WHITE PAPER

beyondtrust®

Beyond Traditional Security

AppLocker and Least Privilege

Table of Contents

Abstract

This white paper examines the pros and cons of AppLocker, and illustrates how using AppLocker alone as a solution for Least Privilege is not enough to protect your enterprise. However, integrating AppLocker with BeyondTrust PowerBroker® Desktops enables users to run with standard user rights, while simultaneously providing them the access they need to perform their job. This equates to a perfect complement of solutions to achieve least privilege.

Executive Summary

The introduction of AppLocker in Windows 7 allows organizations to use built in technology to implement application control policies across the enterprise. By controlling what applications can and cannot run on an endpoint, organizations can significantly improve security by preventing unknown code, including malware, from running on client computers.

Not only can this improve security, but it can also improve license compliance and prevent malicious insiders from doing harm. AppLocker is not a panacea however, and it is vital to continue to implement fundamental security best practices. Desktop hardening, Group Policies, virtualization, anti-virus and User Account Control alone are not enough to secure Windows 7 desktops. In order to have real control over the endpoints, users must be provisioned as Standard Users, not Administrators.

When a user runs as an Administrator, that user has full control over the computer, regardless of the security technologies installed on the endpoint. Users with full administrator privileges can easily circumvent all security controls that are intended to protect the business from security breaches. This whitepaper will discuss how important it is to remove administrator privileges from end users as a critical first step in a successful AppLocker implementation.

Introduction

AppLocker's complete functionality is only available in Enterprise and Ultimate SKUs of Windows 7. Designed as a replacement for Software Restriction Policy (SRP), AppLocker is designed to overcome the shortcomings of SRP. AppLocker is a set of Group Policy settings that evolved from Software Restriction Policies to restrict which applications can run on a corporate network. The methodology of controlling application execution with AppLocker is performed by creating either a "blacklist" or "whitelist" of applications.

Small and medium enterprises rarely deploy SRP, especially in Windows XP, mainly due to problems with launching applications from shortcuts, and because path rules are too easy to circumvent. In many cases, SRP certificate rules offer limited configuration options and hash rules are problematic when applications are upgraded. Applications that are on an AppLocker blacklist are blocked from executing, whereas applications on an AppLocker whitelist are allowed to run. Typically, organizations choose to implement either a white list approach or a black list approach, with the goal of attaining least privilege.

While AppLocker is a huge improvement over SRPs, it still falls short in a number of areas to ensure that organizations are meeting least privilege. As an employee's access requirements become more complex, AppLocker creates a difficult challenge for IT departments to continually update policies.

AppLocker Positives	**AppLocker Negatives**
Usability over SRPs	No reporting capabilities
User-friendly interface	Only available in Windows 7 Ultimate & Enterprise editions
Executable, Installation Package and Script support	Cannot handle advanced policies for privileged users
Central management using AD	Only supports computer-based policies

This white paper will illustrate how using AppLocker alone as a solution for Least Privilege is not be enough to protect your enterprise. However, integrating AppLocker with BeyondTrust PowerBroker® Desktops enables users to run with standard user rights, while simultaneously providing them the access they need to perform their job. This equates to a perfect complement of solutions to achieve least privilege.

Whitelisting vs. Blacklisting

BLACKLISTING

The best way to understand a blacklisting approach is to imagine a bouncer at a local watering hole or club. Imagine a patron at the bar is doing many antics that are classified as bad behavior. Anything from harassing women on the dance floor to spilling drinks on a continual basis. The face of the matter is, once certain actions have been flagged as inappropriate behavior, it is the bouncer's responsibility to flag that person, kick them out and add them to a blacklist, which prevents that patron from ever entering that bar again.

Unfortunately, this does not solve the problem completely. Even though certain individuals have been flagged and removed from the list, anyone who is not on the blacklist can enter the bar, including people who may have never been to this establishment before, but who may make trouble on any given night.

This analogy explains the challenges with blacklisting for IT administrators who manage Applocker. Implementing a blacklist approach for IT is problematic because even if certain software programs are flagged as a threat, Admins cannot possibly keep track of and ban all bad software. Blacklisting applications alone is simply an impractical approach to application control and security. In order for it to be even remotely close to effective, an organization would have to continually manage the blacklist. This list would grow exponentially over time creating obvious headaches and weaknesses in security and compliance.

