Bitdefender
BUILT FOR RESILIENCE

GravityZone Patch Management

Problem Statement

Unpatched software creates security holes that can be used to compromise entire companies by cybercriminals. An unpatched operating system provides attackers with an easy path to remotely run commands or gain privileges on a system. With such access, an attacker could then create accounts with administrator privileges, install software; and view, change, or delete data. Equally as risky, applications with security vulnerabilities can lead to exploits that can also compromise the security, integrity, and even the reputation of a company. As a result, security teams cannot afford to leave operating systems and software unpatched. The responsibility of security teams to keep systems up-to-date has become more demanding of time and resources.

Security teams are faced with several different challenges involved in keeping operating systems and software up-to-date:

- The increased frequency of operating system patches can be daunting to keep up with.
- Operating system updates can sometimes be problematic and cause crippling issues to production environments.
- It's difficult to keep track of installed software and available updates for those applications.
- With different time zones and uptime requirements, it's challenging to schedule patches during maintenance windows.
- Deploying patches to large environments can be slow and network bandwidth intensive.

Feature Overview

GravityZone Patch Management offers a complete Operating System and application patching solution for Windows and Linux environments.

Through scheduled patch scans, administrators can keep track of operating system updates, as well as software installed on the systems, and any available patches for those applications. GravityZone Patch Management allows setting up automatic, comprehensive maintenance windows to prevent workflow interruptions. It also enables the use of a patch caching server, thus significantly reducing patch install's bandwidth utilization, and increasing the speed at which the patches are distributed to the endpoints.

At-a-Glance

Patch Management keeps operating systems and software applications up to date and provides a comprehensive view on the patch status for your managed Windows and Linux systems.

Key Capabilities

- **Provides visibility into installed software –** using the patch scan feature, security teams can keep track of installed software and available patches.
- **Manage patches for the Windows & Linux Operating Systems –** organize critical and non-critical Windows updates for workstations and servers, also supports CentOS, SUSE, and Redhat Linux distributions
- **Schedule patches during maintenance windows –** configure maintenance windows that allow security teams to control when patches are installed so as to not interrupt productivity
- **Search for and deploy patches –** search for patches by several different identifiers **–push out patches you want, automatically ignore specific patches that can create conflicts or present other issues**

With Bitdefender's central administration, we've reduced time to deploy security software at client sites from two or three days to a couple of hours

