Technical Brief

Web version only.
Not for print.

Bitdefender®

GravityZone Ultra Plus

Prevention, Detection and Response across Endpoint, Network and Cloud

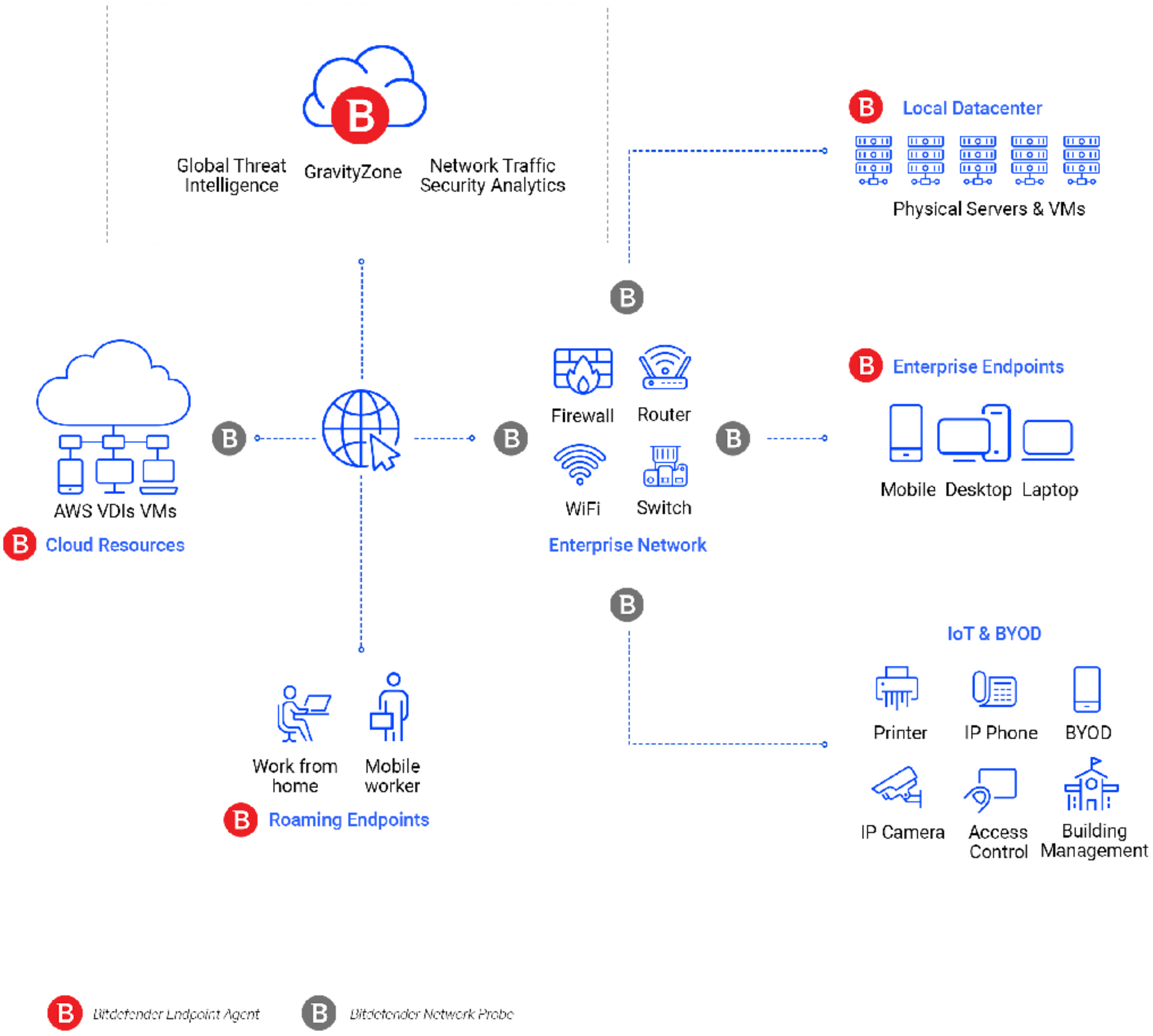
www.bitdefender.com

Overview

GravityZone Ultra Plus combines endpoint-based and network-based security technology stacks to collect data from the entire infrastructure to:

- Increase capabilities to detect advanced threats
- Provide 360-degree visibility into threat activity in the enterprise environment
- Equip organizations with the full set of incident-investigation capabilities
- Enable the complete set of incident response options: automatic, semi-automatic and manual.

