WHITEPAPER

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

5 Steps to Being Privilege Ready in Today's Threat Environment

Contents

Data Breaches Are Never a Matter of "If" 2
Too Much Access for Too Many 2
Opening the Door to the Cyber Attack Chain 3
A 5-Point Plan for Privilege Readiness 4
1. Fix vulnerabilities and reduce the attack surface 4
2. Adopt the Principle of Least Privilege 4
3. Protect privileged accounts and credentials 5
4. Report on user activity and monitor critical resources 5
5. Automate wherever possible 6
Why Privilege Readiness Matters 6
The PowerBroker Privileged Access Management Platform 7
Next Steps & Privilege Ready Infographic 7
Infographic 8
About BeyondTrust 9

Data Breaches Are Never a Matter of "If"

Humans make mistakes. These mistakes are often reversible, forgivable, and forgettable. But what about when an innocent blunder enables an attacker to gain a foothold on your network, exploit powerful privileged accounts, and take control of your organization's data?

In a world where being breached is never a matter of "if" and always a matter of "when," being Privilege Ready means breaches are fewer, they are detected faster, and – when they do happen – they're survivable.

People are an organization's most valuable resource. But they can also be its greatest vulnerability, especially when armed with weak credentials, all-too-powerful privileged accounts, and security ignorance or hubris.

Most organizations focus ample security resources on controlling and protecting the boundaries of their networks, but many pay inadequate attention to what's happening on the inside. Once an outside threat makes it to the inside, these organizations are ill-equipped to identify, impede, or stop it.

To combat today's threats, organizations must be able to monitor for suspicious behavior, take the destructive potential out of users' hands, and become "Privilege Ready."

This white paper reveals strategies to help your organization get Privilege Ready by implementing the proper privileged access management (PAM) program. Being Privilege Ready will also help make regulatory and security processes more repeatable and automated.

Too Much Access for Too Many

The problem is simple: Too many users have too much access. In 2017, a BeyondTrust survey revealed that 38 percent of organizations grant admin rights to their workforce by default, despite 79% saying it is a major security risk.

The Cyber Essentials Scheme, a UK government standard designed to help businesses with cybersecurity, warns of the powers of privileged admin accounts. Its guidance on IT infrastructure notes that "when such accounts are compromised, their greater freedoms can be exploited to facilitate large-scale corruption of information, disruption to business processes and unauthorized access to other devices in the organization."[1]

Source: BeyondTrust, "The Five Deadly Sins of Privileged Access Management"

[1] https://www.cyberessentials.ncsc.gov.uk/requirements-for-it-infrastructure.html

For example, when a user with an administrator account clicks on a phishing link, the associated malware can act with the broad access and capabilities inherent of that account. This is how simple mistakes morph into dire consequences.

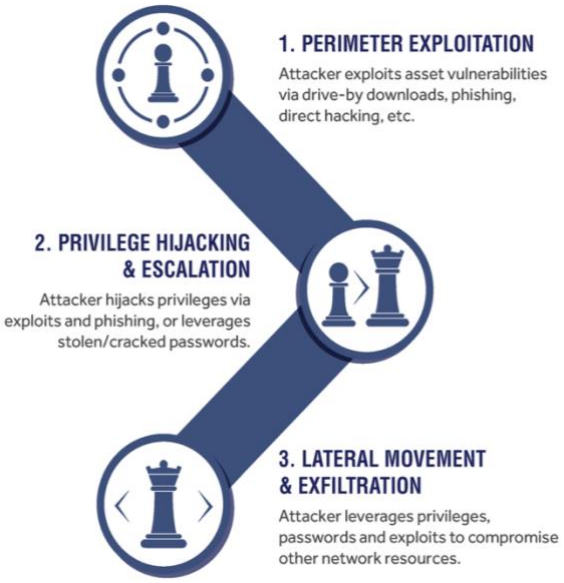
Moreover, holders of privileged accounts (such as system administrators) often share account access with other users. In practice, this means people with bad intentions or bad security habits are granted access to powerful accounts, with limited oversight.

Even if privileged access isn't readily handed out, poor security practices are rampant. For instance, the 2017 BeyondTrust survey showed that users regularly committed the security sins of reusing passwords, sharing passwords, and using default and easily guessable passwords.