Daniel Hayes, Centralized Services Team Leader, Morefield Communications

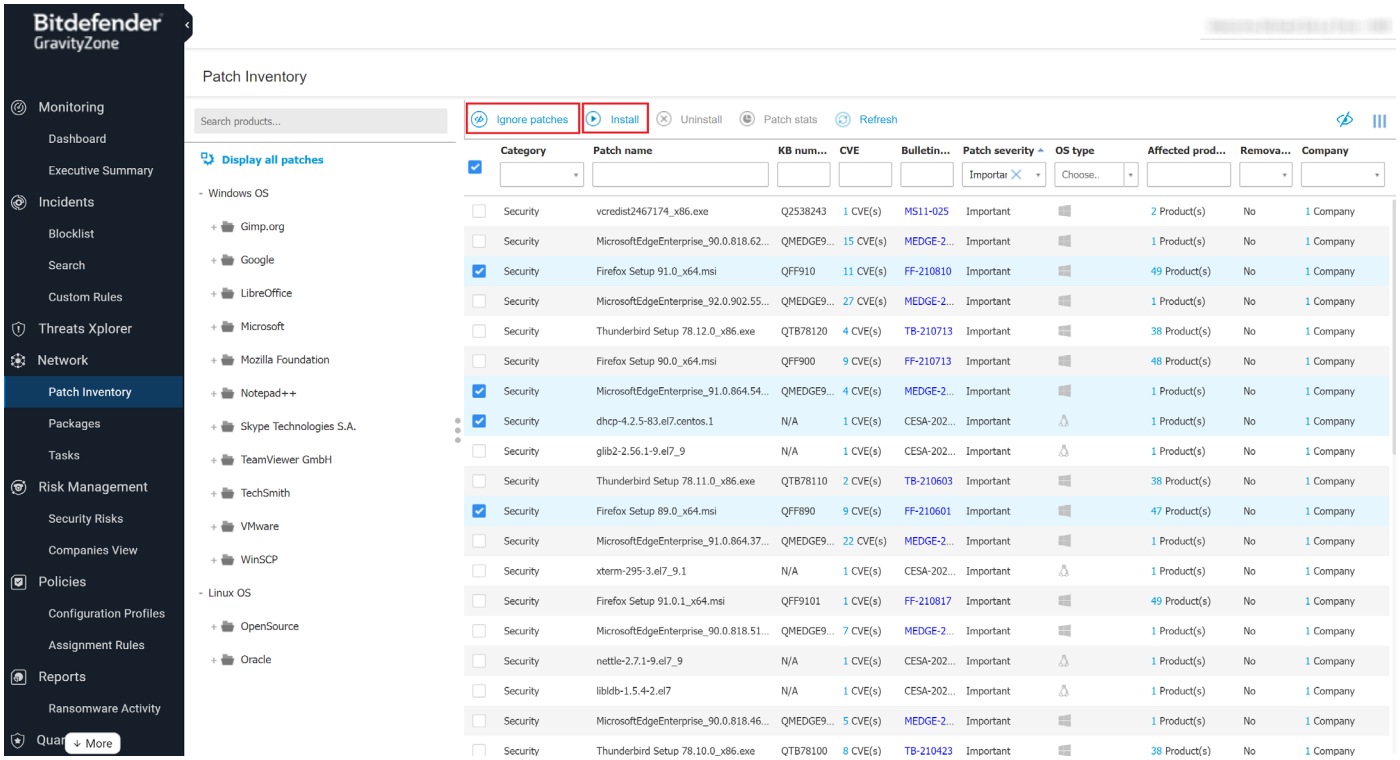

Figure 1.1 – GravityZone's Patch Management allows security teams to easily keep an inventory of available patches. It also allows fast patch installation and the option to ignore problematic patches.

Capabilities

Gravityzone Patch Management is an add-on component that can be easily installed to systems through the GravityZone console's simple package creation. Security teams can choose to also install the Patch Management Cache Server role to specific Windows or Linux systems. This role allows all relevant patches to be stored on the local network, which not only helps accelerate the deployment of patches, but also reduces the overall internet bandwidth needed for distributing patches and updates. If the patch caching server is unavailable, systems can be configured to fall back to downloading the patches from the manufacturer's website.

GravityZone Patch Scanning

Once the Patch Management feature has been deployed, security teams can manually trigger patch scans on endpoints that can both scan for operating system updates, as well as available software patches. These patch scans can also be configured via GravityZone's policies and configuration profiles. The available Smart Scan feature can automatically scan newly installed software for any available patches or updates. The completion of the patch scan will then populate the Patch Inventory.

