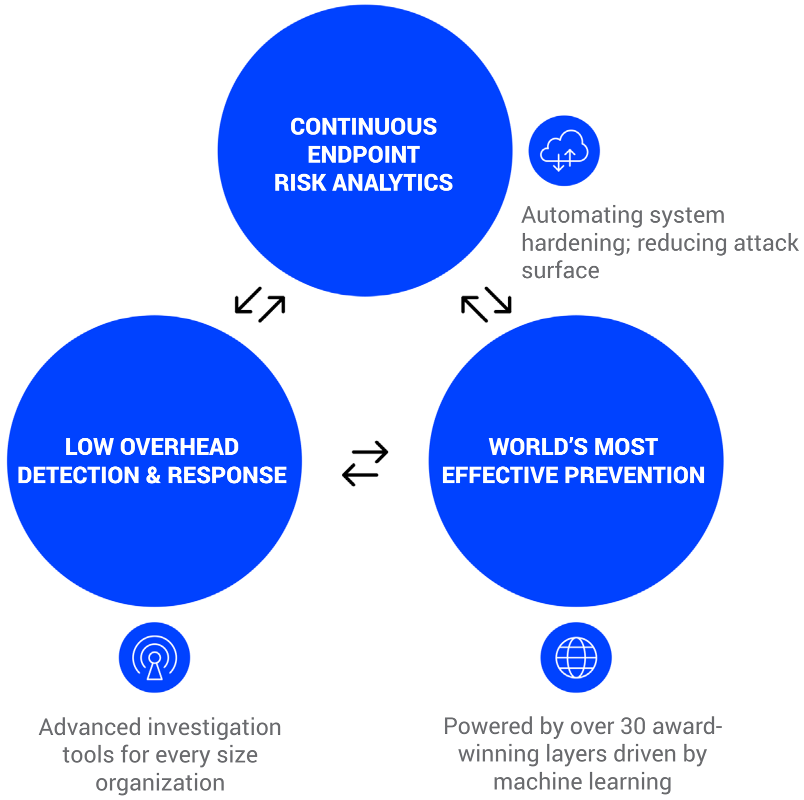
Bitdefender GravityZone Ultra Suite

Unified Endpoint Prevention, Detection, Response and Risk Analytics

With over 30 layers of protection technology, GravityZone Ultra is the first solution to offer the world's most effective protection integrated with unique low overhead EDR and Endpoint Risk Analytics in a single agent, single console architecture. This dramatically reduces the endpoint attack surface, helping companies of any size avoid breaches, simplify security management and dramatically reduce the cost of security operations. GravityZone Ultra provides:

- **The world's most effective Endpoint Protection** which regularly ranks at the top in independent prevention tests
- **Low overhead Endpoint Detection and Response** which makes it easy for any IT organization to adopt EDR, improve response time and lower the personnel cost of EDR
- **Integrated Endpoint Risk Analytics** constantly scans your endpoints for misconfigurations and makes recommendations to reduce your attack surface
- **Single agent-single console** for all capabilities including patch management, firewall, encryption, application control, content control and more
- Optional **Patch Management**, **Advanced Email Security** and **Data Protection** add on modules streamline security processes and reduce incident response times
- **Blocks majority of attacks at the pre-execution phase** before they affect your system via machine learning real-time process inspection and automated sandbox analysis
- A single solution that covers **physical**, **virtual** and **cloud** deployments from one console
- Optional **Network Threat Analytics Solution** to provide insights into IoT and potential network threats
- Protection for Complex, Heterogeneous Environments: as an integrated endpoint protection suite, GravityZone Ultra ensures a consistent level of security across all of your platforms, from Windows™ to MacOS, Linux, VMware™ to iOS to Android to AWS™. The results is that attackers can find no gaps in protection to exploit. GravityZone Ultra relies on a simple, integrated architecture with centralized management for both endpoints and datacenter. It lets companies deploy the endpoint protection solution quickly and requires less administration effort after implementation.


CONTINUOUS ENDPOINT RISK ANALYTICS
Automating system hardening; reducing attack surface
LOW OVERHEAD DETECTION & RESPONSE
Advanced investigation tools for every size organization
WORLD'S MOST EFFECTIVE PREVENTION
Powered by over 30 award-winning layers driven by machine learning

Key Benefits

As Bitdefender's premier security suite, GravityZone Ultra provides security analysts and incident response teams with the tools they need to analyze suspicious activities and investigate and adequately respond to advanced threats:

- World leading threat prevention
- Real-time detection and automatic remediation
- Fast incident triage, investigation and response
- Suspicious activity detection
- Configuration risk analytics
- One-click incident response
- Automatic hardening
- Current and historic data search for threat hunting
- MITRE tagging of events

