Solution Brief

Bitdefender®

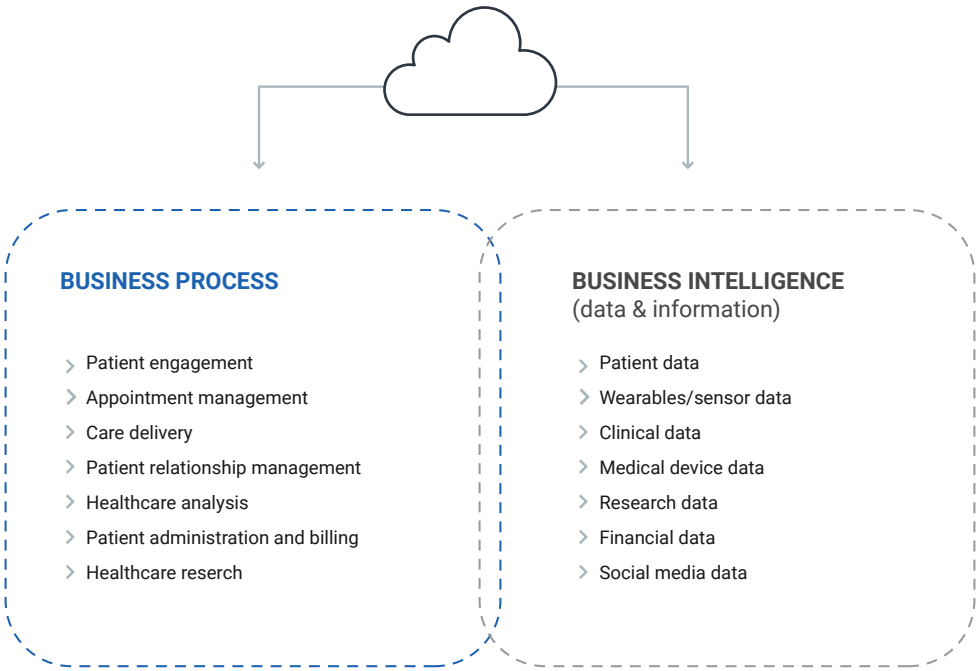
Securing complex infrastructures in healthcare organizations with Bitdefender GravityZone™

Contents

Healthcare IT infrastructure - vital and always changing

Technology has become indispensable to how healthcare is distributed and how effective it is. In the process, IT infrastructure in the sector has become increasingly intricate to accommodate progressively specific needs and boost productivity.

The industry's digital transformation is also **adding layers of complexity and changing workflows**. Each change introduced into the organization, from devices to processes, adds new items on security leaders' agenda.



Source.

From an IT infrastructure perspective, healthcare organizations are substantially diverse which makes securing them an even more challenging process than it already is.

While healthcare CISOs may have similar challenges in common, they also have vastly different resources to overcome them. And it's not just malicious behavior they have to protect against, but less obvious threats that impact productivity and weaken their organization's security posture.

For example, new internet-connected devices expand the attack surface and reduce the overall security of healthcare organizations in both obvious and less conspicuous ways.

During a proof of concept, Bitdefender uncovered a strain of cryptocurrency mining malware inside an MRI machine. The cryptojacking malware took a toll on the machine's performance but not to a degree that would raise suspicion. While trying to disguise its malicious behavior, it interfered with doctors' activity, impacting productivity.

It's threats like these that often dwell in healthcare organizations for lack of a security suite powerful enough to identify and remove them before they escalate into data breaches or other forms of compromise.