Opening the Door to the Cyber Attack Chain

Unpatched vulnerabilities are pervasive. In 2017, the WannaCry and Petya attacks swept the globe, paralysing multinationals and government organizations alike. The first common element was that the attacks leveraged a vulnerability in Windows SMB protocols, for which a patch had already been released. The second common element was how few of the victims had applied that patch. When organizations don't patch their perimeter vulnerabilities or fail to account for threats within their organization, they effectively turn their security solutions off.

Attackers will exploit vulnerabilities and user privileges to gain a foothold in even the best-armored organization. They then solidify their presence by laterally moving through the network, taking control of more assets, and picking up credentials and critical data as they go.



Source: BeyondTrust, "Disrupting the Cyber Attack Chain"

The credentials the infiltrator finds may give him/her higher levels of authority within the network, control over more critical systems (like domain controllers), and increased access to sensitive data. In other words, a breach occurs.

This entire attack process – from exploiting a vulnerability to get an initial foothold, to stealthily zig-zagging throughout a network to increase access and rights – is commonly referred to as the Cyber Attack Chain. With privileged accounts and credentials exploited in 80 percent of breaches[2], controlling privileges and mitigating the threat of lateral movement can be the difference between a breached organization and a Privilege Ready one.

[2] The Forrester Wave™: Privileged Identity Management, Q3 2016

A 5-Point Plan for Privilege Readiness

Traditional security measures start at the perimeter, but they are not enough. Today's threats just burrow under or through perimeter defenses, exploiting key individuals and fault lines within an organization to cripple the entire structure. A Privilege Ready organization is prepared to solve this challenge by adhering to the following five best practices:

1. FIX VULNERABILITIES AND REDUCE THE ATTACK SURFACE

The first step to Privilege Readiness entails ensuring that the system and application vulnerabilities that could open pathways into your environment are prioritized according to risk. Vulnerabilities should be patched regularly, and this process should be automated, if possible.

Enable whitelisting to ensure that the only applications running are those that come from a trusted source. Closing off these inroads reduces the attack surface, making it considerably more difficult for an outside attacker to gain that initial foothold that would enable them to become an insider.

2. ADOPT THE PRINCIPLE OF LEAST PRIVILEGE

The second key piece of Privilege Readiness is to adopt the Principle of Least Privilege. Any end user or application should be granted the minimum possible privileges and rights they need to perform their role or function. While it might seem more efficient to grant users as much leeway as possible when working on the organization's network, this proves to be unjustifiably risky in practice.

Least privilege doesn't only apply to those who use these accounts, but also to how and when the accounts are being used. Role-based access control is key to helping least privilege work as smoothly as possible, ensuring an optimal balance between access and security, while making the actual process seem invisible.

A tiering model for access, in which even admin accounts only have access to the rights they need, will also help. This will limit the size of those highly privileged targets, meaning that it will be that much harder for attackers to escalate their capabilities when attempting to laterally move through your network.

> *Networks with strong boundary protection, but no internal security, give attackers free rein to traverse the network once they have gained access. The chances of achieving their goals will increase the longer that they're able to maintain a foothold.*
>
> - The UK's National Cyber Security Centre (NCSC) on lateral movement[1]

Admin accounts should be used separately from day-to-day, "non-privileged" accounts and only when a task requires their wide-ranging powers. This practice is referred to as privilege separation.

As Tier 1 Unix and Linux servers handle critical data, it's important to limit the potential for lateral movement. Broad access rights to these resources can equate to almost uncapped risk potential, jeopardizing your most sensitive data and assets. Either enable users to log in as themselves and elevate specific activities that they can perform, or delegate specific, granular privileges.

Organizations should also consider implementing time-based privileged access controls to prevent access at irregular hours, meaning that attackers will find it more difficult to assume powerful accounts at night or on weekends when no one is looking.

Network segregation is also included under the concept of least privilege. This involves segregating the parts of your network that do not need to be interacting. This security measure impedes lateral movement by eliminating pathways.