Digitally signed by Ciocleа Victor
Date: 2020.05.21 10:30:33 EEST
Reason: MoldSign Signature
Location: Moldova

The World's Most Effective Endpoint Protection

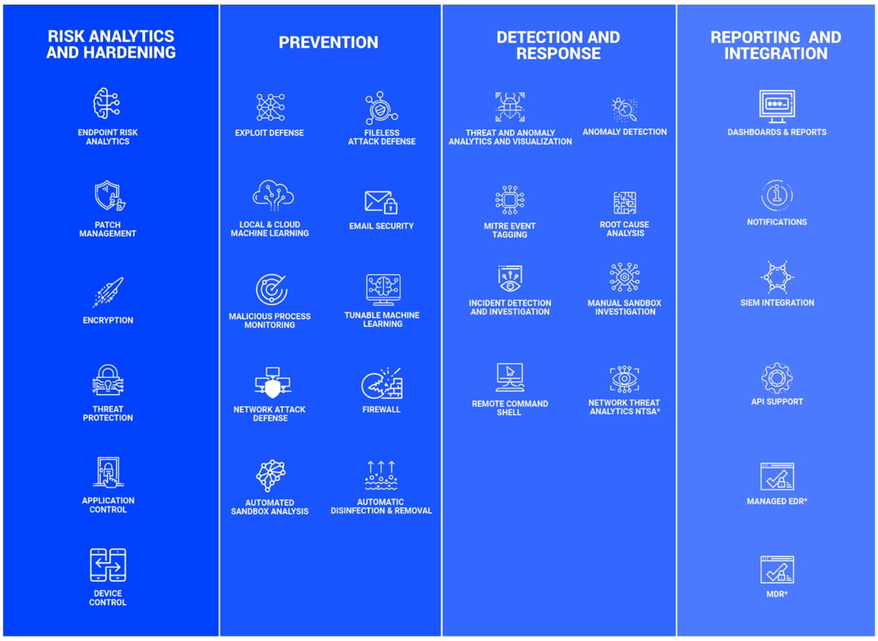
For end-to-end breach defense

Over 30 protection technologies developed over 18 years by Bitdefender's world class researchers, mathematicians and data scientists result in superior protection that is currently licensed and used in over 38% of all IT security products.

- **Local and Cloud based Machine Learning:** Bitdefender first launched machine learning in 2009, resulting in increased threat detection with low false positives that can stop unknown threats at pre-execution and on-execution
- **Hyperdetect - Tunable machine learning:** Enables IT teams to tune protection on sensitive business services with the highest risk
- **Anomaly Defense:** Advanced machine learning technology that baselines system services and monitors for stealthy attack techniques. Able to protect custom apps from malicious attack
- **Cloud-Based Sandbox:** provides pre-execution detection of advanced attacks by automatically sending files that require further analysis to cloud sandbox and taking remediation action based on the verdict
- **Network Attack Defense:** Detect and block new types of threats earlier in the attack chain, such as brute force attacks, password stealers, lateral movement
- **Exploit Defense:** Several exploit prevention engines protect memory and block attacks before they exploit systems, reducing triage efforts
- **Fileless Attack Defense:** Detect and block script-based, file-less, obfuscated and custom malware with automatic remediation
- Integrated client firewall, device control, web content filtering, app control and more
- **Add-on modules:** Email Security, Full Disk Encryption, Patch Management

GRAVITYZONE ULTRA TECHNOLOGY MAP

GravityZone Ultra is the ultimate in advanced protection, detection, response and risk analytics designed to address the entire threat lifecycle. With GravityZone Ultra, you can reduce the number of vendors while compressing the time it takes to respond to threats via an integrated security stack.



RISK ANALYTICS AND HARDENING
ENDPOINT RISK ANALYTICS
PATCH MANAGEMENT
ENCRYPTION
THREAT PROTECTION
APPLICATION CONTROL
DEVICE CONTROL

PREVENTION
EXPLOIT DEFENSE
FILELESS ATTACK DEFENSE
LOCAL & CLOUD MACHINE LEARNING
EMAIL SECURITY
MALICIOUS PROCESS MONITORING
TUNABLE MACHINE LEARNING
NETWORK ATTACK DEFENSE
FIREWALL
AUTOMATED SANDBOX ANALYSIS
AUTOMATIC DISINFECTION & REMOVAL

DETECTION AND RESPONSE
THREAT AND ANOMALY ANALYTICS AND VISUALIZATION
ANOMALY DETECTION
MITRE EVENT TAGGING
ROOT CAUSE ANALYSIS
INCIDENT DETECTION AND INVESTIGATION
MANUAL SANDBOX INVESTIGATION
REMOTE COMMAND SHELL
NETWORK THREAT ANALYTICS NTSA*

REPORTING AND INTEGRATION
DASHBOARDS & REPORTS
NOTIFICATIONS
SIEM INTEGRATION
API SUPPORT
MANAGED EDR*
MDR*

*OPTIONAL

Low Overhead EDR Made Easy

Full featured investigation tools designed for any size organization

With clear visibility into indicators of compromise (IOCs) and one-click threat investigation and incident response workflows, GravityZone Ultra reduces resource and skill requirements for security teams.

