
Bitdefender

Keeping You Safe in the Wild Wild Web

Michael Reeves, CISSP
Technical Director, Cloud & MSP

WHO IS Bitdefender®

Advanced Threat Intelligence continuously built into GravityZone hardening, prevention, detection and response technologies

WHO IS Bitdefender

Advanced Threat Intelligence continuously built into GravityZone hardening, prevention, detection and response technologies

30 Billion Daily threat queries from hundreds of millions of sensors worldwide

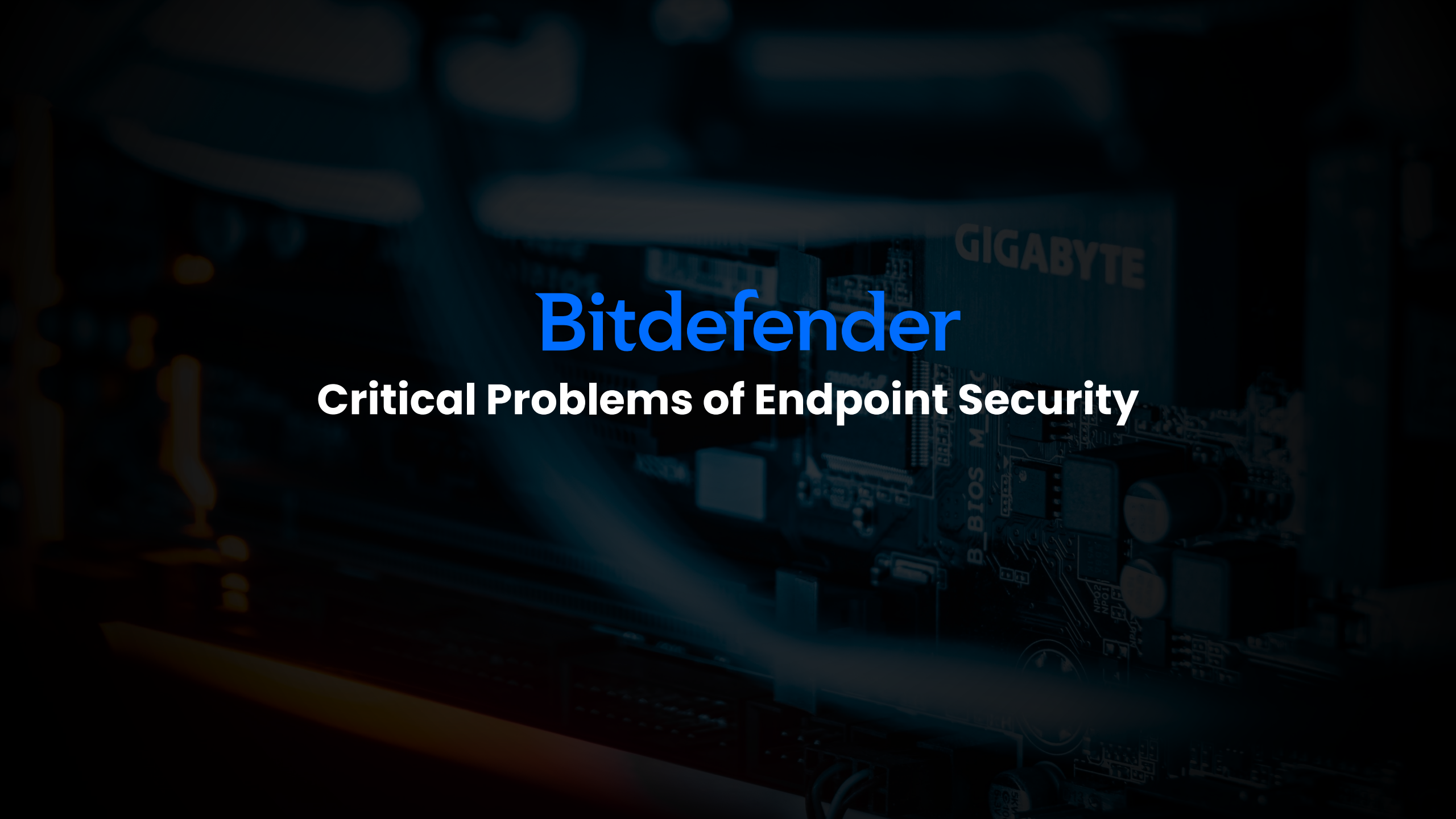
400+ Threats discovered and processed every minute (criminals, nation-states, malicious actors)

$1.6 Billion In savings for over 55,000+ customers by **32** ransomware decryptors provided free to the market

476 Patents issued for core technologies

285 Elite security researchers, threat hunters and security analysts. Close collaboration on incident response with law enforcement; Working with leading academics on quantum computing and cryptography

400+ R&D employees focused on cloud, emerging technology, IoT research and machine learning



Bitdefender

Critical Problems of Endpoint Security

Bitdefender

Critical Problems of Endpoint Security

Prevention

High Efficacy Prevention is Essential:

- Reduces incidents
- Reduces staff workload
- Reduces breaches

Bitdefender

Critical Problems of Endpoint Security

Prevention

High Efficacy Prevention is Essential:

- Reduces incidents
- Reduces staff workload
- Reduces breaches

Detection and Response

- Correlated 360 Degree Continuous Monitoring of all Endpoints
- Use Response Tools to Quickly Recover from an attack

Bitdefender

Critical Problems of Endpoint Security

Prevention

High Efficacy Prevention is Essential:

- Reduces incidents
- Reduces staff workload
- Reduces breaches

Detection and Response

- Correlated 360 Degree Continuous Monitoring of all Endpoints
- Use Response Tools to Quickly Recover from an attack

System Hardening

Use Risk Analytics to Reduce the Attack Surface by Fixing Misconfigurations, Identifying Vulnerable Applications, and Identifying User Vulnerabilities

Bitdefender

Critical Problems of Endpoint Security

Prevention

High Efficacy Prevention is Essential:

- Reduces incidents
- Reduces staff workload
- Reduces breaches

Detection and Response

- Correlated 360 Degree Continuous Monitoring of all Endpoints
- Use Response Tools to Quickly Recover from an attack

System Hardening

Use Risk Analytics to Reduce the Attack Surface by Fixing Misconfigurations, Identifying Vulnerable Applications, and Identifying User Vulnerabilities

Bitdefender

Security Hardening

Bitdefender

ENDPOINT RISK ANALYTICS

- System Misconfiguration is the second biggest cause of security breaches.
- Majority of threats target well-known applications and configuration vulnerabilities.
- Many forms of ransomware can be blocked with simple configuration changes.
- “Patch panic” caused by not knowing which systems are truly at risk

Bitdefender

Endpoint Risk Analytics

KEY FEATURES

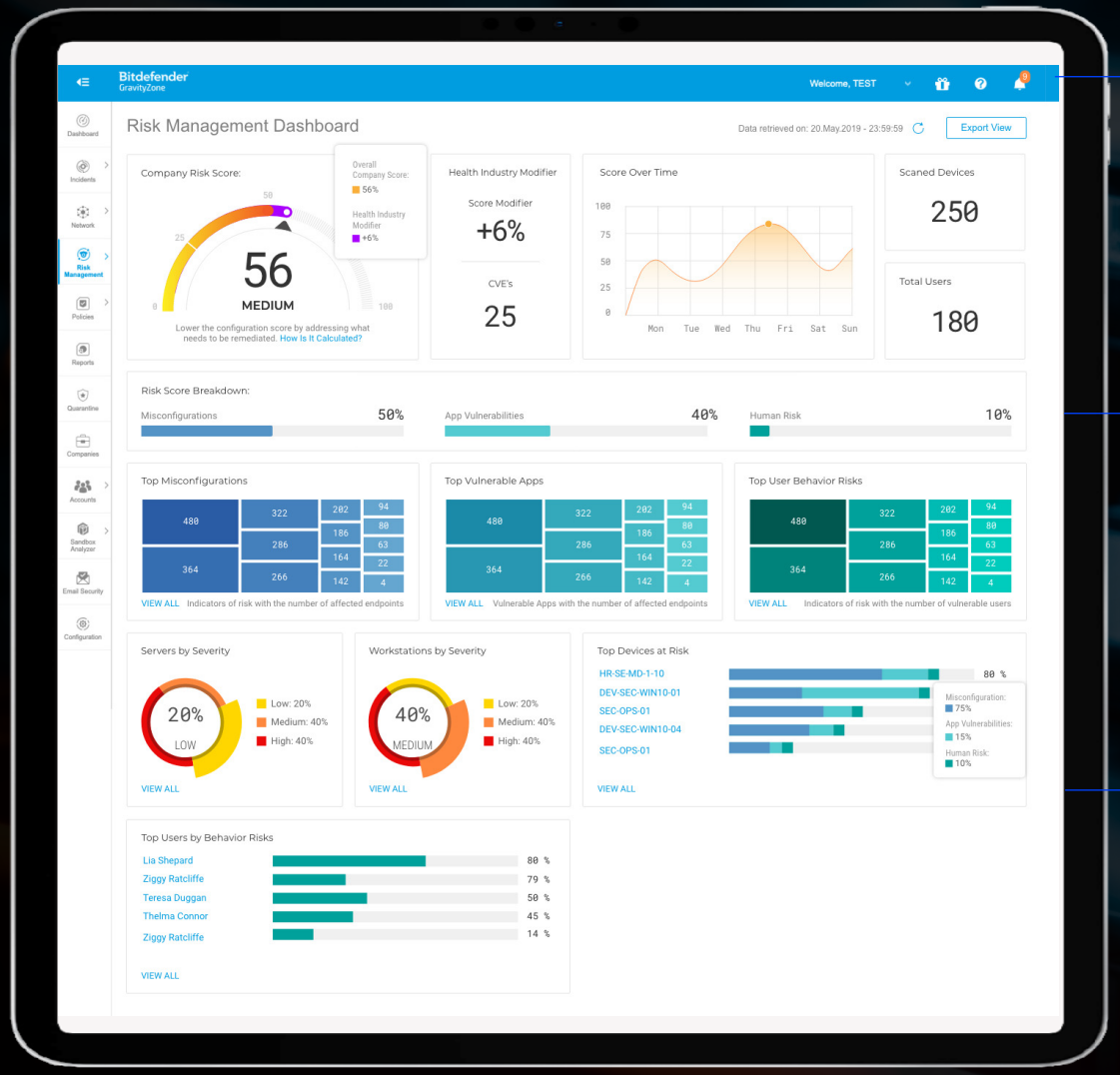
- Risk analytics engine continuously computes a risk score to easily sort and prioritize assets
- Prioritizes security remediation on risk severity and prevalence across 206 indicators
- Automatic fix available for many indicators
- Enables System Hardening with Gravity Zone Patch, Encryption, Device Control, Application Control and Firewall
- Fully native to all Gravity Zone products
- Powered by Bitdefender Labs global threat research

Example Configuration Analytics Rules:

- ASLR Disabled
- Session Manager Protection Mode Disabled
- Insecure Guest Logon Enabled
- No Autorun Disabled
- Telnet Service Enabled