3. PROTECT PRIVILEGED ACCOUNTS AND CREDENTIALS

Your highly privileged and shared accounts must be discovered, grouped for easier management, monitored, and audited.

Passwords must be strong, unique, and changed regularly (referred to as password rotation). Furthermore, when using work services, passwords should only be entered into approved devices that can ensure the security of those credentials. Additionally, you should eliminate hard-coded/embedded credentials where possible and, if not, these credentials will have to be watched closely in real-time.

While passwords present an intrinsic weak link, a variety of solutions can bolster security and help prevent lateral movement within the network. These solutions include multi-factor authentication, single sign-on, and biometrics, among others. Enhanced authentication security should be applied for any internet-facing service or high-risk account.

You should strongly consider the use of automated password managers to cut down on the storage of passwords in plain text/embedded in the code, and to provide better enforcement around password security.

4. REPORT ON USER ACTIVITY AND MONITOR CRITICAL RESOURCES

Regardless of how you manage privileged access, ensure that all privileged activity is logged and monitored. This entails implementing session recording and other technologies, which can be accomplished, to some extent, by setting up screen recording and other manual processes. However, session reporting and management quickly becomes untenable in environments with hundreds or thousands of concurrent sessions. Automated privileged session management and monitoring solutions can enable streamlined visibility and control over privileged access to servers, databases, and network devices, while capturing keystrokes, text/graphical screen output, and mouse movements.

To gain deeper visibility into risk, correlate the privileged user activity reporting against other behavioral metrics. This will help you spot risky users, compromised accounts, and abnormal access by flagging suspicious behavior in your environment.

Auditing and reporting can also be automated against compliance objectives by highlighting directory changes that would threaten security or hamstring compliance, giving you the clarity and detail demanded by regulatory regimes such as GDPR.

5. AUTOMATE WHEREVER POSSIBLE

While it is possible to forge a path to Privilege Readiness through manual processes and by accumulating and implementing multiple tools, nearly the entire pathway to Privilege Readiness can be automated with solutions like BeyondTrust's PowerBroker privileged access management platform. By applying automation throughout each step – from managing vulnerabilities and enforcing least privilege, to managing privileged accounts and conducting advanced threat analysis – you can vastly reduce your organization's attack surface and become Privilege Ready.

