WHITE PAPER

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

Fusing Vulnerability Data with Actionable User Intelligence

Table of Contents

A New Threat Paradigm

There was a time not long ago when IT professionals believed that patching was the path to redemption: "If we can only identify all our vulnerable systems and apply the proper patches to them, then attackers won't be able to get a foothold," the reasoning went. Frustrated by the absence of an easy way in, malicious hackers would move on to a different target and pick lower-hanging fruit.

That was a nice theory. Unfortunately, history has proven the theory wrong. Just in recent months, sophisticated and coordinated hacking campaigns against prominent financial services institutions, retail stores, high tech firms and government agencies demonstrated that the threat environment has fundamentally changed. Today, even reputable web sites can be "watering holes" armed with code to exploit previously unknown vulnerabilities on systems used by visitors to the site. Adversaries employing these techniques aren't likely to be dissuaded by organizations that merely do a "pretty good" job managing security.

Once they have a foothold within an organization, sophisticated attackers use their victim's access permissions to move laterally through the IT environment; stepping carefully from low value end-user systems to critical file shares, databases and application servers storing sensitive data and intellectual property.

"The fact is that both advanced and unsophisticated attacks can start with the exploitation of a software vulnerability," said Marc Maiffret, BeyondTrust's chief technology officer. "But by the time attackers start going after servers and data, they're not hacking anymore. They're leveraging their access to move through the environment as an ordinary user would."

Vulnerabilities Outside, Privileges Inside

If the "how" and "why" of sophisticated attacks are well known, why is it that so many technologically sophisticated firms fall victim to these attacks? One explanation is that many organizations still have a hard time assessing their real risks and allocating resources to them. This is in spite of gigantic IT security investments in the last decade.

Even today, security professionals often have blinkered views of their IT environments. Vulnerability management tools show which IT assets contain high risk (that is: "exploitable") vulnerabilities and allow security staff to rank or weight those assets according to their importance to the organization. However, IT staff often lacks a corresponding view of user activity on the network. That means even the most tenacious vulnerability management program will fail to stop sophisticated attacks that move quickly from exploits on low value systems to higher-value assets, leveraging legitimate user access in the process.

On the operations side of the IT department, administrators are swimming in logs of application events and user behavior, but cannot see the "forest" of malicious activity for the "trees:" a flood of innocuous-seeming commands, access requests and account creations.

Lacking a comprehensive view of their network security posture, they are blind to the risk posed by external or internal attackers who will use excessive permission grants to take control of network assets and steal sensitive data.

"Knowing that your systems are exploitable is one thing. But if you don't know what an attack looks like as it migrates from external to internal assets, then you're blind," said BeyondTrust's CTO Maiffret.

BeyondTrust: Fusing Asset and User Intelligence

BeyondTrust is an industry leader in vulnerability management and privileged account management. We have close to two decades of experience helping sophisticated organizations protect themselves from cyber attacks.

We recognized that the ability of sophisticated attackers to leverage low-value endpoints to traverse organizations demanded a new formula to assess cyber risk in the context of sophisticated and deliberate adversaries. What was needed was a security solution that bridges operational silos and correlates intelligence from both the IT operations and security disciplines.

Delivering on our pledge to provide IT professionals with context-aware security intelligence, we integrated our Retina Vulnerability Management and Powerbroker Privileged Account Management solutions. The result is a fusion of asset and user information on one platform that enables IT operations and security staff to understand and reduce their exposure to attacks and other adverse events.

BeyondInsight: A Collaborative Approach to IT Risk Management

The BeyondInsight™ IT Risk Management Platform is an integrated suite of software solutions used by IT professionals and security experts to collaboratively:

- Reduce user-based risk and mitigate threats to information assets
- Address security exposures across large, diverse IT environments
- Comply with internal, industry and government mandates

The platform integrates two foundational security methodologies:

1. **Privileged Account Management** enforces and audits access control policies by enabling IT to limit access to key systems, applications and data.
2. **Vulnerability Management** enables Security to assess risk, measure breach likelihood, and make remediation recommendations.

With BeyondInsight, IT and Security teams have one lens through which to view user and asset risk. This clear, consolidated risk profile puts events in context and enables joint decision-making within your IT organization. That ensures daily operations are guided by common goals for reducing risk.

BeyondInsight customers also gain a reporting and analytics platform that provides IT and business leaders with a view of the real risks facing their organization and the efficacy of risk reduction efforts enterprise-wide.

Asset Discovery

Security and IT professionals use the BeyondInsight IT Risk Management Platform to keep track of assets, assess and mitigate risk, ensure compliance, and communicate progress throughout the organization.

The platform's comprehensive asset discovery and profiling features locate IT assets that have been deployed locally and in remote locations. Web, mobile, cloud and virtual environments are all visible to BeyondInsight.

The product gathers rich detail on each IT asset it discovers including IP address, DNS address, operating system, MAC address and hardware profile information. Any visible ports and services, as well as any event logs are also gathered. All results and data are stored in a central data warehouse and leveraged to inform future assessment and vulnerability management activities.

