BeyondTrust Defendpoint Version 5.3

New and Updated Features

BeyondTrust Defendpoint reduces the risk of privilege misuse by assigning admin privileges to only authorized tasks that require them, controlling application and script usage, and logging, monitoring, and reporting on privileged activities. By providing fine-grained control over privileged access, IT protects users while improving the efficiency of least privilege management.

Defendpoint version 5.3 introduces market-leading capabilities for integrating with third-party solutions to simplify workflows. Please see the release notes for additional details on these important enhancements.

New Feature Highlights

New Power Rules Automate Workflows and Speed Application Exception Handling

While whitelisting and blacklisting rules are generally straightforward to develop and enforce, applications where there is only limited information available – for example, just a hash, publisher, whether it has been signed, etc. – can introduce risk into an environment if not properly vetted prior to allowing the application's use. The process to investigate whether an application is malicious or vulnerable could result in delays to the user due to additional processes and teams' involvement, negatively impacting productivity.

Defendpoint version 5.3 introduces Power Rules to help speed decisions on whether to allow an application to run, or allow it to run with admin rights, by automating the integration of third party intelligence sources. Power Rules is a business rules engine that enables customers to more easily configure Defendpoint to their unique business requirements and integrate Defendpoint into other systems.

Based on PowerShell, organizations can simply write a script and embed it in the policy itself. For example, when it runs, the PowerShell script can automatically trigger a service desk workflow, raising a ticket with your helpdesk that provides all the information they require about the application or task. Or, it can call out to a third party to check the hash, or to a vulnerability management system to check for CVEs on the application, thereby adding custom logic to building Defendpoint rules.

.

Introducing Power Rules for ServiceNow

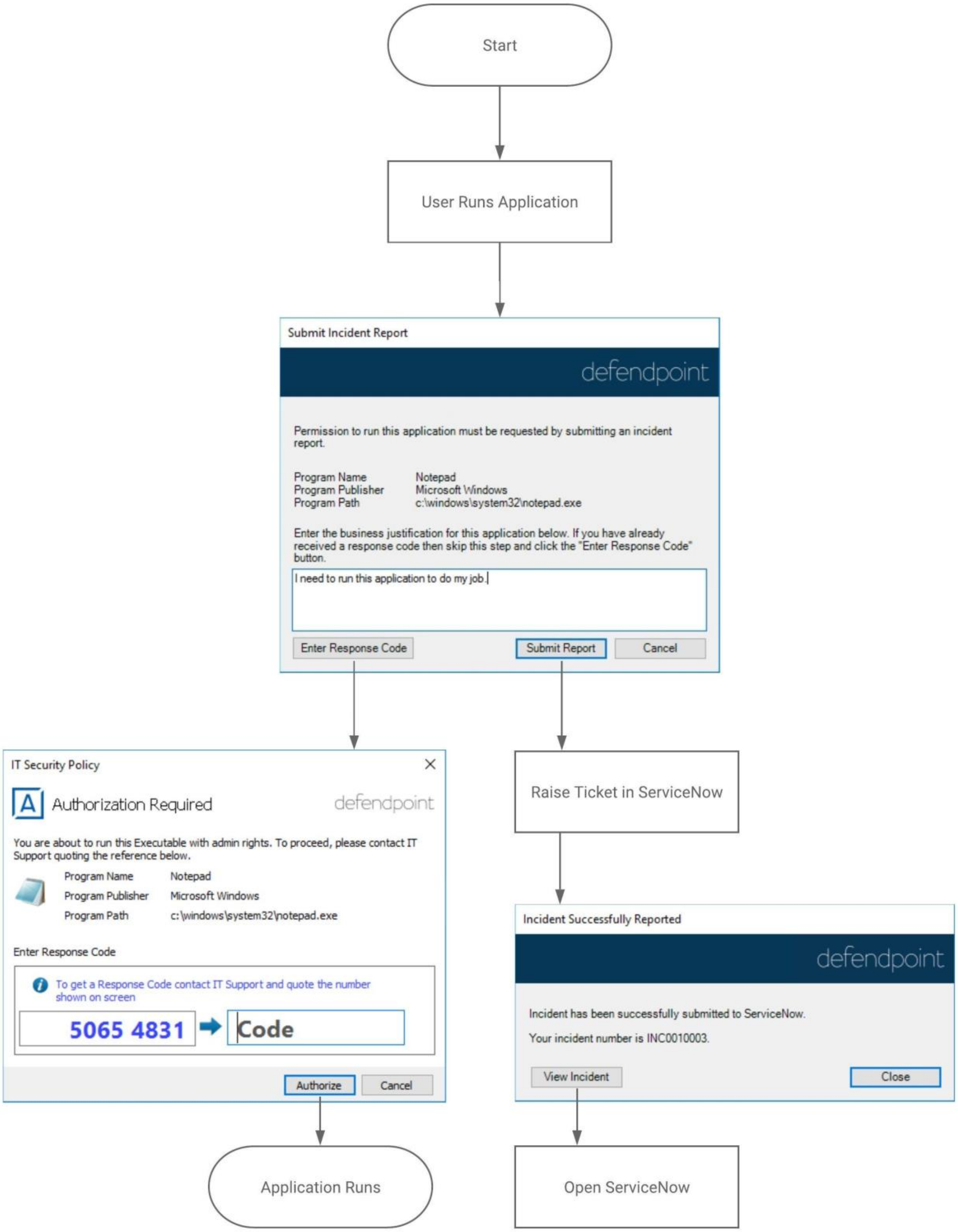
With version 5.3, Defendpoint now uses Power Rules to integrate with ServiceNow to automatically submit a ticket to the IT team, so that they can make an informed and expedited decision on the user's request to run an application, installation, script or task. This new capability improves automation and application exception handling.