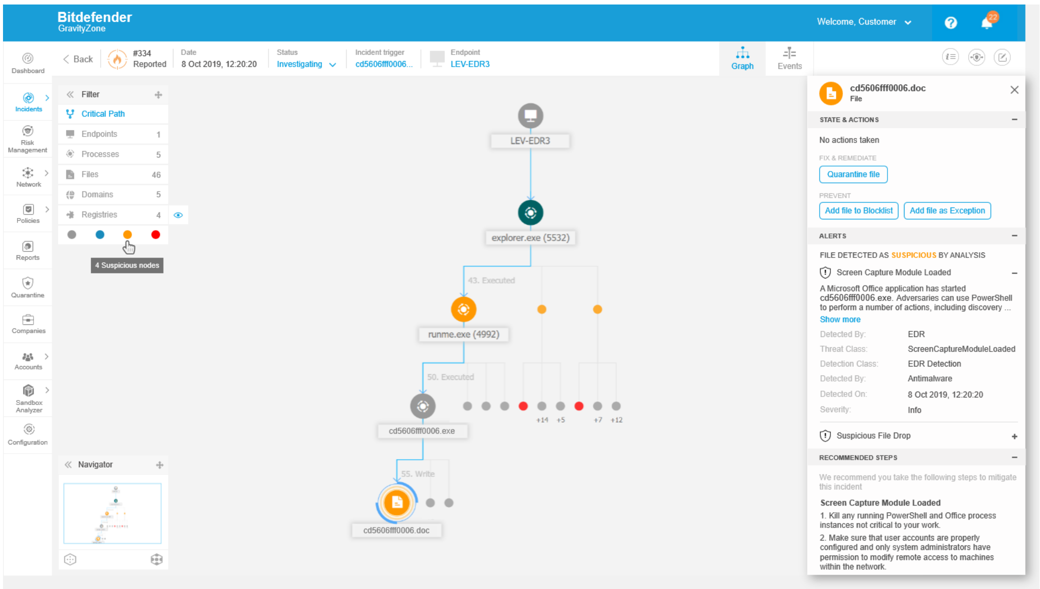
Threat analytics module operates in the cloud and continuously sifts through behavioral events in system activities and creates a prioritized list of incidents for additional investigation and response.

Smart response means evolved prevention

Because GravityZone Ultra is an integrated prevent-detect-respond solution, it enables quick response and restoration of endpoints to a "better-than-before" stage. Leveraging threat intelligence gathered from the endpoints during the investigation process, a single interface provides the tools to immediately adjust policy and patch vulnerabilities to prevent future incidents, improving the security of your environment.

Address the Security Skills Shortage and Avoid alert fatigue.

Only relevant, correlated and severity-rated events are presented for manual analysis and resolution. Noise and redundant information is kept at a minimum, as the vast majority of attacks and advanced attacks are blocked at the pre- or on-execution stages. Elusive threats, including fileless malware, exploits, ransomware and obfuscated malware are neutralized by the highly effective layered next-gen endpoint prevention technologies and on-execution behavior-based process inspector. Automatic response and repair eliminate the need for human intervention in blocked attacks.



#334 Reported

Date: 8 Oct 2019, 12:20:20

Status: Investigating

Incident trigger: cd5606fff0006...

Endpoint: LEV-EDR3

Endpoints	1
Processes	5
Files	46
Domains	5
Registries	4

cd5606fff0006.doc
File

STATE & ACTIONS

No actions taken

FIX & REMEDIATE

Quarantine file

PREVENT

Add file to Blocklist | Add file as Exception

ALERTS

FILE DETECTED AS SUSPICIOUS BY ANALYSIS

Screen Capture Module Loaded

A Microsoft Office application has started cd5606fff0006.exe. Adversaries can use PowerShell to perform a number of actions, including discovery ...
Show more

Detected By:	EDR
Threat Class:	ScreenCaptureModuleLoaded
Detection Class:	EDR Detection
Detected By:	Antimalware
Detected On:	8 Oct 2019, 12:20:20
Severity:	Info

Suspicious File Drop

RECOMMENDED STEPS

We recommend you take the following steps to mitigate this incident

Screen Capture Module Loaded

1. Kill any running PowerShell and Office process instances not critical to your work.
2. Make sure that user accounts are properly configured and only system administrators have permission to modify remote access to machines within the network.

