TECHNICAL SOLUTION BRIEF

WEB USE ONLY

Bitdefender

Security

Ransomware Prevention and Mitigation with Bitdefender GravityZone

www.bitdefender.com

Contents

Ransomware Overview

What is Ransomware?

Ransomware is malicious software that seeks to encrypt files and hold them for ransom. Ransomware victims must pay the attackers to regain access to resources, typically in untraceable cryptocurrency, in return for a decryption key which may or may not arrive after payment is made. For an individual, files like pictures, videos or important documents can cause anxiety if compromised, but for a business entity the ransomed content could easily include proprietary information, customer personal information, account and payment card details, or other valuable data.

Ransomware is nearly always motivated by profit, however advanced ransomware attacks can have wider objectives and cause tremendous harm to organizations, including existential concerns should the ransomware attack cause the entity to be unable to continue in its normal course of business. In extreme cases, human lives can even be put at risk.

Examples of recent high-profile ransomware attacks with outsized monetary losses and negative social impact:

- Hospitals: British National Health Service (est. total costs of £92 million in direct costs and lost productivity)
- State/Local Government: State of Louisiana (state of emergency declared), 2 Florida cities ($1.1 million paid)
- Education: University of Utah ($457,000 paid), University of California San Francisco ($1.14 million paid)

Ransomware can manifest on an infected laptop, desktop or server in multiple ways, typically denying user access to the system until the ransom is paid:

- Encrypts sensitive and personal files with no possibility of decryption
- Threatens the public release of sensitive and personal files
- Locks the computer's screen denies complete access to the system
- Blocks certain applications from running, crippling user productivity

Ransomware is highly adaptable, carefully designed to avoid detection by security software. Even small delays in detection can provide enough time for potentially irreversible file encryption to take place.

How does Ransomware Penetrate the Organization?

Ransomware has many viable paths into the organization and cybercriminals are very creative in their exploitation of both technological and human vulnerabilities. Despite years of security awareness training, risky user behavior persists at stubbornly high rates, leading to risky clicks on dubious links and ill-considered application/file downloads.

- Targeted phishing email laden with malicious links and file attachments
- Malicious document downloads, either user-initiated or triggered via drive-by downloads
- Malicious application/executable file downloads, including bogus software and fake product updates
- Fileless attacks in memory space initiated from the browser, without ever touching the disk drive
- Infected documents and media files from network file shares and portable media drives

Figure 1: Common ransomware attack vectors

What does Ransomware Protection Entail?

Comprehensive ransomware mitigation requires proactive vigilance on multiple simultaneous fronts, each of which must be covered by the security solution.

- **Preemptive Protection** – Create tamperproof backup copies of user files that are inaccessible to ransomware
- **Blocking and Prevention** – Deploy adaptive defenses not reliant on signature-based detection techniques
- **Monitoring & Early Detection** – Watch suspicious processes and network activity, correlate attack indicators
- **EDR and Incident Response** – No prevention is 100% effective all the time, so EDR looks for suspicious indicators on the endpoint and in the network traffic to correlate into specific incidents for response
- **Vulnerability Patching** – Update vulnerable applications and operating systems with the newest vendor-supplied patched, applied automatically
- **Risky Configuration Management** – Identify and close all readily available sources of ingress for ransomware by identifying and correcting system misconfigurations, many of which can be remediated automatically
- **User Behavior Risk Monitoring** – …Identify and correct user behaviors that increase risk to the organization like password reuse, falling for phishing lures, risky clicks and downloads, and logins to unencrypted websites
- **Application and Device Control** – Monitor usage and allow only the required applications to run and only the necessary external devices to access the system.

Beating ransomware requires understanding the full cyber kill-chain and mapping defenses to each attack stage.