Bitdefender

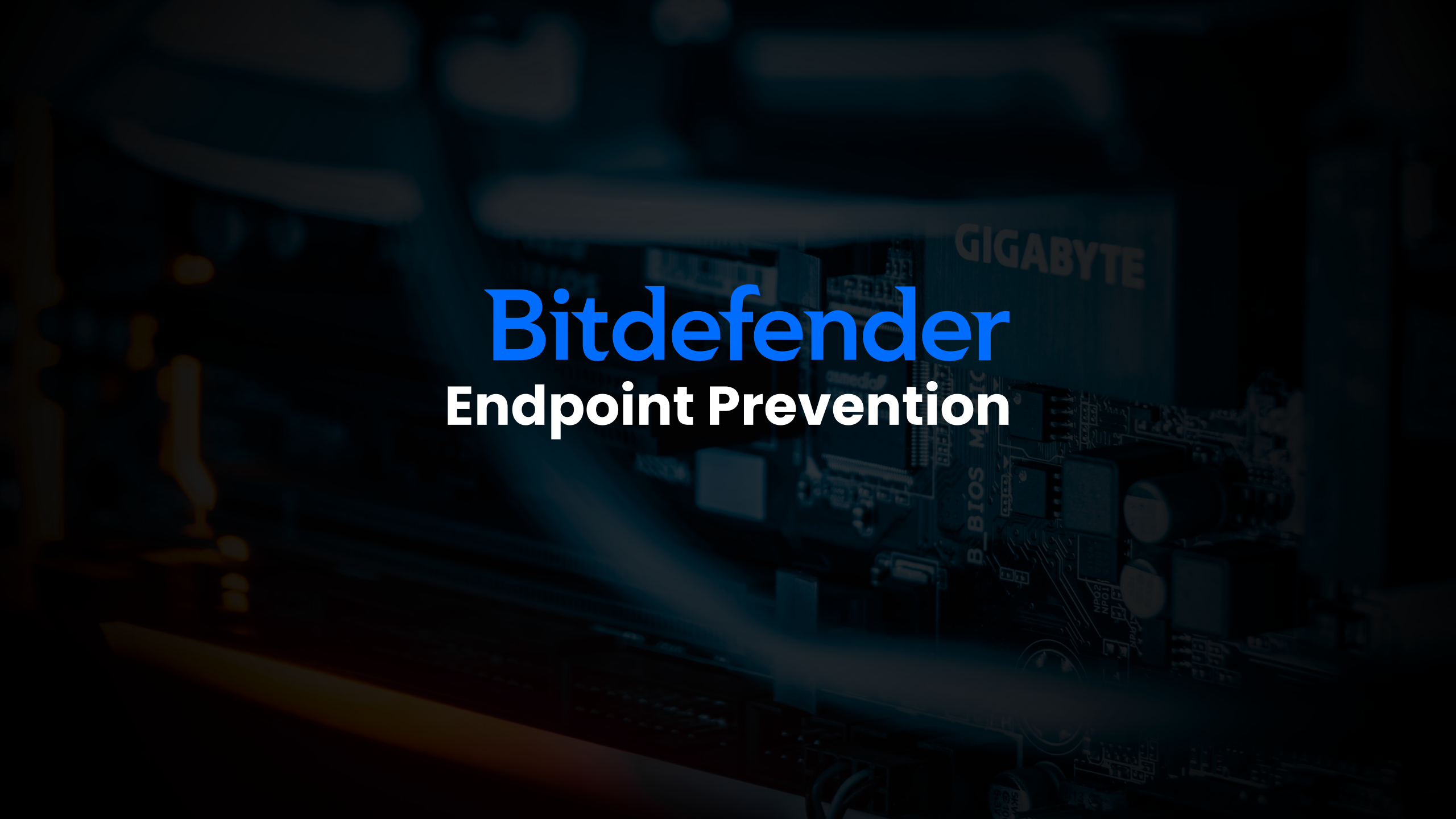
Gravity Zone Endpoint Risk Analytics



Customer Risk Dashboard

View Prioritized Risk

See the highest priority endpoints by Risk Score

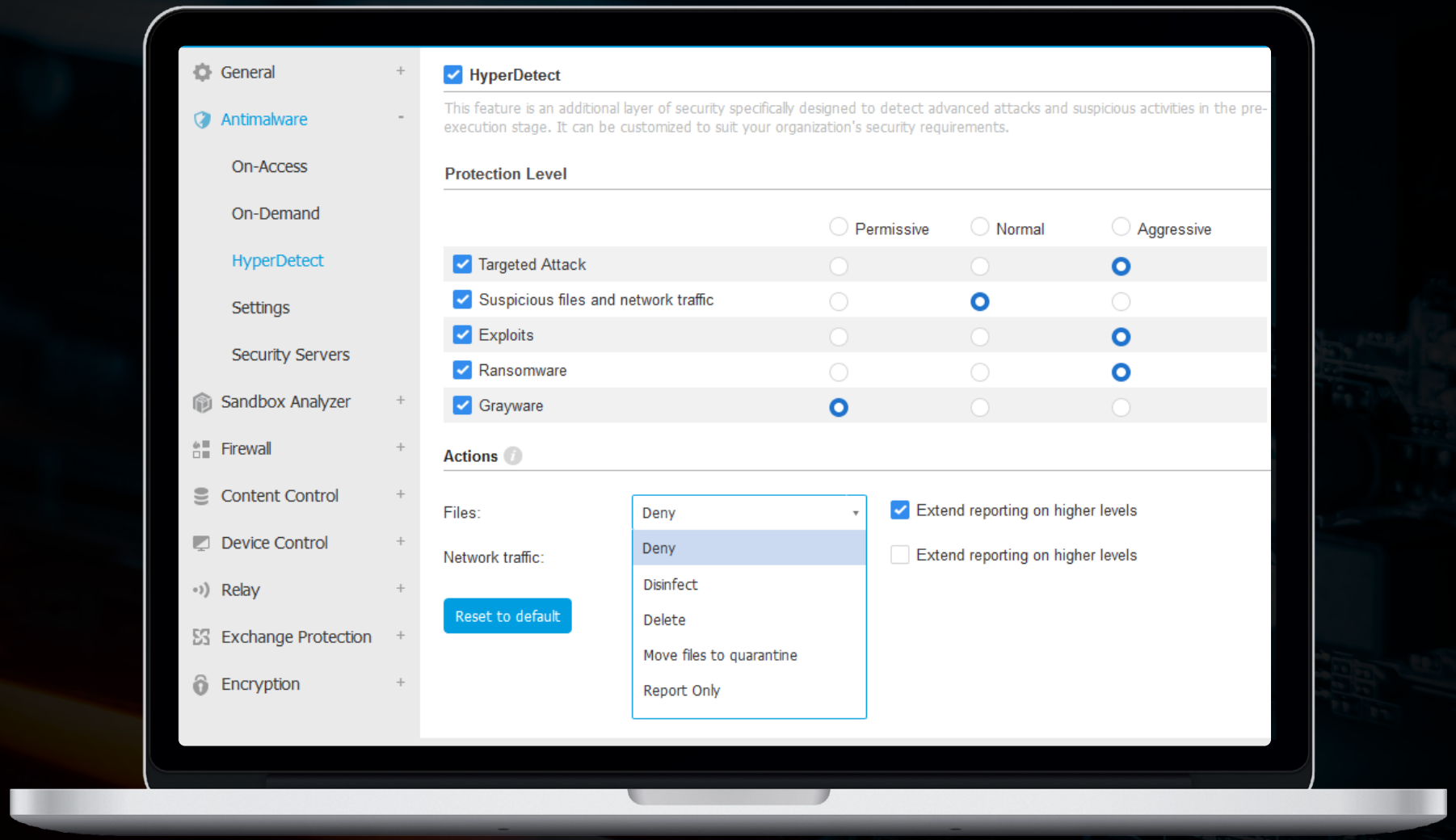


Bitdefender