To meet the current needs of the sector, security must match **the 4 Ps of medicine**:

Predictive

Preventive

Personalised

Participatory

The range of connected medical devices, systems & applications

Desktops

- Servers
- Smartphones
- Tablets
- Specialized medical equipment
- Bedside computer terminals
- Bedside medication verification
- Medical imaging devices
- Implantable medical devices (IMD), etc.
- IoMT
- BYOD
- Self-service kiosks
- mHealth systems

Medical Software

- EHR/EMR systems
- Medical practice management software
- PACS (Picture Archiving & Communication Systems)
- Patient Data Management Systems
- Patient scheduling systems
- ePrescription applications
- Telemedicine platforms
- Patient portals
- Medical billing systems with/without online payment
- Third-party clinical systems integrations
- Real-time locating services for tracking systems for instruments, devices & clinical staff

IT infrastructure

- VDIs, public cloud or multi-cloud deployments
- On-premises data centers
- Hybrid infrastructures
- Legacy systems
- Internal networks connecting all devices, cloud deployments & medical equipment

A benefits vs security risks overview for healthcare IT infrastructure elements

Technology layer	Healthcare benefits	Security risks
Specialized medical devices (medical imaging devices, IMDs, etc.)	• In-dept medical investigations • More accurate results • Better patient care	• Exposed to targeted cyber attacks • Highly valuable target for their data and processing power
BYOD	• More flexibility • Better data accessibility • Improved availability to medical staff	• Insecure texting • Data leakage • Device theft or loss • Device fragmentation
IoMT	• Improved patient care through real-time data • Better chronic disease and drug management • Useful health alerts	• Unencrypted devices • No 2FA options • No regular security updates • No remote data erasure
mHealth systems	• Enhanced access to patient data • Better patient compliance with medication/treatment • Statistical data to improve healthcare on mass population level	• Unauthorized access to patient data through social engineering attacks • Mobile malware attacks • Device misuse such as connecting to unprotected public Wi-fi
EHR/EMR systems	• More accurate diagnostics based on up to date patient data • Reduced rate of medical errors • Coordinated, more efficient patient care	• Encryption blind spots • Phishing and social engineering attacks • Patient care disruption because of extended EHR unavailability caused by cyber attacks
Virtual Desktop Infrastructure	• Improved accessibility to patient data • Decreased administrative costs • Can be used for BYOD deployment	• Visibility loss because of faster desktop deployment • Increased IT governance complexity • Single point of failure
Hybrid infrastructures	• Enhanced operational agility • Expanded storage environments • Virtualized and highly automated	• Poor data redundancy • Unprotected APIs • Authentication failure • Weak IP protection • Data leakage

For lack of a security suite that can protect this wide range of devices, systems, and infrastructures, healthcare organizations continue to fall victim to motivated attackers.

To maintain compliance with key industry regulations and support growth, healthcare organizations much ensure they meet current security requirements.

Security requirements for healthcare IT infrastructures

Keeping up with patient demands, industry regulations, and business needs, security leaders must identify the security suite capable to meet their growing and highly specialized needs.

- **Secure data collection, storage, and management** - essential for compliance, improved patient care, and business growth
- **Safe and flexible access to medical data** - fundamental for mobility and data accessibility and availability
- **High visibility across types of infrastructure and devices** - indispensable for identifying threats in their early stages and mitigating them
- **Hypervisor integration** - necessary to identify memory manipulation techniques associated with zero-day vulnerabilities
- **Automated response to threats** - crucial for access blocking, early containment, and effective clean-up
- **Thorough logging and forensics** - to enable both compliance and strategic security decisions for the entire organizations
- **Unified management** - instrumental for the performance of any security program and for effective use of resources
- **Clear reporting and timely alerts** - vital for prompt response to threats and attacks in their early stages
- **Compliant with healthcare regulations** - essential for avoiding fines and preserving reputation