There is one major caveat to this. You must remove administrator privileges from users in order to guarantee that blacklisted software does not run on the computer. You can think of a user with administrator privileges on a computer as a patron with the key to the backdoor of the club. Even though the bouncer will not let that individual in the front door, he can just let himself in the back door.

Blacklisting applications alone is simply an impractical approach to application control and security. In order for it to be even close to effective, you would have to manage the blacklist constantly and it would grow exponentially over time. This is why many organizations are opting to abandon blacklisting altogether and focus on a whitelisting strategy instead. For these reasons, we will focus this paper on whitelisting with AppLocker.

WHITELISTING

When trying to understand the whitelisting approach, we can use the same analogy of a bouncer at a local watering hole or club. With a white list, imagine those special VIP lists at an exclusive bar or nightclub. Under the whitelisting approach, if you are not on the list, the bouncer will not let you into the organization. End of story.

One could reasonably assume that if a whitelisting approach were implemented, the collective behavior (security) of the people who are let inside would improve dramatically. The same holds true for computers.

Whitelisting technology has enjoyed a resurgence of interest lately, with antivirus companies such as Symantec, McAfee, and Microsoft planning to add it to their blacklisting-based malware detection tools and some enterprises even dropping blacklisting altogether in favor of whitelisting alone. All thanks to the proliferation of botnets, stealthier malware, and the near epidemic in data breaches have led enterprises to search for something other than the standard approach of blacklisting known threats.

1. See the BeyondTrust whitepaper "Least Privilege Application Compatibility for Windows 7 Migrations" for details why Windows does not have a solution to the least privilege problem.

However, it is vital to understand that whitelisting is not the cure-all for least privilege. The only way whitelisting could truly stand alone is if an enterprise were to return to the old-fashioned whitelisting lockdown mode, where users can only run specific, approved apps and nothing else -- no browser add-ins, gadgets, etc., This obviously unrealistic for most organizations because most companies today have to let their users install some things.

This is why integrating PowerBroker for Windows with Applocker represents the true solution to these challenges. As shown later in this paper, PowerBroker for Windows free up IT resources by transparently giving end-users the power to run all required Windows applications, processes and ActiveX controls safely, securely and in compliance. Simply put, removing administrator privileges from users has never been faster or easier using whitelisting and PowerBroker together.

Configuring AppLocker Policy

AppLocker is configured inside Group Policy Objects. By creating the default AppLocker rules, an organization can create a whitelist that will allow everything located in the Program Files directory and the Windows directory to run, as shown in Figure 1.