Ultra delivers mainstream EDR requirements:

- Suspicious activity detection and visualization
- Anomaly detection
- Root cause analysis
- MITRE event tagging
- Threat confidence score
- Attack indicators
- Remote command shell
- Guided incident investigation
- Advanced threat containment options
- Sandbox analysis
- Optional managed detection and response service.

Advanced detection and response shows precisely how a potential threat works and its context in your environment. MITRE attack techniques and indicators of compromise provide up to the minute insight into named threats and other malware that may be involved. Easy to understand visual guides highlight critical attack paths, easing burdens on IT staff.

Endpoint Risk Analytics for Continuous Attack Surface Management

Enables Active System Hardening Processes Across the Enterprise

Bitdefender’s Endpoint Risk Analytics (ERA) engine enables organizations to continuously assess, prioritize, and harden endpoint security misconfigurations and setting with an easy-to-understand prioritized list. With unique risk analytics, there is continuous attack surface reduction

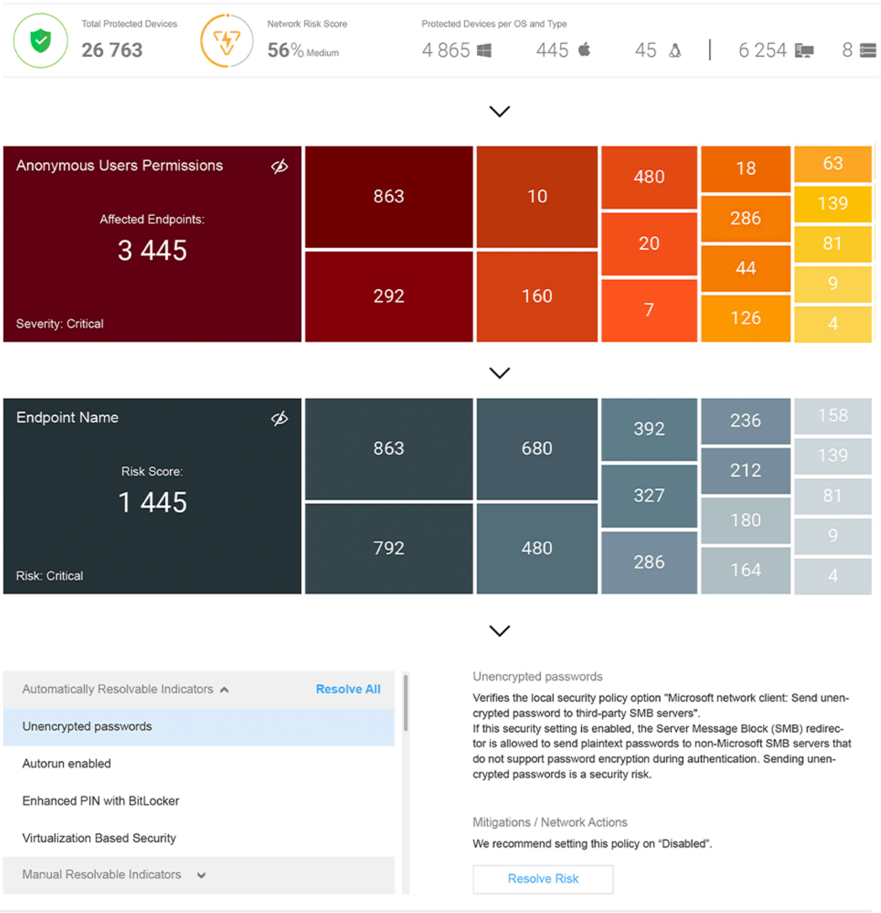
.

1 Enterprise-Wide **Risk Dashboard**

2 View prioritized
risks across the Enterprise

3 **See the highest priority**
endpoints by Risk Score

4 View Indicators of Risk by endpoint
and **manually or automatically**
fix specific recommendations.



Unencrypted passwords

Verifies the local security policy option "Microsoft network client: Send unencrypted password to third-party SMB servers".
If this security setting is enabled, the Server Message Block (SMB) redirector is allowed to send plaintext passwords to non-Microsoft SMB servers that do not support password encryption during authentication. Sending unencrypted passwords is a security risk.

Mitigations / Network Actions

We recommend setting this policy on “Disabled”.

Third Party Ecosystem partner integration

Supports integration with your existing security operations tools (including Splunk) and optimized for datacenter technologies including all major hypervisors.

For more information and detailed system requirements please visit:
https://www.bitdefender.com/business/enterprise-products/ultra-security.html

Or contact your local Bitdefender partner.

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.

FOR MORE INFORMATION VISIT: bitdefender.com/business