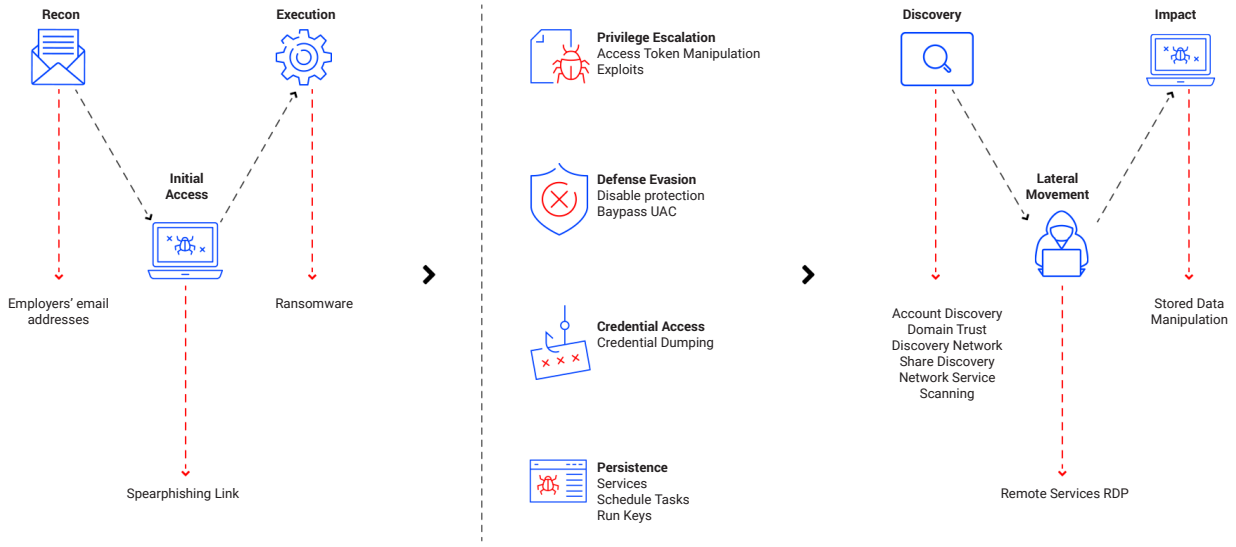

Figure 2: Ransomware attack tactics and the typical cyber kill-chain

Protected Ransomware Attack Vectors

Relief from ransomware all of its devastating effects also requires coverage of all common attack vectors:

- Phishing or spam email links and malicious file attachments
- Malicious file downloads, both user-initiated and caused by drive-by downloads
- Malicious application or executable file downloads
- Fileless attacks in memory space initiated from the browser without ever touching the disk
- Portable media drives and network or remote file shares

How Bitdefender Ransomware Mitigation Works

Tamperproof Backups

Bitdefender creates automatic, up-to-date tamperproof backup copies of user files, without using shadow copies that have been repeatedly proven to be easily deleted by ransomware. It's hands-free protection, with nothing for the user to do. Ransomware can't access the protected backup files and the user is unaware of their presence. Ransomware Mitigation identifies whenever a possible new ransomware attempts to encrypt files and automatically creates a backup of targeted files that will be restored after the malware is blocked. Bitdefender blocks all processes involved in the attack and starts remediation, while also notifying the user.

Blocking and Prevention

Fileless Attack Defense and Hyper Detect

When activated, Bitdefender automatically discovers and blocks fileless attacks at the pre-execution stage, preventing file encryption and preserving full system access. HyperDetect can detect and block fileless attacks at pre-execution using highly tuned machine learning models to spot new and unknown malware with high accuracy to successfully defeat fileless ransomware during multiple stages of the attack kill chain by analyzing the behavior at code level.

Machine Learning Anti-Malware

Bitdefender security automatically and continuously trains and improves its malware recognition capabilities using one of the industry's largest sample repositories, collected in the wild from a vast network of global sensors. As ransomware continues to evolve, Bitdefender accurately detects new patterns in pre-execution and at runtime.