Asset Smart Groups

Once IT assets have been identified, they can be organized for easy tracking. BeyondInsight's Asset Smart Groups allow administrators to logically group IT assets based on characteristics like IP range, operating system, domain, application type, business function or naming convention, Active Directory configuration and more. Smart Groups provide a manageable way to assess and report on groups of related IT assets.

Privileged Account Management

By employing BeyondTrust's PowerBroker solutions with the BeyondInsight platform, IT administrators can institute least-privilege policies proven to reduce the risk of damaging hacks infiltrating organizations. IT staff can use PowerBroker to discern which user accounts, applications, processes and IT policies are active, which are pertinent, and which have become obsolete.

PowerBroker solutions that currently operate within the BeyondInsight platform environment include:

- **PowerBroker for UNIX/Linux** provides granular privilege management for UNIX, Linux and OS X servers, allowing users to authorize system access and delegate root tasks without disclosing elevate accounts passwords.
- **PowerBroker for Windows** can be used to safely elevate Windows Administrator permissions for desktops and servers on an application-by-application basis. This is a far more secure path than granting frustrated users excessive administrative permissions for the entire environment.
- **PowerBroker PasswordSafe** stores, manages and rotates administrative account passwords for critical systems. The solution also monitors and audits shared password usage for increased accountability.

Vulnerability Management

BeyondInsight provides security teams with powerful vulnerability assessment and risk analysis across their entire IT environment. BeyondInsight's Retina CS Enterprise Vulnerability Management capabilities enable security professionals to identify software vulnerabilities that expose IT assets to attack. They can also analyze the business impact of those vulnerabilities, then plan and execute a program to remediate those vulnerabilities across their entire network, including traditional IT assets, web-based applications, mobile devices, and cloud and virtual infrastructures.

Retina Enterprise Vulnerability Management features powerful reporting and analytics, enabling security professionals to make smart decisions, effectively communicate risk, and report progress to executives and compliance auditors.

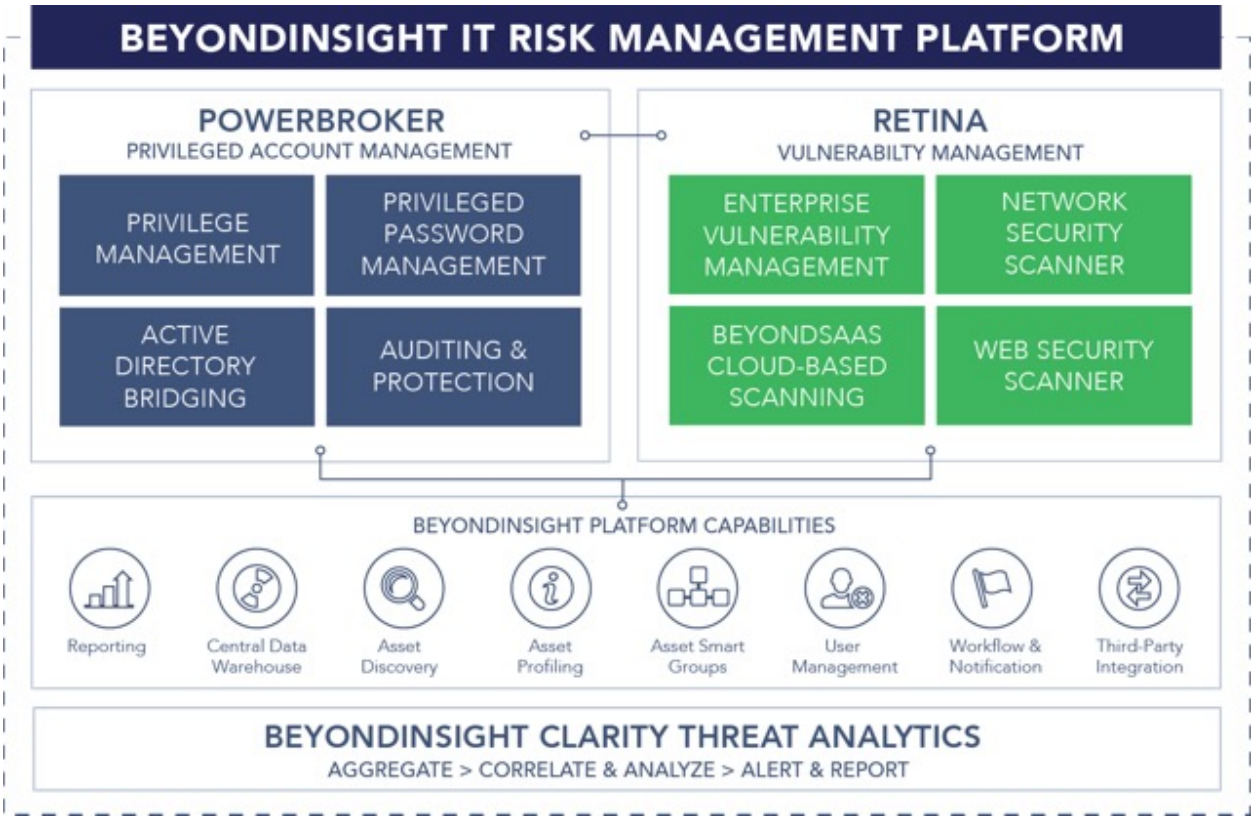
Bringing It All Together with BeyondInsight