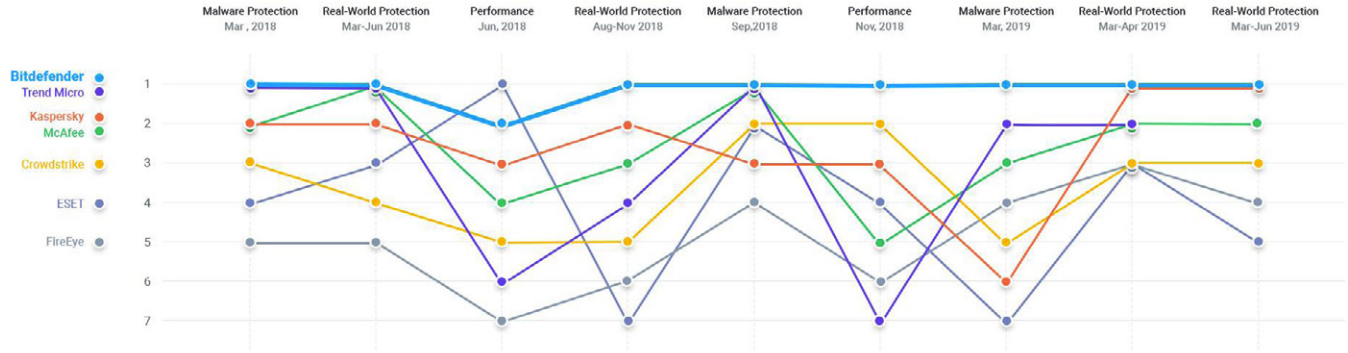
Bitdefender GravityZone™ Ultra Engineered for securing complex healthcare organizations

In the threatscape, we developed a cybersecurity suite that focuses on **a continuous cycle of identifying, protecting, detecting, responding, and recovering from potential cybersecurity incidents**.

Our key objective is to constantly improve the overall security posture of your healthcare organization through:

Top-level performance in terms of protection and agility

Address your healthcare security challenges by choosing a security partner that excels in independent industry tests and has been declared a 2018 Forrester Wave Leader in endpoint security suites.



Robust security across infrastructures and devices

Protect your entire range of devices, systems, and applications with a security suite that covers both traditions and non-traditional infrastructure elements, such as MRIs, IMDs, and more.

GravityZone Control Center

Manage your infrastructures' security from an intuitive and easy to use central console that enables visibility, simplified administration, and automation.

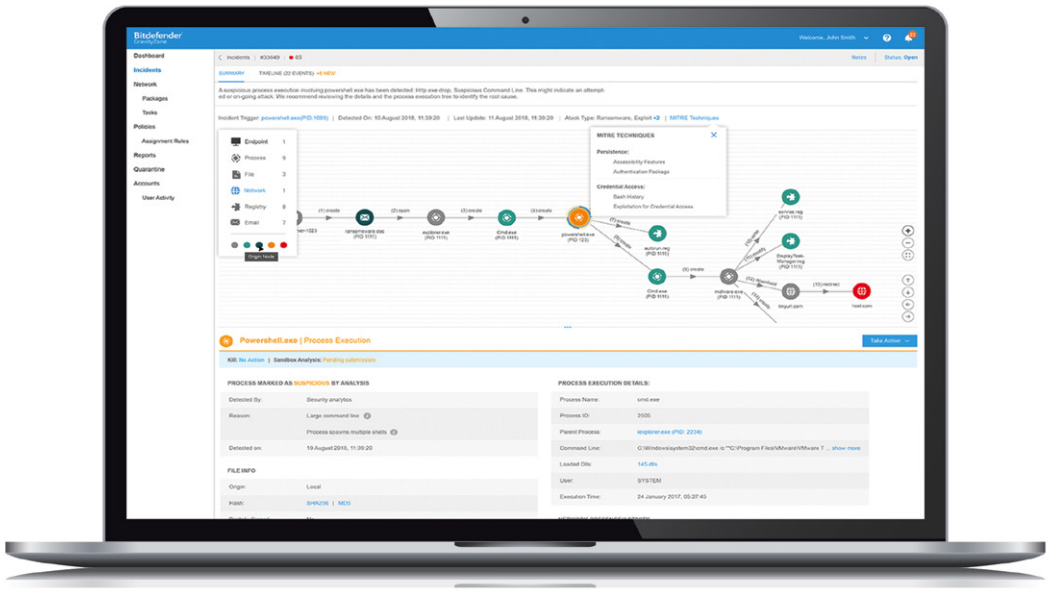
Bitdefender Global Protective Network

Leverage information analyzed from 500M systems that enables GravityZone to anticipate, prevent and detect attacks anywhere in the world in under 3 seconds.