Advanced Anti-Exploit

Ransomware authors use exploit kits that take advantage of zero-day or unpatched vulnerabilities to gain a system foothold. Bitdefender focuses on attack techniques to protect systems and prevent ransomware from spreading. Advanced anti-exploit technologies can quickly identify and terminate malicious processes automatically.

Network Protection

Network Attack Defense uses behavioral heuristics to analyze host network activity in real-time and harden controls against exploit techniques that can exfiltrate personal information from your network. It uses machine learning to block ransomware exploits that arrive via network ingress points such as BlueKeep. Network Protection also serves to halt malicious activity in the initial access, credential access, discovery and lateral movement attack stages.

Monitoring and Early Detection

Advanced Threat Control

GravityZone monitors running processes in real time—registry key modifications, file reads/writes, encryption action—to identify suspicious or malicious processes for automatic or manual termination by security teams.

EDR and Incident Response

Not all attacks can be blocked or prevented, and some attack stages manifest slowly over time. EDR will always have a role in ransomware mitigation. GravityZone EDR automatically correlates multiple indicators of attack and compromise (IOAs/IOCs) with malicious activity observed on the system and on the network, facilitating fast and accurate incident response that reduces attacker dwell time and facilitates fast file recovery from ransomware.

User and System Risk Mitigation

Vulnerability Patching

Unpatched systems leave organizations susceptible to ransomware attacks. GravityZone's Patch Management module helps organizations keep operating systems and applications up to date across the entire Windows install base including desktop and laptop workstations, physical servers and virtual servers.

System Misconfigurations

Improperly configured systems leave doors wide open to ransomware attacks including browser security settings, network and credential settings, operating system security settings like open ports, nonessential services and administrative scripting tools (e.g. PowerShell) enabled. GravityZone scans for system misconfigurations and can automatically update many settings of misconfigured machines remotely while notifying the admin to reset the rest.

Application Vulnerabilities

Outdated applications with known vulnerabilities (CVEs) can be exploited by ransomware authors to misuse program functionality or to download harmful content from the internet. Risky applications can either be updated to a newer, safer version or can be removed from the system if the application is not required by the user. GravityZone scans for CVEs and ranks the application vulnerabilities by severity so that administrators can take prompt corrective action.

Risky User Behaviors

Users add risk of ransomware infection every time they open an email, click a link or download a file. GravityZone Human Risk Analytics looks at where users browse, what files they open, what file locations they access, how and where they login to risky websites and monitors password hygiene and reuse so risky behavior can be corrected.

Why You Need Bitdefender Ransomware Mitigation

Comprehensive ransomware protection on endpoints is critical, as endpoints are the gateways to high-value servers and other targets hosting proprietary information, customer data, payment details and other valuable intellectual property. The benefits of Bitdefender Ransomware Mitigation include:

- Hands-free business continuity assurance against all common ransomware attack vectors
- Peace of mind that your security solution is adaptive to defeat new and emerging ransomware techniques
- Freedom from exclusive reliance on problematic onsite backups or long restore times from cloud backups
- Local, network and incident-based file restoration and breach mitigation options to recover from attacks
- Mistakes happen! Bitdefender moves the restrictive security vs. user productivity balance in favor of the user

Bitdefender Ransomware Mitigation Use Cases

Bitdefender covers more ransomware mitigation use cases than competing solutions, offering users and security admins tools at multiple levels to keep ransomware at bay. Thorough prevention and remediation take place at the endpoint, network and GravityZone Console administration levels, whether the initial attack was successful or not.

Local Ransomware Mitigation

For Local Ransomware Mitigation, administrators can configure Bitdefender security policy to monitor endpoint processes and recover the encrypted files as soon as the adaptive technology detects and blocks the attack. Even if ransomware manages to encrypt the local files, mitigation technology immediately jumps in to recover those files, either automatically or on-demand where the admin controls the timing of the recovery of the encrypted files.