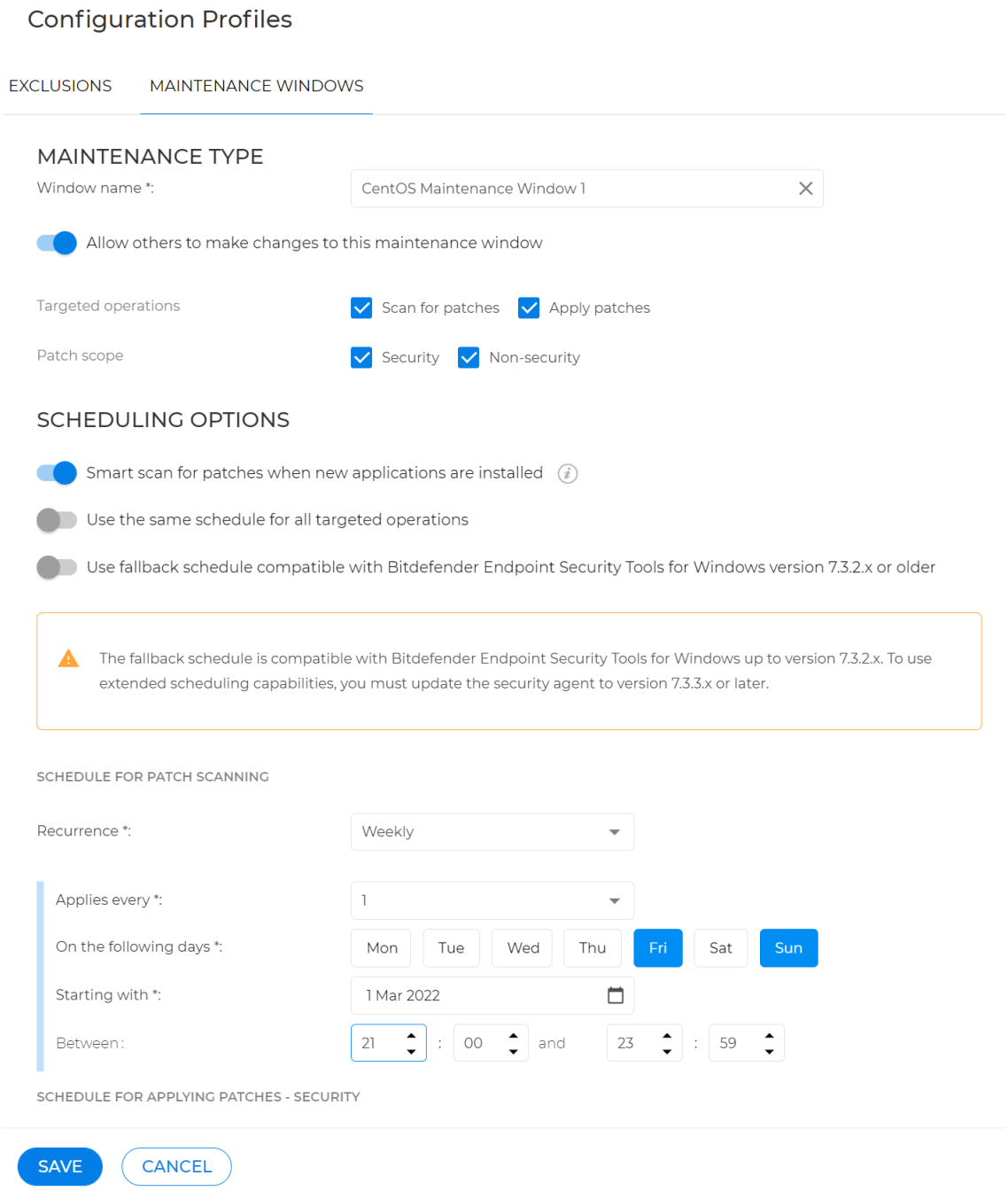

Figure 2.1 – Using GravityZone's Patch Management maintenance windows, security teams can schedule automatic patch scans and patch installs during convenient times so as to not impact productivity.

Comprehensive Patch Visibility

The Patch Inventory provides a complete view into any available Windows or Linux patch. Through the Patch Inventory, security teams can sort patches by Operating System type, software manufacturer, patch category (security and non-security), and patch severity— patch severity includes: none, low, moderate, important, critical, and unassigned. Managed Service Providers and customers using a multi-tenant GravityZone console can also view available patches by managed company.

Patches can easily be searched for by patch name, Knowledgebase (KB) number, Common Vulnerabilities and Exposures number (CVE), Bulletin ID, and affected product.

Deploy Patches You Want, Ignore Problematic Patches

The Patch Inventory allows security teams to choose the updates and patches they want to deploy— and on what systems they want to deploy those patches.

From time to time, patches and updates will be released for the operating system or software that can be problematic. These updates can create conflicts with other software and become crippling to businesses. Problematic updates have been known to cause systems to crash, keep systems in a boot loop, destroy data, and more. With GravityZone Patch Management, security teams can choose to ignore such precarious patches, and selectively deploy them to test environments until they are deemed safe for installation in production environments.

Automatic Patch Scans & Deployments During Maintenance Windows

GravityZone Patch Management includes the ability to configure Maintenance Windows through its Configuration Profiles. These maintenance windows can define a specific date and time range when patch scans can be automatically triggered, and patches installed. Different maintenance windows can be assigned to through GravityZone's accessible policies. Security teams can specify the software they want automatically updated, down to the distinct version number.

Powerful Integration & Reporting

From the GravityZone dashboard, security teams can see a view of the network patch status – this allows immediate visibility into successful and unsuccessful patch installations for security and non-security patches. With a simple click into the Network Patch Status chart, security teams can access a detailed report of the patches and updates that were installed, have failed, or are pending installation. With just a few more clicks, patches can be deployed to the affected systems right from the report. There's no need to fumble with different menus and interfaces to quickly deploy patches. The report can also be exported to a PDF or CSV file, or emailed to the configured GravityZone manager account.