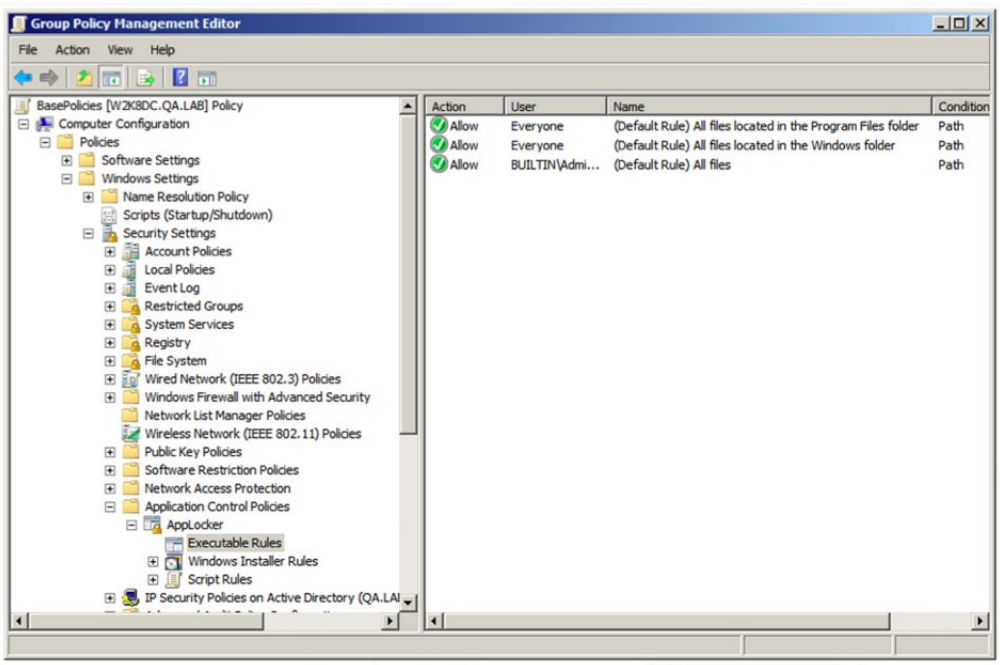


Figure 1. Group Policy Management Editor

This means that every executable that runs from ***c:\Program Files*** and ***c:\Windows*** will run successfully. If an application is launched from anywhere else, the application will be blocked by default and the user will receive a message stating that the application is blocked, as shown in Figure 2.

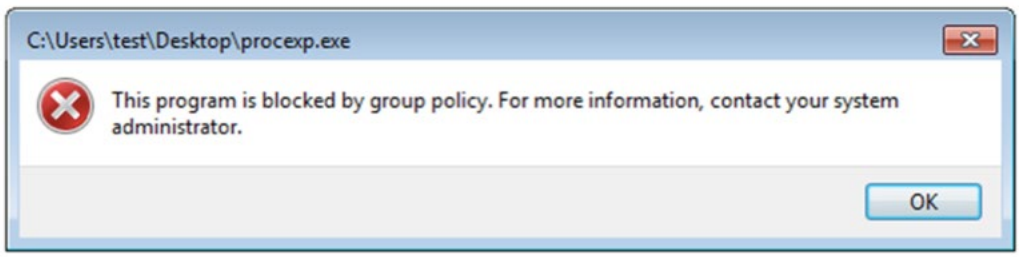


Figure 2. Message Box

Note that there is a third default rule that is created which allows any user who is a member of the local administrators group to run any application. This is because AppLocker assumes that users who are administrators should be allowed to run any application. Clearly, Microsoft intends the AppLocker policies for application control to apply to Standard Users, not administrators.

The major reason that Microsoft has implemented the default rules in this way is because they know that there are simply too many ways that a user who is an administrator can circumvent the AppLocker policies. Here are some examples of how a user could run an application that is not currently on the whitelist:

- Boot in Safe Mode and install an application to Program Files. Since the default rule to allow all executables to run from Program Files is in place, the new application will now execute
- Disable the Application Identity Service. Since the default rule to allow all executables to run from the Windows folder is in place, an administrator can disable the service that enforces AppLocker policies
- Create AppLocker Policies in Local Security Policy. AppLocker policies that are configured at the domain level are merged with policies that are defined locally. Since local administrators have the ability to edit Local Security Policy, based on the default AppLocker rules, they can add applications to the white list
- Right-click a blocked executable and select "Run As Administrator"

There are many other ways that a local administrator can circumvent AppLocker policies, which is again, why Microsoft intended for AppLocker policies to apply to Standard Users, not Local Administrators.

You can implement customized policies to plug some of the security gaps that exist when users are Local Administrators, but this will create significant operational overhead and downstream problems for users. The consensus among security experts is that it is not enough to implement whitelisting alone; you should also remove administrator privileges from end users.

Unfortunately, removing administrator privileges is not trivial, and there are consequences that will affect end users. Typically, the issues break down into three main categories:

- Applications that require administrator privileges to run
- Software and ActiveX installations that require administrator privileges to install
- System Tasks that require administrator privileges

Many organizations that have attempted to remove administrator privileges in the past have experienced these consequences first hand and have had to stick with the status quo and keep users configured with administrator privileges.

This is dangerous from a security perspective and costly from an operations perspective. Not only can an administrator circumvent any security measure you have configured or installed on the computer, his/her machine is much more likely to be infected with malware or be targets of advanced persistent threats, leading to having their computers mis-configured accidentally or maliciously.

Unfortunately, Microsoft does not have a solution to the problems associated with removal of administrator privileges.[1] In order to allow a user to run applications, software installations or system tasks that require administrator privileges, organizations need a solution to elevate applications on a per-process basis.