Remote Ransomware Mitigation

For Remote Ransomware Mitigation, the security administrator can enable the technology to monitor network share paths that can be accessed remotely and prevent the files from being encrypted. On the remote endpoint, the user agent confirms that Ransomware Mitigation intercepted the remote malicious process behavior and protected the files. Bitdefender administrators can quickly run audit reports and find out more information about the IP address from where the remote ransomware attack was launched and the security module which protected the endpoint, and they can also receive an email notification when an attack is blocked containing information about the attacker's IP address.

Incident Management from GravityZone

On GravityZone, security teams have complete visibility of the attack kill chain and the files affected by the ransomware attack. Bitdefender EDR detects the ransomware activity and security administrators can either kill the active malicious process or quarantine the infected files. They can also permanently blacklist the IP address of the attacker.

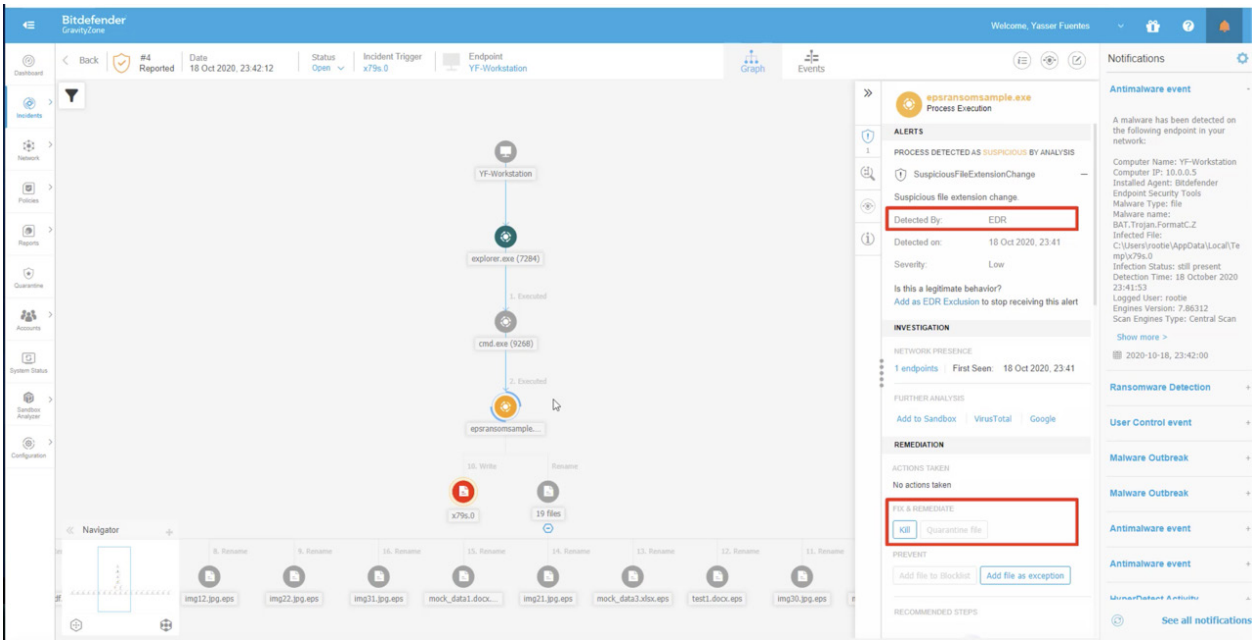

Figure 3: GravityZone EDR incident response shows the full ransomware attack kill-chain

The GravityZone Difference

Ransomware prevention and mitigation is built into the GravityZone Management Console and the Bitdefender Endpoint Security Tools (BEST) client at multiple levels, far exceeding competing security solutions.