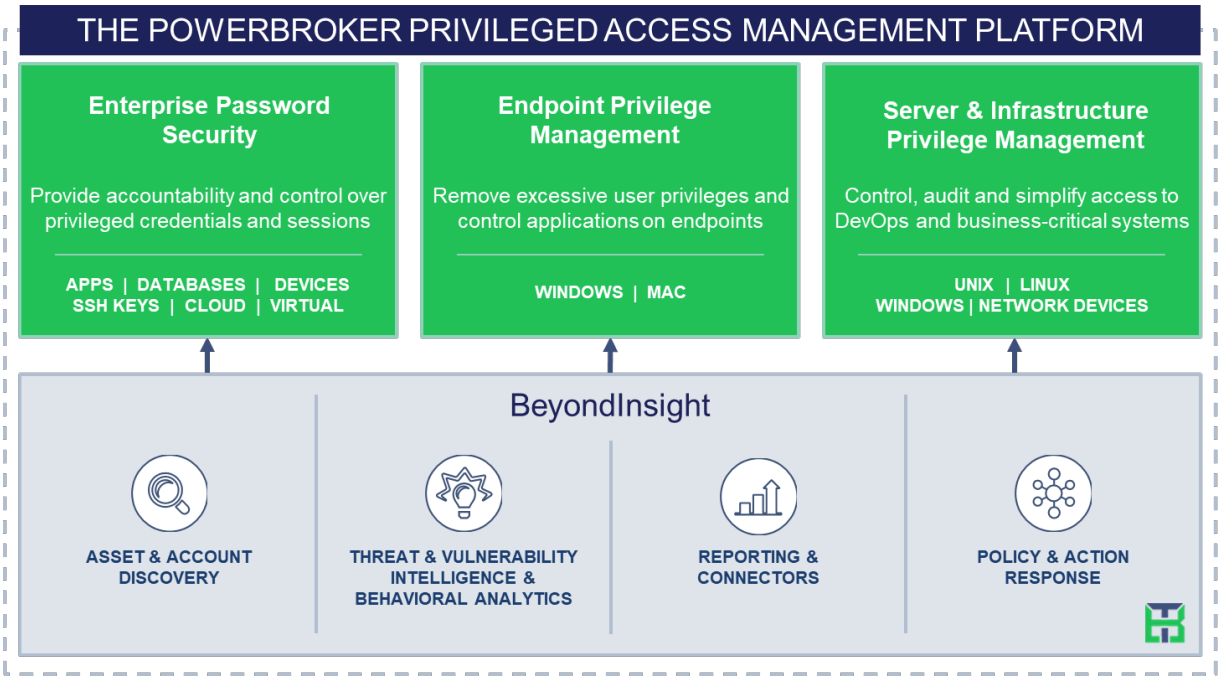
Why Privilege Readiness Matters

You should always assume that an attacker with enough time and resources will eventually be successful. When that does happen, it's important to detect those breaches as soon as possible, stop lateral movement, and limit the damage the attacker can cause.

Limiting privileges is sometimes seen as a hindrance to an efficient workflow, but it need not be. BeyondTrust solutions allow the strict enforcement of roles and responsibilities while enabling people to effectively do their jobs. The easier it is for someone to do his/her job, and to understand why a slip-up or workaround can be fatal for the organization, the better secured an organization will be. By taking that unknowable potential for harm out of users' hands, you can put them "beyond trust."

The PowerBroker Privileged Access Management Platform

BeyondTrust's solutions for Privilege Readiness are part of the PowerBroker Privileged Access Management Platform – an integrated solution to provide control and visibility over all privileged accounts and users. By uniting best-of-breed capabilities across on-premise, virtual, and cloud platforms that many alternative providers offer as disjointed tools, the PowerBroker platform simplifies deployments, reduces costs, improves system security, and closes gaps to reduce privileged risks.



Next Steps & Privilege Ready Infographic

Chances are that your organization already has some level of Privilege Readiness, but there is still work do. How do you move forward from where you are today, to where you need to be? Our free guide, Seven Steps to Complete Privileged Access Management, is relied on by organizations like yours to help mature their organisation's Privileged Readiness. This guide helps you assess your organization's privilege readiness, and guides you toward a programmatic, phased in approach to increased privilege maturity in a path that makes the most sense for your organization. Download it now.

Or, to learn more about BeyondTrust solutions, visit us on the web, request a free trial or contact us today.

5 STEPS TO PRIVILEGE READINESS

Most organizations appear secure on the surface, but many fail to focus on security beneath the IT perimeter. Here are 5 things you can do to stop attackers who dive under your boundary defenses.

1 REDUCE THE ATTACK SURFACE

Identify, prioritize and patch system and application vulnerabilities.

94% of compromises used familiar, well-worn patterns to gain an initial foothold.

2 ADOPT LEAST PRIVILEGE

Grant users the minimum possible rights and privileges they need to perform their jobs.

38% of organizations grant admin rights to users as default.

3 PROTECT PRIVILEGED CREDENTIALS

Securely store, rotate and manage passwords, SSH keys and other privileged credentials.

80% of data breaches involve the use or abuse of privileged credentials.

4 MONITOR USER AND SYSTEM ACTIVITY

Monitor, log and audit all privileged activity. Correlate behavioral data with other security data to identify potential threats.

68% of breaches aren't discovered for months, but data loss starts within just minutes in 87% of all breaches.

5 CONSOLIDATE AND AUTOMATE

Reduce complexity with unified, integrated solutions that centralize management, reporting and analytics on a single platform.

DISCOVER HOW TO MAKE YOUR ORGANIZATION PRIVILEGE READY:

WWW.BEYONDTRUST.COM/PRIVILEGE-READY

Sources:
1 Verizon, "2017 Data Breach Investigations Report"
2 BeyondTrust, "The Five Deadly Sins of Privileged Access Management"
3 Forrester, "Forrester Wave: Privileged Identity Management, Q3 2016"
4 Verizon, "2018 Data Breach Investigations Report"

BeyondTrust™

About BeyondTrust

BeyondTrust® is a global cybersecurity company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Access Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.