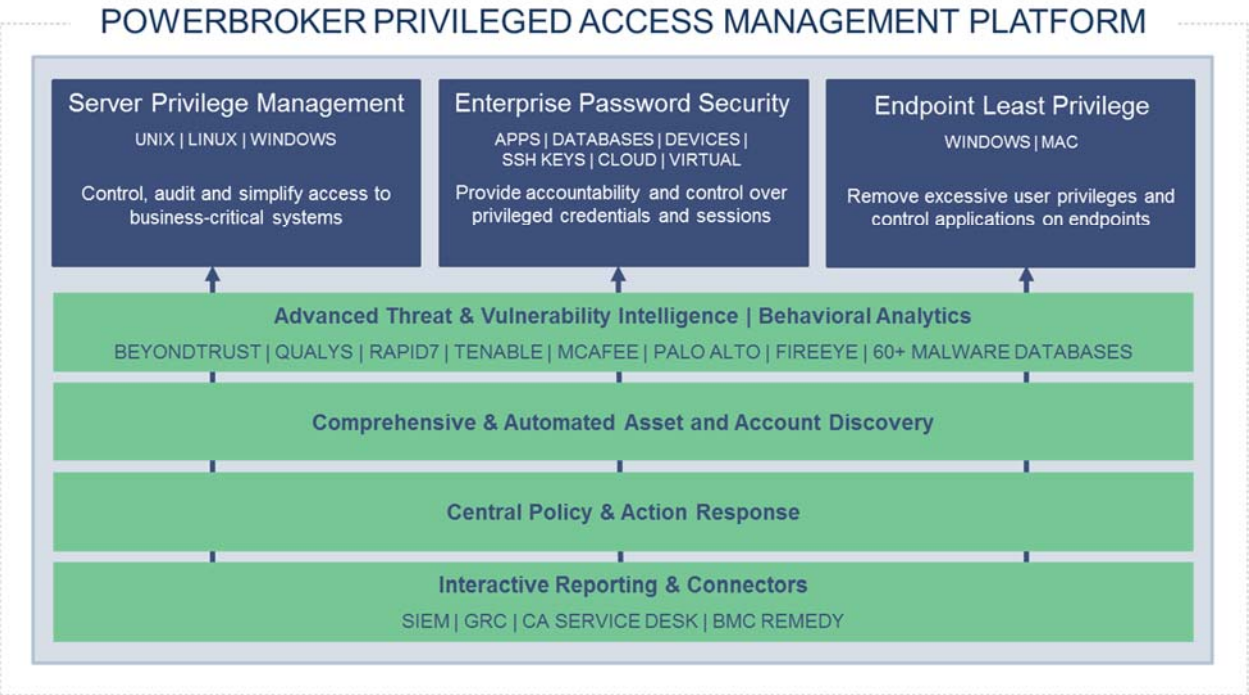
PowerBroker enables IT organizations to blacklist hacking tools, whitelist approved applications, and greylist applications based on rules to keep systems safe. This rules-based approach eliminates the need to manage complex whitelists with thousands of signatures for complete application control.

Understand Password, User, and Account Behavior

PowerBroker analyzes privileged password, user, and account behavior and augments it with additional threat attributes to assign a Threat Level – a key indicator of elevated risk – to each event based on the user, asset, and application launched. This capability makes it easier for security teams to uncover emerging risks in the organization, pinpoint specific at-risk systems, report on the findings, and take action to eliminate the threat before the potentially damaging effects of a breach.

Simplify Deployments with a Single Platform

With PowerBroker, security and IT operations teams benefit from a single pane of glass to manage their privileged access management policies and deployment, and provide reporting to multiple stakeholders. BeyondTrust delivers the PowerBroker Privileged Access Management Platform as a modular, integrated set of solutions united by common components. This approach dramatically simplifies deployments, helps to control costs, and provides a foundation to reduce the evolving risks of privileged access.



For more on how BeyondTrust solves this problem, visit www.beyondtrust.com/solutions/least-privilege-management/.