Contextual awareness by combining EDR with a strong EPP

By blending functions specific to an **Endpoint Detection and Remediation** solution with those of an **Endpoint Protection Platform**, we are able to deliver contextual threat indicators and real-time insights into your threatscape.

This enables healthcare organizations like yours to stay ahead of sophisticated threats by having **constant access to accurate, actionable, and relevant threat intelligence**.



Operational efficiency through prevention & automatic remediation

Bitdefender GravityZone™ Ultra is a dependable suite when focusing on improving your effectiveness in terms of security.

Its benefits extend beyond your cybersecurity program, as ensuring the safety of your systems, devices, and data **enables your organization to scale its operations**.

Relying on Bitdefender means you can maintain legacy systems in conjunction with new ones without compromising security throughout the entire digital transformation process.

Bitdefender's **automatic threat response** effectively blocks malware threats from doing additional damage and making lateral movements through your network so you can focus on what matters.

Validated in real-world complex healthcare organizations

"Bitdefender reliably protects our growing enterprise, while eliminating the 'performance tax' the previous security solution imposed on our infrastructure.
It also ***helps our IT staff save time on managing security,*** so they can focus on strategic projects."

Kevin Schokora, Director, IT Operations, Great Expressions Dental Centers - 4,400 endpoints

"We›ve now consolidated workstations and servers, everything is now protected by Bitdefender and it›s centralized. [..]
The console is much easier to use than anything we've used before. We can easily pull up reports and see the status of everything so from that perspective as well it›s freed up a lot of time."

Josh Gilliland, Security Analyst Team Lead, Government Employees Health Association

Bitdefender GravityZone™ A layered security suite that meets your specific needs

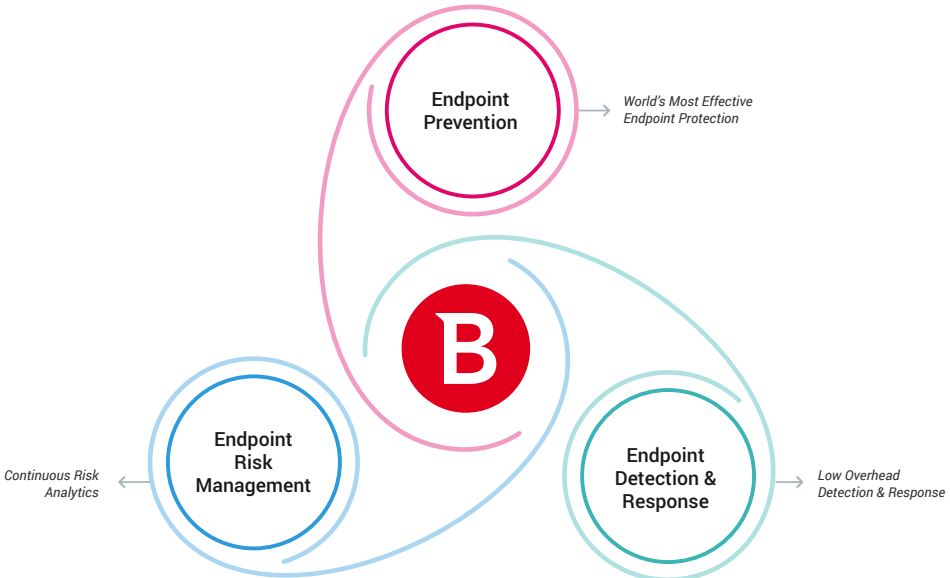
ENDPOINT

Bitdefender GravityZone™ Ultra

The world's most effective security suite integrates **30 layers of protection** for all of your endpoints while maintaining usability and without generating alert fatigue.