Endpoint Prevention

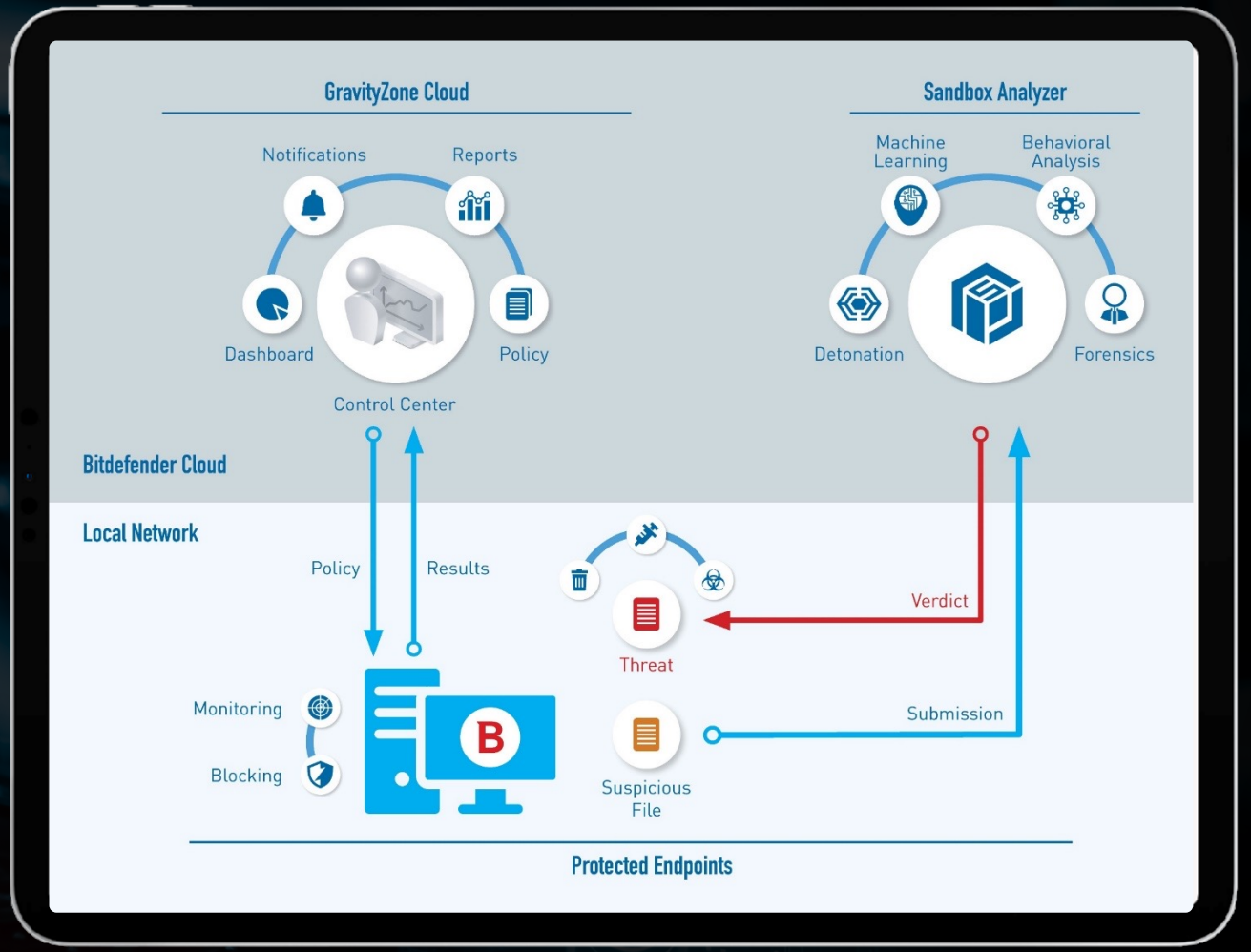
Bitdefender

Hyper detect – Tunable Machine Learning



Bitdefender

Sandbox Analyzer



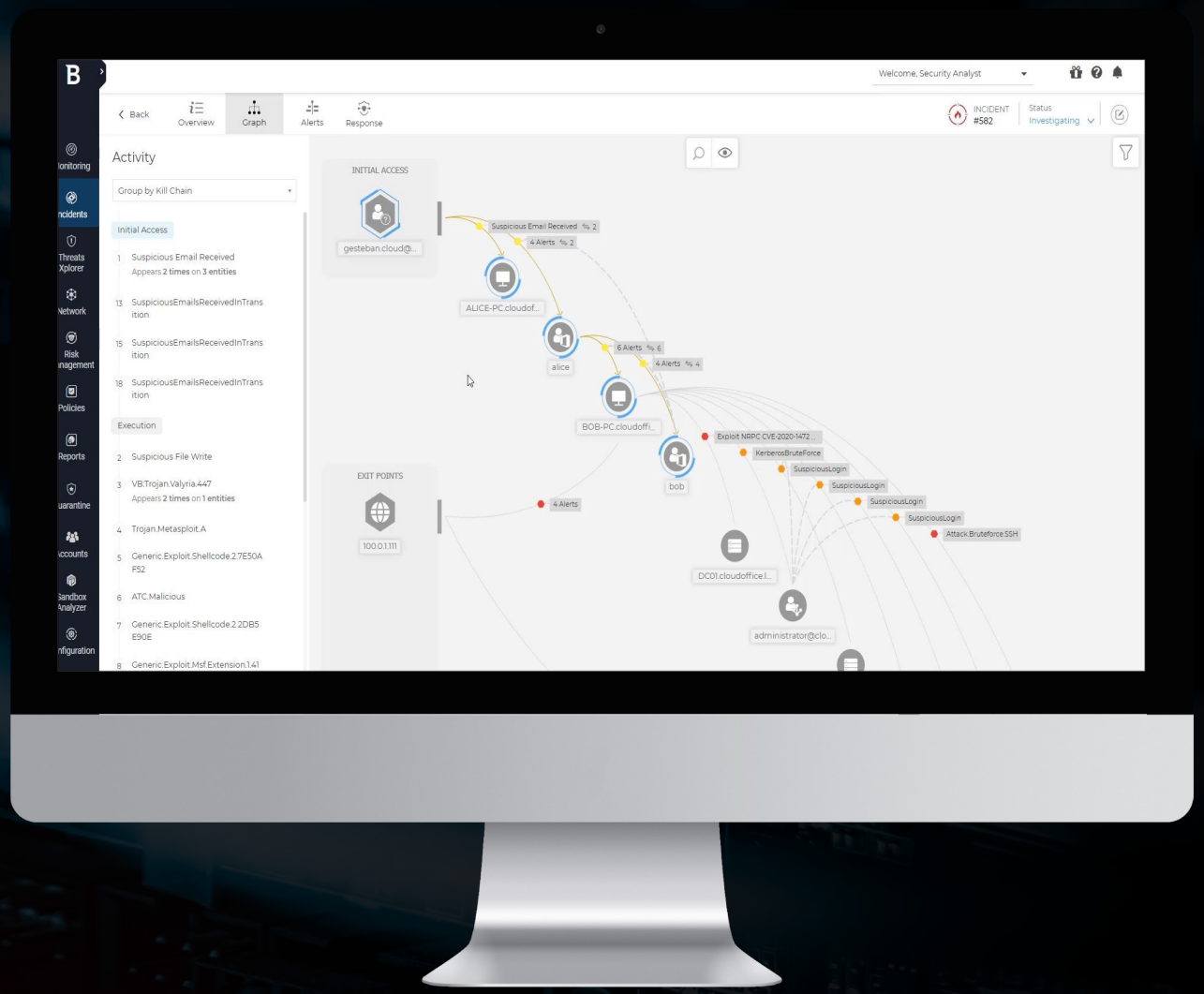

Bitdefender
EDR

Bitdefender

Correlated Visualization Across Endpoints

- Extended detection and response shows precisely how a potential threat works and its context in your environment.

- Easy to understand visual guides highlight critical attack paths, easing burdens on IT staff.