The BeyondInsight IT Risk Management Platform delivers a comprehensive view of the vulnerabilities that provide doors into an environment, as well as the individual user privileges that are corridors to sensitive assets. By centralizing and correlating privilege, access and vulnerability data, the BeyondInsight platform provides IT and security staff with a clearer, more-informed picture of enterprise risk.

With BeyondInsight, users can answer questions such as:

- Which applications are running within the environment and how often?
- Which users and applications are operating with administrative permissions? How? And on which assets?
- Which IT assets contain exploitable vulnerabilities? Is there a correlation between a vulnerable asset and suspicious user or application activities?

IT security teams benefit from being able to correlate vulnerability information with user activity, while the whole IT organization gains a clearer view of how privilege policies impact overall security.



The BeyondInsight IT Risk Management Platform

Here are some ready applications for BeyondInsight:

Fine-Grained User and Application Control

Your organization likely has thousands of employees and scores of internal applications that must be managed daily. Understanding the connection between IT assets and the permissions granted to both users and applications is a critical element in stopping advanced attacks, either by insiders or those that gain access to insider's credentials.

When critical vulnerabilities in common platforms like Microsoft Office or Adobe Reader are identified, organizations are often left with difficult choices about whether to take a hard stand on security, thereby reducing worker productivity, or to look the other way at vulnerable and potentially exploitable IT assets.

The BeyondInsight IT Risk Management Platform augments static management- and application-control solutions by providing flexible, granular options for managing user and application privileges. For instance, rules can be created to address the age and risk of application vulnerability and perform an appropriate action. Here's an example risk compliance rule that users can create with BeyondInsight configured with PowerBroker for Windows:

1. *Allow administrator privileges* if the system contains any vulnerability that maps to PCI or HIPAA and is less than 30 days old.

2. *Allow standard user privileges and display a warning* if the system contains any critical vulnerability less than 90 days old, regardless of regulation.

3. *Deny operations and alert operations and security staff* if the system contains any critical vulnerability that is older than 90 days.

Using BeyondInsight, administrators can pursue a far more nuanced response: matching application privileges and runtime operations to larger business rules and objectives such as regulatory compliance requirements or industry-standard risk concepts.

Risk-Oriented Reporting and Decision-Making

The ability to view asset vulnerabilities in the context of user activity together is enhanced by more than 260 reports that allow operations and security staff to communicate vital risk and compliance data to both technical- and non-technical audiences within your organization. For example, BeyondInsight reports can prioritize vulnerabilities based on factors like asset scores, risk index ranking and more. Similarly, IT staff can spot user-specific risks by mapping that vulnerability data to user privilege and access management data.

Insight's powerful reporting engine keeps IT security and IT operations teams aligned and focused on business goals – whether that means complying with industry regulations like PCI

and HIPAA or simply reducing your risk profile by employing least privilege where it makes the most sense.

Conclusion: Delivering the Right Information, in the Proper Context, to the People Responsible for Mitigating Risk

Security experts agree: the question isn't "whether" your company will be attacked, but "when." This undeniable reality necessitates substantial changes in the way that IT organizations work and communicate.

Historical boundaries between distinct but overlapping groups like IT operations and IT security must be lowered. At the same time, better tools are needed to help these professionals share information and respond to threats and attacks. Finally, the marketplace demands that IT align its activities with an organization's overall business goals.

BeyondTrust is uniquely situated to provide your organization with the tools and technology it needs to secure your organization from advanced threats. Our BeyondInsight IT Risk Management Platform integrates two industry-leading risk management technologies:

1. PowerBroker privilege management solutions enable IT staff to configure "least privilege" policies that subordinate user and application permissions to operational and business priorities such as job function, regulatory frameworks, business objectives and risk management priorities. BeyondInsight maps PowerBroker data to Retina CS vulnerability data, enabling IT to see how privileges and vulnerabilities may combine to present paths of exposure to attackers.
2. Retina CS Enterprise Vulnerability Management enables security staff to identify, prioritize and remediate the remotely exploited vulnerabilities that give malicious hackers a foothold on your network. BeyondInsight maps Retina CS data to PowerBroker privilege management data, revealing risks triggered by users as they interact with systems and applications.

With BeyondInsight, users not only manage privileges and reveal vulnerabilities, but also gain insights into how privileges and vulnerabilities interrelate and impact your organization's overall security posture in the context of its business priorities.

About BeyondTrust

BeyondTrust® is a global security 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 Account 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.