eXtended Detection and Response (XDR)

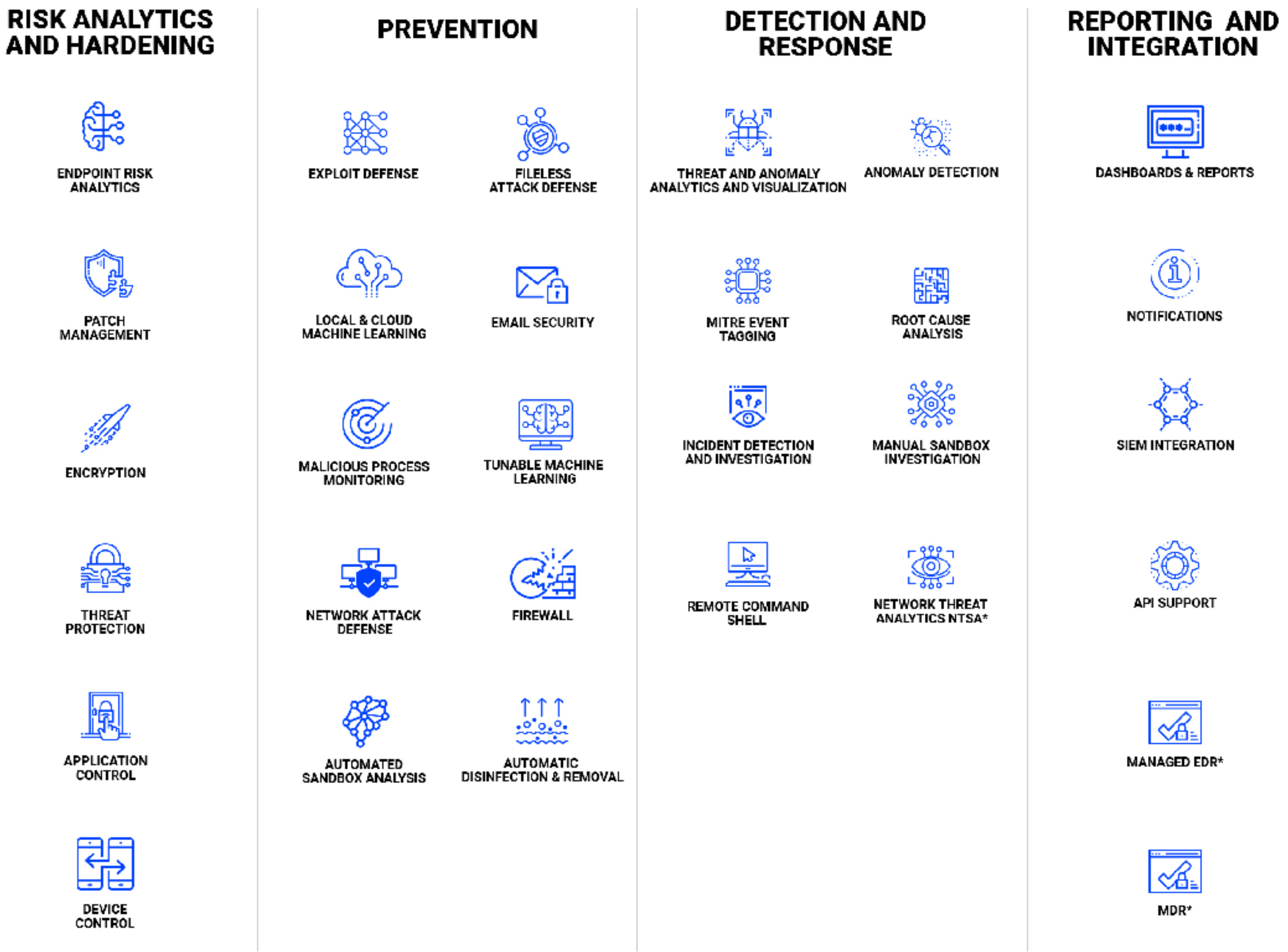


Traditional Endpoint Detection and Response solutions rely on the analysis of endpoint data alone to detect cyber threats. As attacks evolve, this might deprive the security team of valuable insights that can come out of other types of information, such as network traffic. GravityZone Ultra Plus uses an XDR model and applies ML, event correlation and threat intelligence to data collected from all elements of the enterprise infrastructure: endpoints (physical or virtualized), cloud resources and network elements.