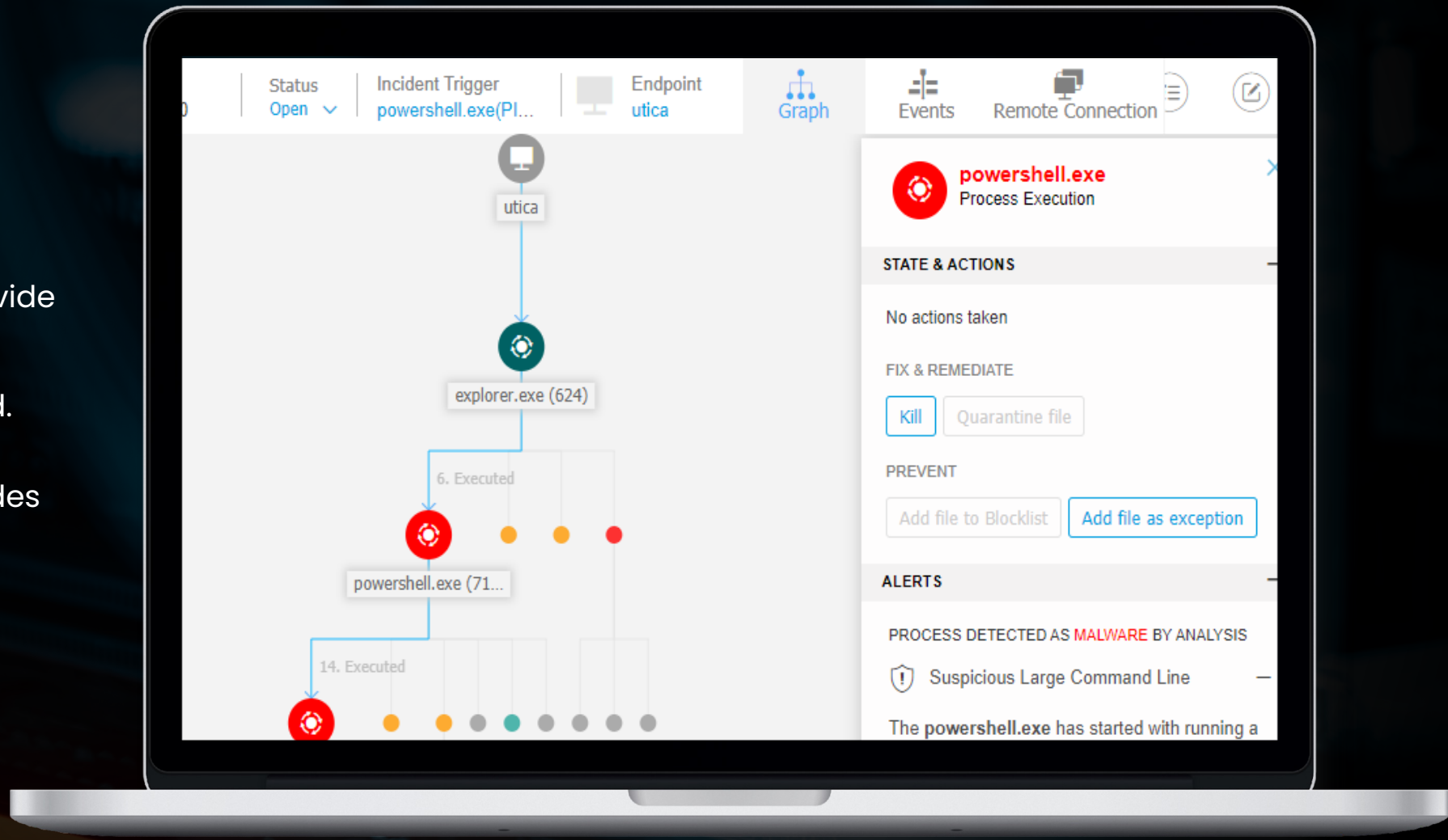


Bitdefender

EDR WORKFLOW & VISUALIZATION

- **MITRE** attack techniques and indicators of compromise provide up to the minute insight into named threats and other malware that may be involved.

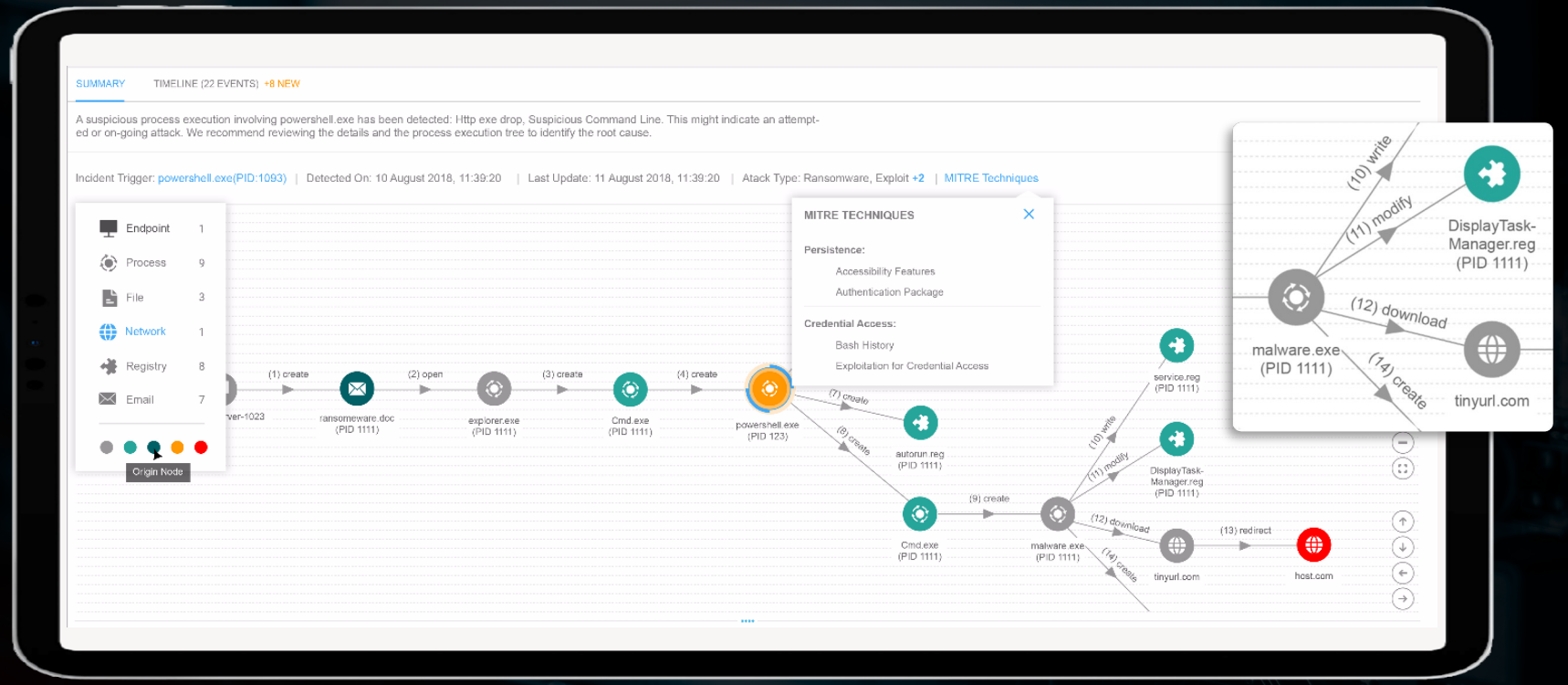
- Easy to understand visual guides highlight critical attack paths, easing burdens on IT staff.



Bitdefender

Pre and Post compromise attack forensics

Root Cause Analysis



The end-to-end attack forensics provides visibility into past actions covering the lifecycle of an attack (before, during and after). It covers both blocked attacks and suspicious activities.

Bitdefender

MITRE Engenuity ATT&CK Evaluation

Highest number of detections among all 29 solutions evaluated

- This confirms the results obtained in other industry 3rd party tests and sets apart Bitdefender Gravity Zone as the best solution in detecting the full range of cyber-threats.
- Bitdefender also stands out in the results for enabling efficient security operations and reducing alert fatigue by providing analytics insights for 96% of all detections.