In the default configuration, when a user runs an application that you are targeting with the ServiceNow Rule Script, the user is presented with the option to raise an incident in ServiceNow or cancel the request. The ServiceNow ticket includes caller, a short description, and a more detailed description that includes the business justification, the program name, program publisher, program path, challenge code, and the business justification the end-user provided.

Administrators can then action the incident in ServiceNow and supply the end-user with a response code. The end-user can then use the response code to 'unlock' the application, allowing it to run.

Using the ServiceNow integration is simple - just create a new Power Rule in any workstyle or set any existing rule to use a Power Rule and import the integration script. Any application that matches the rule will then trigger your ServiceNow workflow. And because the integration is scripted, it can easily be tailored based on your own ServiceNow workflows. For a representation of the workflow involved in invoking this Power Rule, please see the diagram below.

Be sure to see the ServiceNow Integration Guide and the release notes on version 5.3 on Avecto Connect for more information.



Submit Incident Report

Permission to run this application must be requested by submitting an incident report.

Program Name	Notepad
Program Publisher	Microsoft Windows
Program Path	c:\windows\system32\notepad.exe

Enter the business justification for this application below. If you have already received a response code then skip this step and click the "Enter Response Code" button.

I need to run this application to do my job.

IT Security Policy

You are about to run this Executable with admin rights. To proceed, please contact IT Support quoting the reference below.

Program Name	Notepad
Program Publisher	Microsoft Windows
Program Path	c:\windows\system32\notepad.exe

Enter Response Code

To get a Response Code contact IT Support and quote the number shown on screen

5065 4831 → Code

Incident Successfully Reported

Incident has been successfully submitted to ServiceNow.

Your incident number is INC0010003.

About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing data breaches related to stolen credentials, misused privileges, and compromised remote access.

Our extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. BeyondTrust unifies the industry's broadest set of privileged access capabilities with centralized management, reporting, and analytics, enabling leaders to take decisive and informed actions to defeat attackers. Our holistic platform stands out for its flexible design that simplifies integrations, enhances user productivity, and maximizes IT and security investments.

BeyondTrust gives organizations the visibility and control they need to reduce risk, achieve compliance objectives, and boost operational performance. We are trusted by 20,000 customers, including half of the Fortune 500, and a global partner network. Learn more at www.beyondtrust.com.