Low overhead EDR and Endpoint Risk Analytics (ERA) are built into a single agent with a unified console architecture.

Explore the suite



NETWORK

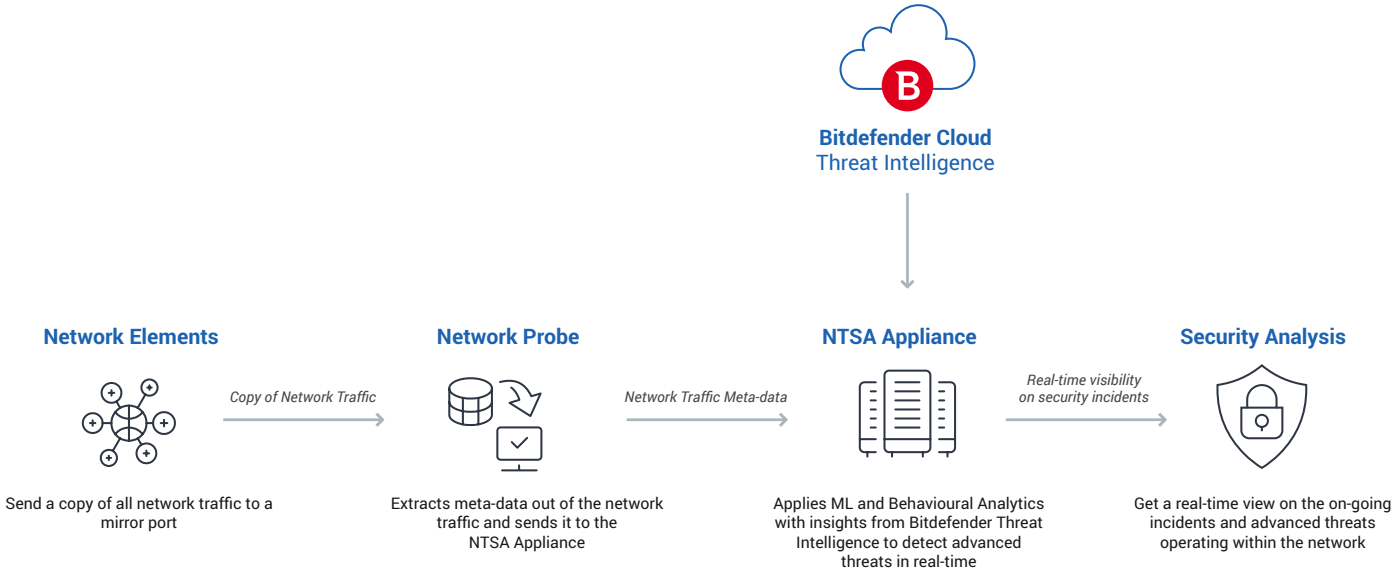
Bitdefender Network Traffic Security Analytics (NTSA)

Bitdefender NTSA is a **plug-and-play, out-of-band solution** that comes with flexible deployment options.

Because it's focused on traffic meta-data, its analysis extends over longer periods of time to **accurately detect the most sophisticated malware** and Advanced Persistent Threats (APTs) with high accuracy.

Bitdefender NTSA excels at protecting your investment in IoMT and other specialized medical devices because it provides **complete visibility** across infrastructures. You can rely on it for **real-time breach detection** and automated triage.

Secure your network



CLOUD

Bitdefender GravityZone™ Security For Virtualized Environments

We engineered the cloud security layer in Bitdefender GravityZone™ to **safeguard software-defined, hyperconverged, and cloud infrastructures** often present in healthcare organizations.