Total Number of Detections

Bitdefender

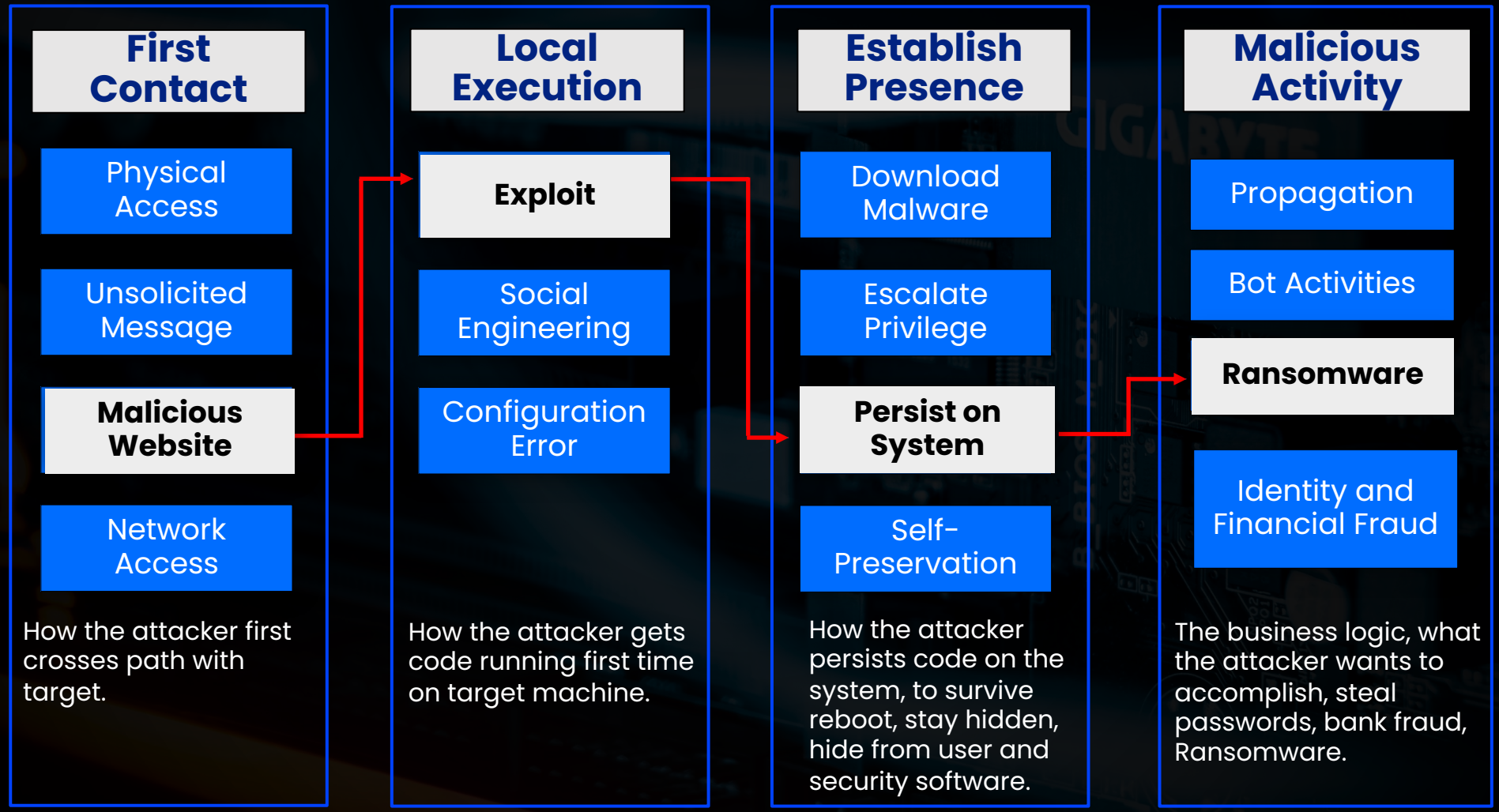
Detections vs Analytics Insights In EDR Solutions