Best Practice Flow Chart for Least Privilege

If an application is allowed to run because it is on the AppLocker white list, but the application also requires administrator privileges to run, it will not run successfully, and the user will be prompted by User Account Control (UAC) for administrator credentials (See: Figure 3).

The only way to get an application to run properly is to either give the user administrator credentials (effectively making that user an administrator), or elevating the application by using a product like PowerBroker for Windows.

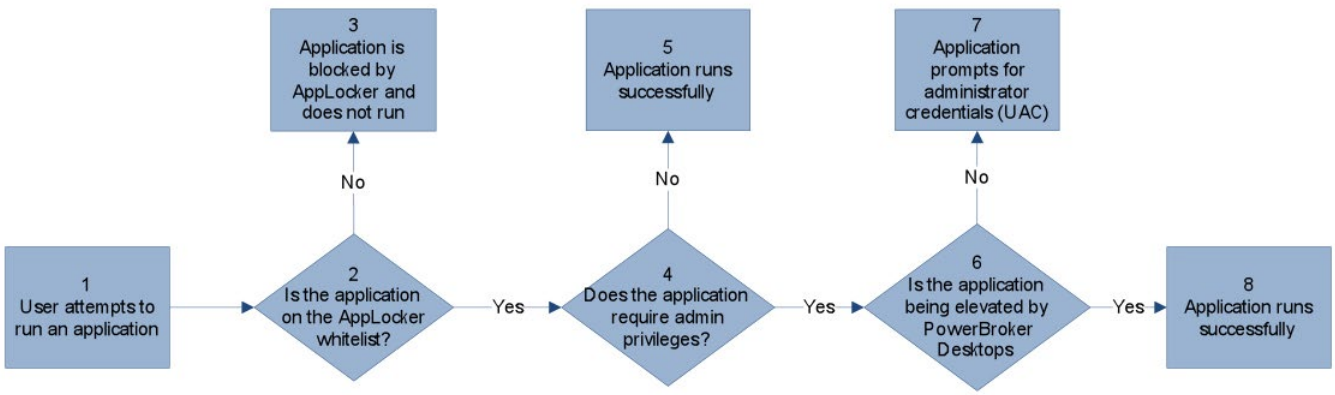


Figure 3. Flow chart of application execution for whitelisted application via AppLocker, in addition, elevation of applications that require administrator privileges using PowerBroker for Windows.

The best of breed, most cost effective and most integrated solution to this problem is to configure AppLocker policies on desktops alongside PowerBroker for Windows policies for elevating applications that require administrator privileges.

PowerBroker for Windows can elevate applications, giving the application any set of privileges or permissions it requires, without giving the end user excessive rights. PowerBroker for Windows policies (Figure 4) are configured in a nearly identical fashion as AppLocker Policies (Figure 5), all within the same Group Policy Object.