GravityZone's Unmatched Combination of Ransomware Defenses	
Multiple Blocking Layers	Endpoint and network, pre-execution and on-access, file-based and fileless
Multiple Detection Layers	Process inspection, registry monitoring, code inspection, Hyper Detect
Multiple Recovery Layers	Effective rollback from local machine, remote system or EDR incident
Adaptive Defenses	Advanced anti-exploit, adaptive heuristics, tunable machine Learning
Risk Mitigation Technologies	Automatic vulnerability patching, system misconfigurations, user behavior
Tamperproof Backups	No use of vulnerable shadow copies, ransomware can't delete the backups
Remote Ransomware Blocking	Blocks remote and network ransomware attacks and blacklists attacker IPs
Enterprise-Wide Cleanup	Kill processes remotely, easy global file quarantine and removal

GravityZone's unmatched combination of ransomware defenses

The Most Awarded Endpoint Security Vendor

Bitdefender is consistently ranked tops in independent third-party tests and evaluations:

- Ranked #1 and PC Editors' Choice for "Best Hosted Endpoint Protection and Security Software for 2020"
- Ranked #1 and PC Editors' Choice for "Best Mac Antivirus Protection for 2020"
- Leader in the Forrester Wave for Cloud Workload Security, Q4-2019
- "The biggest EDR vendor you haven't considered but should have" – Forrester Research
- 100% detection vs. real world threats, AV-Test (Jan-Aug 2020)

See Bitdefender GravityZone in Action

- See for yourself: Watch the demo video highlighting the many ways that Bitdefender counteracts ransomware.

Get Protected against Ransomware

Get a free 90-day full-product evaluation of GravityZone Ultra Plus with our unique, limited time offer.

Service providers, get a free 45-day full-featured trial of multi-tenant Bitdefender GravityZone Cloud MSP Security.

Contact Us for More Information and a Demo

For further information, please contact us to schedule an in-depth product demonstration and discussion of Bitdefender GravityZone and how it works to prevent and mitigate ransomware attacks.

Bitdefender is the technology provider of choice, with 38% of cybersecurity vendors worldwide using one or more Bitdefender technologies, validating our product quality and highest detection accuracy. We are committed to developing technologies in house and to maintaining over 50% of our workforce in research and development roles.

Why Bitdefender

Proudly Serving Our Customers

Bitdefender provides solutions and services for small business and medium enterprises, service providers and technology integrators. We take pride in the trust that enterprises such as **Mentor, Honeywell, Yamaha, Speedway, Esurance or Safe Systems** place in us.

Leader in Forrester's inaugural Wave™ for Cloud Workload Security
NSS Labs "Recommended" Rating in the NSS Labs AEP Group Test
SC Media Industry Innovator Award for Hypervisor Introspection, 2nd Year in a Row
Gartner® Representative Vendor of Cloud-Workload Protection Platforms

Dedicated To Our +20.000 Worldwide Partners

A channel-exclusive vendor, Bitdefender is proud to share success with tens of thousands of resellers and distributors worldwide.

CRN 5-Star Partner, 4th Year in a Row. Recognized on CRN's Security 100 List. CRN Cloud Partner, 2nd year in a Row
More MSP-integrated solutions than any other security vendor
3 Bitdefender Partner Programs - to enable all our partners – resellers, service providers and hybrid partners – to focus on selling Bitdefender solutions that match their own specializations

Trusted Security Authority

Bitdefender is a proud technology alliance partner to major virtualization vendors, directly contributing to the development of secure ecosystems with **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS, and Pivotal.**
Through its leading forensics team, Bitdefender is also actively engaged in countering international cybercrime together with major law enforcement agencies such as FBI and Europol, in initiatives such as NoMoreRansom and TechAccord, as well as the takedown of black markets such as Hansa. Starting in 2019, Bitdefender is also a proudly appointed CVE Numbering Authority in MITRE Partnership.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

CRN AV-TEST AV Gartner 451 Research FORRESTER IDC GLOBAL

TECHNOLOGY ALLIANCES

Microsoft NUTANIX aws Pivotal Cloud Foundry CITRIX

Bitdefender

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-TechSolutionBrief-FIPM_DSZ-WEB_USE_ONLY-creat4845-en_EN
10/20/20January 4, 2021 9:42 pm01/04/21