The XDR is the optimal security approach for the modern enterprises with a complex environment and growing attack surface. It can protect traditional endpoints that support agent-based security, devices that lack the resources to run a security agent, like IOT, or devices outside the control of corporate IT, like BYOD. In contrast to using multiple security solutions to achieve the same goal, Ultra Plus provides a coherent management approach and consistent security across all devices in the environment.

GravityZone Ultra Plus key components

The endpoint-based 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*

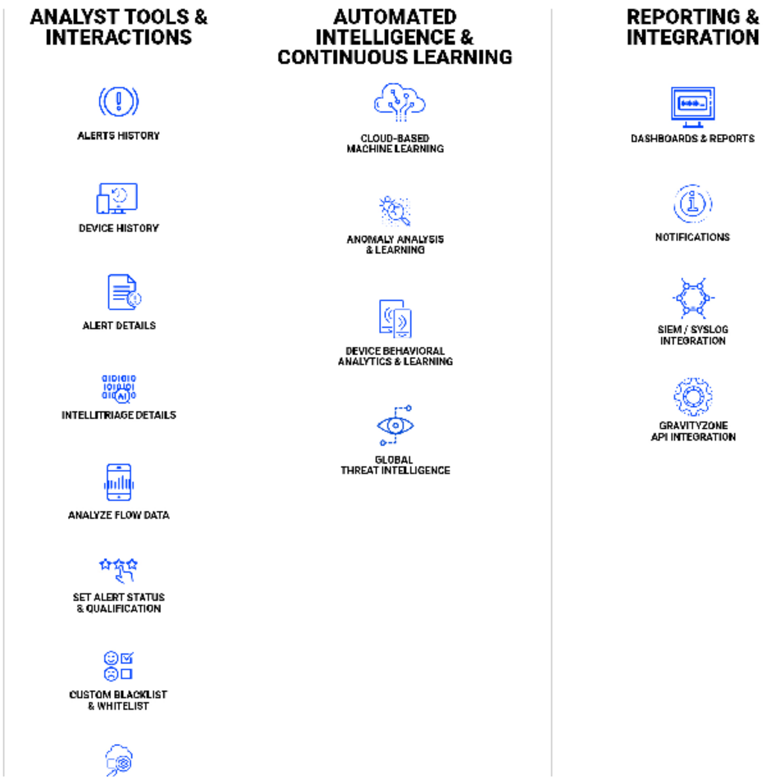
REPORTING AND INTEGRATION

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

The Bitdefender Endpoint Agent incorporates multiple layers of security technologies that can detect and block attacks throughout the threat lifecycle:

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

The network-based security stack


ANALYST TOOLS & INTERACTIONS
ALERTS HISTORY
DEVICE HISTORY
ALERT DETAILS
INTELLITRIAGE DETAILS
ANALYZE FLOW DATA
SET ALERT STATUS & QUALIFICATION
CUSTOM BLACKLIST & WHITELIST
AUTOMATED INTELLIGENCE & CONTINUOUS LEARNING
CLOUD-BASED MACHINE LEARNING
ANOMALY ANALYSIS & LEARNING
DEVICE BEHAVIORAL ANALYTICS & LEARNING
GLOBAL THREAT INTELLIGENCE
REPORTING & INTEGRATION
DASHBOARDS & REPORTS
NOTIFICATIONS
SIEM / SYSLOG INTEGRATION
GRAVITYZONE API INTEGRATION

Bitdefender Network Traffic Security Analytics uses network communications as the foundational data source for detecting and investigating malicious behavior and security threats.

Network flows data (meta-data) extracted by the network probes is analyzed by applying ML, Behavioral Analytics and Bitdefender Threat Intelligence. The security incident alerts are automatically triaged to reduce operational effort and to provide context and insights on threat-related activity.

WHY BITDEFENDER?

UNDISPUTED INNOVATION LEADER.

38% of all cybersecurity vendors worldwide integrated at least one Bitdefender technology. Present in 150 countries.

#1 RANKED SECURITY. AWARDED ACROSS THE BOARD.

WORLD'S FIRST END-TO-END BREACH AVOIDANCE

The first security solution to unify hardening, prevention, detection and response across endpoint, network and cloud.

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-GZUltra-TechnicalBrief-creat4315-en_EN
03/11/20March 11, 2020 3:07 pm03/11/20