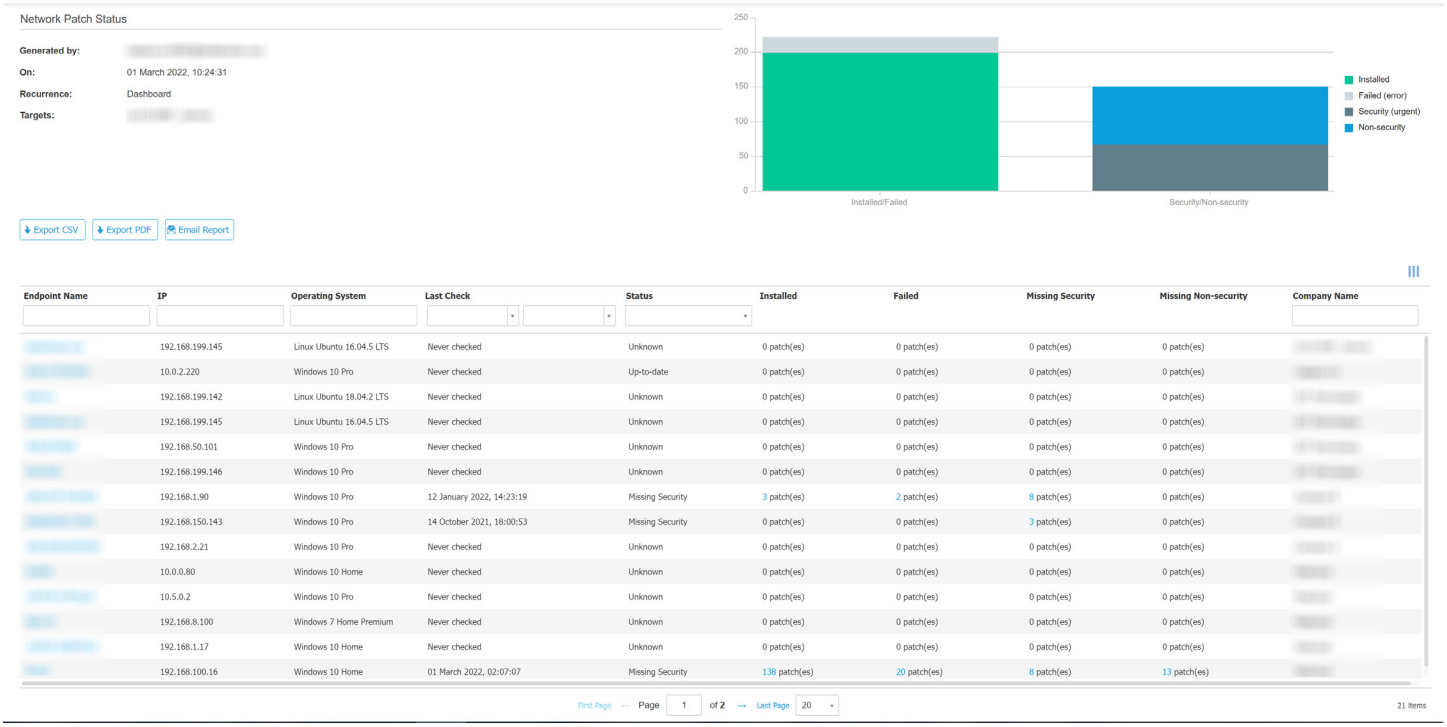

Figure 3.1 – GravityZone Patch Management reports give detailed view into network patch status with several search and sorting options. The report can be exported in a number of different formats or emailed to the GravityZone account manager.

Integration with GravityZone Endpoint Detection and Response (EDR), provides the ability to immediately patch vulnerable software on systems where a threat was detected. Furthermore, Patch Management integrates with GravityZone's Risk Management, allowing fast and immediate patching of potentially unsafe software. All of this functionality is delivered through the same management console.

GravityZone Patch Management takes the stress and complexity out of managing operating system updates and software patches. With the features outlined in this article, security teams can keep their systems up-to-date and help prevent cyberattacks from damaging their businesses

Bitdefender
BUILT FOR RESILIENCE

3945 Freedom Circle
Ste 500, Santa Clara
California, 95054, USA

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

For more information, visit https://www.bitdefender.com.

Bitdefender.BS.62.PatchManagement.TechnicalBrief.NoPrint.DEX.332.en_EN
CD-Mar/30/2022-MD-Apr/05/2022