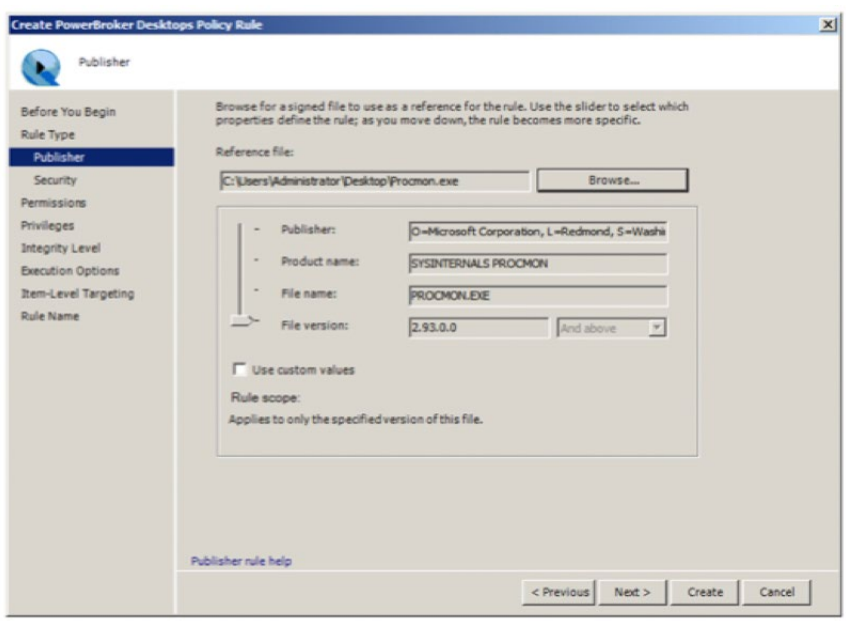
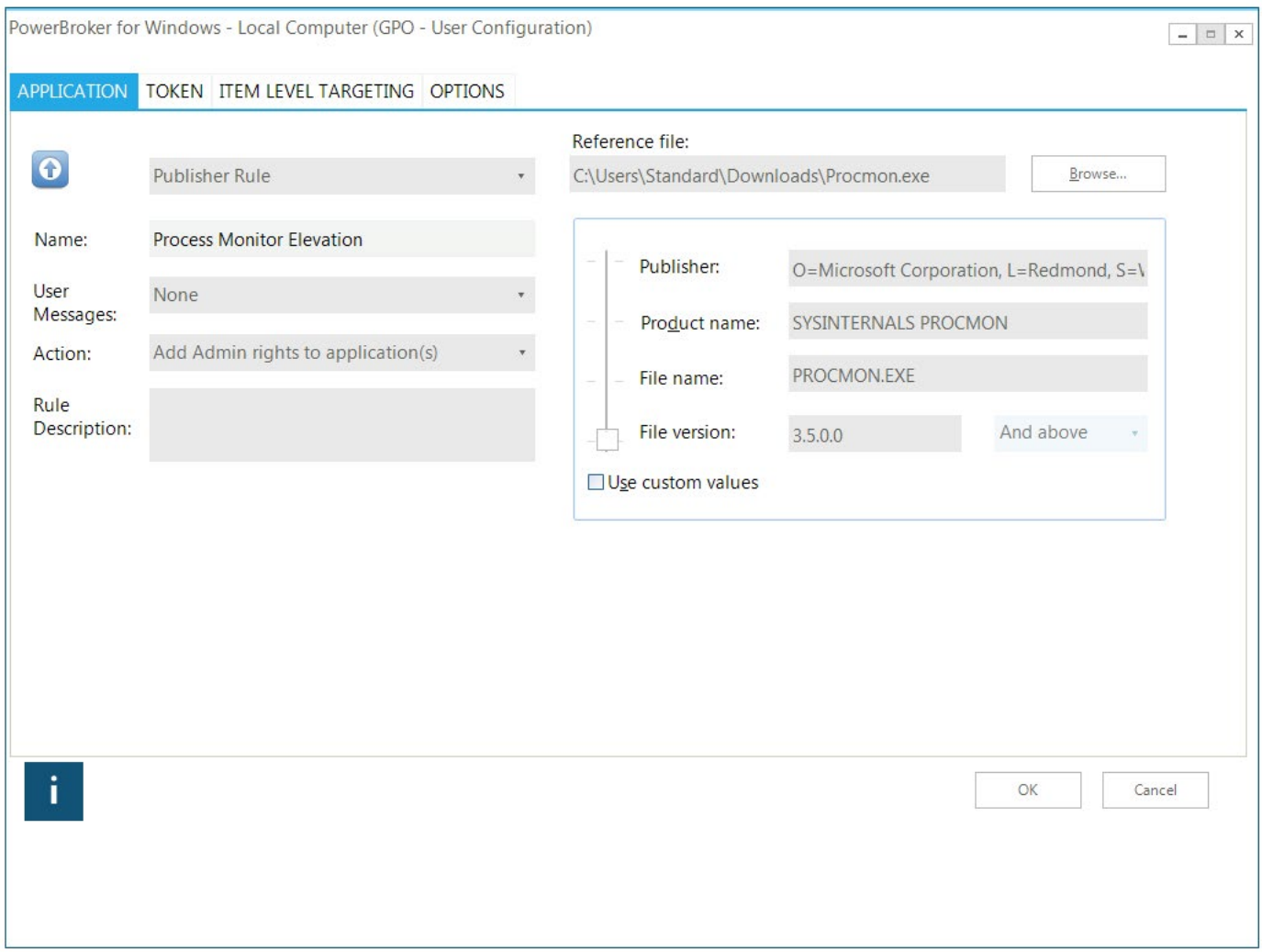


Figure 4. PowerBroker for Windows rule configuration for Process Monitor (procmon.exe)

Since the Process Monitor requires administrator privileges to run successfully, a PowerBroker for Windows rule is required to elevate this application for a standard user. Simply adding it to the AppLocker whitelist alone is not enough to get the application to run successfully.