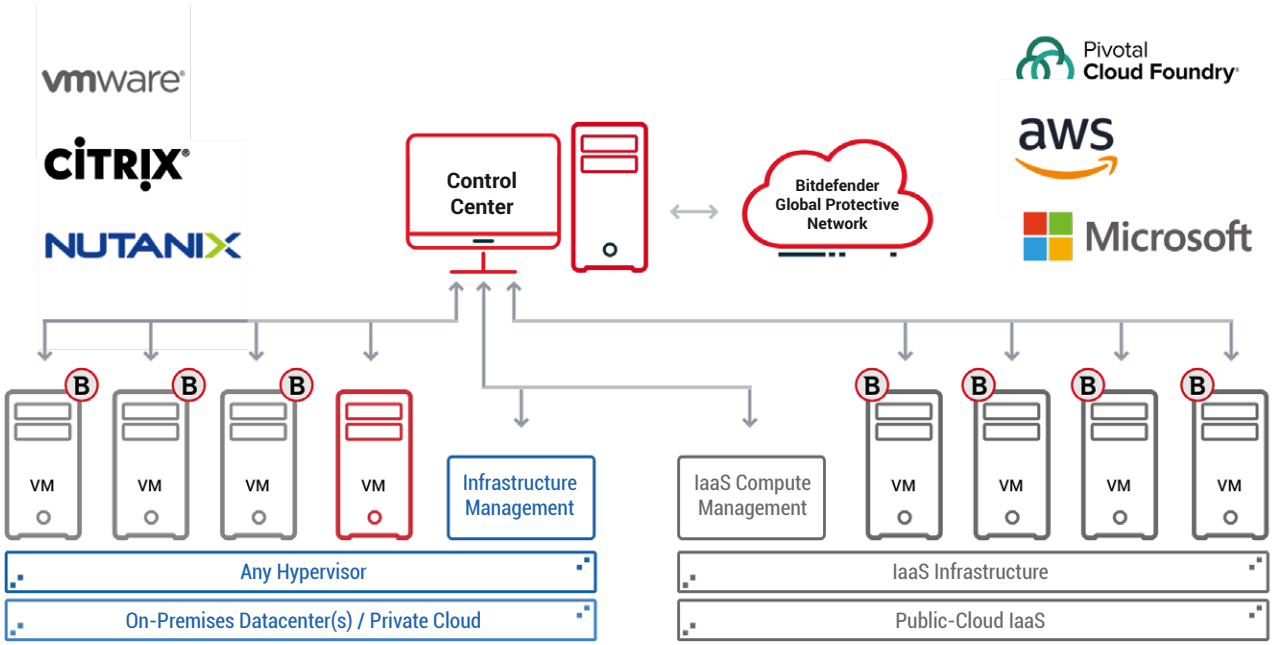
On top of the suite's **award-winning protection**, administrators of datacenter and cloud workloads use it to keep their security agile, efficient, and highly performant.

In hybrid multi-cloud environments (AWS® and Microsoft Azure®), GravityZone™ enables:

- Deep integration with VMware, Citrix, Nutanix, and other software-defined datacenter platforms

- Consistent security-policy administration
- Single-pane-of-glass visibility through centralized management
- Efficient compliance reporting
- Uninterrupted protection as VMs move across the clouds.

Protect your environments



MANAGED

Bitdefender GravityZone™ Endpoint Detection & Response

For healthcare organizations with limited resources and technical skills it can be more effective to **offload threat monitoring, triage, analysis, alerting, and reporting** to an experienced cybersecurity provider.

We created the Bitdefender GravityZone™ Endpoint Detection and Response Service (MDR) especially for this.

Our **managed threat-monitoring service** combs through data and alerts to accurately identify intrusions and malicious activities that try to fly below the radar.

Benefit from the deep expertise of an **elite team of security experts** from Bitdefender and get **24/7 monitoring** of your environment.

Offload security management

For more information on how Bitdefender can protect your healthcare IT infrastructure, please visit bitdefender.com or contact us at www.bitdefender.com/healthcare

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/.

Bitdefender-Solution-Paper-HC-CREA2019-en_EN