DETECTIONS

ANALYTICS INSIGHTS

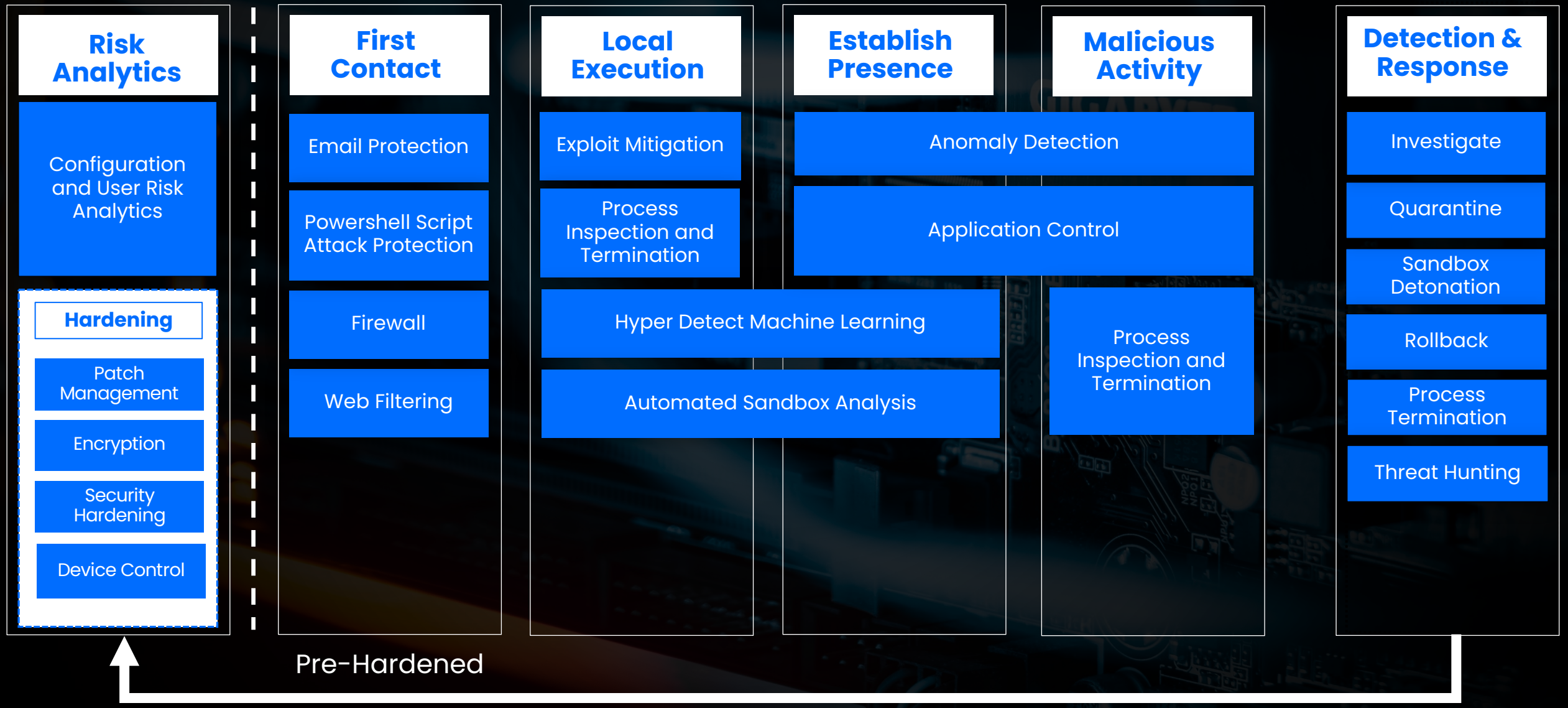
Bitdefender

The Phases of Attacks



Bitdefender

PROTECTION TECHNOLOGIES



Bitdefender

ConnectWise Core Integrations

CONNECTWISE
Automate

- Client Mapping
- Deployment
- Alerting
- Tickets
- Quarantine Management

CONNECTWISE
SIEM

- Threats
- Co-Managed

CONNECTWISE
MDR

- Fully-Managed SOC
- Including Remediation
- Rollback
- Isolate Host
- Sandbox Detonation
- Kill process
- Quarantine object
- Add object to Blocklist
- Add object to Exception List

CONNECTWISE
PSA

- Billing
- Ticketing

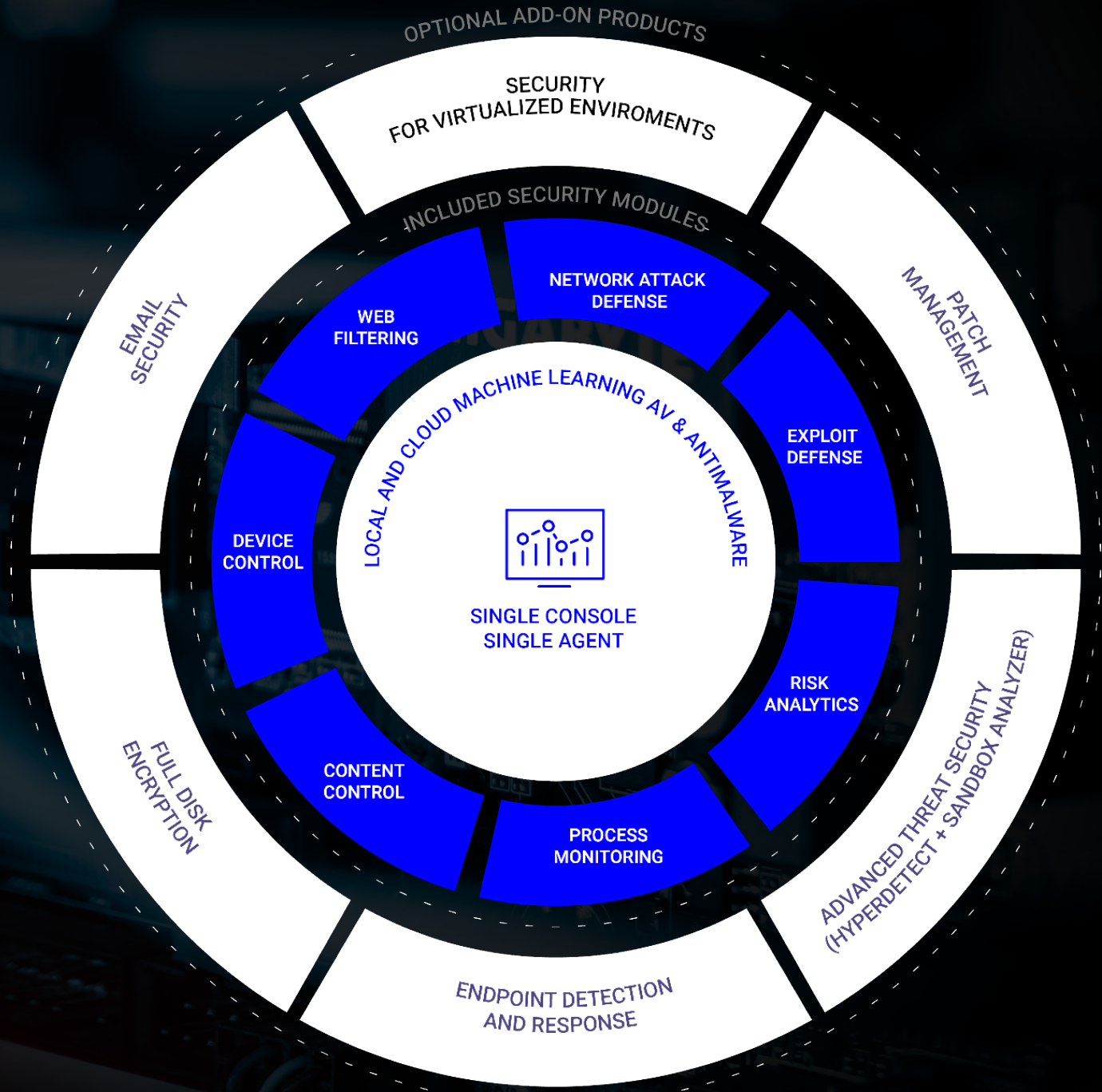
CONNECTWISE
RMM

- Site mapping & creation
- Endpoint provisioning (presence detection, install, uninstall) for windows x32/x64, and Mac & Linux installation

Bitdefender

BITDEFENDER GRAVITYZONE CLOUD MSP SECURITY

- Most comprehensive MSP Endpoint Security Suite
- Automation through APIs and integration with RMM/PSA, SIEM and other platforms
- Single multitenant console + simple usage-based monthly licensing
- Opportunity to grow security & revenues with optional add-on layers




Bitdefender
THANK YOU