AppLocker and PowerBroker for Windows also have built-in automatic rule creation capabilities. In AppLocker, you can create a set of rules for your Window 7 image quickly and easily by automatically detecting all executables on a system outside of the Windows folder and Program Files folder and creating the appropriate rules for them.

For PowerBroker for Windows, you can discover which applications require administrator privileges across the enterprise in one easy step and automatically create rules for elevating those applications. By leveraging the automatic rule generation capability in both products, you can achieve significant improvements in security with very little effort.

The biggest downside to AppLocker is the fact that it is not compatible with Windows XP or Windows Vista. If you have not made the move to Windows 7 yet or if you are still trying to decide if whitelisting is a viable option for your enterprise, there are several things worth considering.

For many organizations, whitelisting is simply impractical, maybe impossible. For users who have rapidly changing needs, it is very difficult to keep up with the management of AppLocker policies. IT staffing levels and needs of the end users will likely weigh into your decision to implement AppLocker or not. For some organizations, the decision may

become one of either deploying whitelisting OR removing administrator privileges.

This is a false choice. As discussed in this paper, in order to make whitelisting secure, you MUST remove administrator privileges. Organizations that choose to remove administrator privileges from users as a first step in improving their security posture on the desktop will reap rewards in the long run. Further, removing administrator privileges can deliver a much bigger bang for your security buck than implementing whitelisting alone.

Summary

In conclusion, the Pareto principle, which is better known as the 80-20 rule, will be used to make an argument as to why you should consider removing administrator privileges before you even consider implementing whitelisting. To remove administrator privileges, it will take very little effort (20) to get an enormous improvement in security (80).

This is because you only need to manage the applications that will no longer function without administrator privileges. You get an enormous security benefit because you are configuring the user the way that Windows wants the user to be configured --the user no longer has full control over the operating system, and neither does malware. If you allow your users to run as administrators and only implement whitelisting, it takes significant effort (80) for a small improvement in security (20).

This is due to the fact that you need to manage a much bigger set of applications, and you also need to attempt to mitigate all of the security vulnerabilities associated with to whitelisting that as I mentioned earlier in this paper. Whitelisting alone really does not provide any real security whatsoever;, adding whitelisting to best security practices, including the removal of administrator privileges, is the only way to make your desktops as secure as possible.

About PowerBroker® for Windows

PowerBroker® for Windows includes powerful new usability enhancements and features to allow organizations to configure user rights on a task-by-task basis without granting administrator access.

This solution can minimize help desk calls and free up IT resources by giving end-users the power to run all required Windows applications, processes and ActiveX controls safely, securely and in compliance. Simply put, removing administrator privileges from users has never been faster or easier.

About BeyondTrust

With more than 25 years of global success, BeyondTrust is the pioneer of Privileged Identity Management (PIM) and vulnerability management solutions for dynamic IT environments. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust to secure their enterprises. Customers include eight of the world's 10 largest banks, seven of the world's 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies, as well as renowned universities. The company is privately held, and headquartered in San Diego, California. For more information, visit **beyondtrust.com**.

CONTACT INFO

NORTH AMERICAN SALES
1.800.234.9072
sales@beyondtrust.com

EMEA SALES
Tel: + 44 (0) 8704 586224
emeainfo@beyondtrust.com

CORPORATE HEADQUARTERS
550 West C Street, Suite 1650
San Diego, CA 92101
1.800.234.9072

CONNECT WITH US
Twitter: @beyondtrust
Facebook.com/beyondtrust
Linkedin.com/company/beyondtrust
www.beyondtrust.com

