Whitepaper

Bitdefender®

Security is more than just compliance for healthcare digital transformation

Contents

Healthcare and security share many principles and similar challenges .From prevention to analyzing a negative event in context ,they align on a common mission :to keep people safe and support them in the long run.

In this whitepaper ,we review how technology is changing workflows and expectations in healthcare at an unprecedented pace .We also look at why healthcare organizations are a prime target for cybercriminals and how the cybercrime economy swells with each new massive data breach.

By examining trends ,challenges ,and solutions ,IT and security leaders can single out opportunities for improvement in their own circumstances .Building towards a stronger setup that combines both compliance and advanced security tactics ,decision-makers can play a pivotal role in the future of healthcare.

There is no debate over the essential role of healthcare security in our current societies and - quite literally - in our lives .The heavy industry regulations impose it and the hugely diverse ecosystems require it.

Healthcare is getting better because medical professionals use a wide range of physical equipment to treat more people more effectively.

As a natural consequence ,security must also keep up to protect these devices across multiple networks .What's more ,operating with sensitive patient data - shared across infrastructures and stakeholders - increases the responsibility security leaders have.

It's precisely this combination of diverse infrastructure and highly valuable medical data that makes the healthcare industry **a preferred target** for cyberattacks.

Almost a third of data breaches (27%[1]) occur in healthcare . This is the largest volume compared to all surveyed industries ,making medical data the most exposed kind of all.

Increasingly diverse attack vectors enable threat actors to constantly probe for and exploit various security loopholes .So does **healthcare digitization**.

Nearly every hospital in the US has made the switch from paper-based systems with **96%[2] of critical care hospitals** and **over83% of regular hospitals**.

Consequently ,electronic health records) EHR (or electronic medical records) EMR (are more likely to face the same - if not greater -security challenges as any other digital data.

1 ENISA Threat Landscape Report 2018

2 Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2015

EHRs - a very lucrative target for cybercriminals

Reports[3] indicate that medical data sells for tens of times more than credit card information on the black market. Cybercriminals will pay up to $250 on average for a single healthcare record. That is **50 times more than credit card records**.

The reason? Social Security numbers, Personally Identifiable Information, financial data and other valuable confidential details are packed into a single patient record.

This is one of the main reasons cybercriminals have such a keen interest in EHR. It's also a source of continuous challenges for the healthcare security that must protect that information from threat actors.

In this industry, **balancing flexibility and accessibility with security is a permanent priority**.

Healthcare digital transformation has now begun to revolve around software-defined, hyperconverged, hybrid and multi-cloud infrastructures. To empower medical professionals to save and improve more lives, these infrastructures must offer:

- **data accessibility**
- **mobility**
- and **availability** while simultaneously enabling **faster doctor-to-patient data sharing** and vice versa.

Digital transformation - more agility but also more risks

Implementing hyperconverged, hybrid infrastructures comes with many benefits for IT leaders in healthcare:

- reduces the number and financial costs of physical servers
- replaces legacy hardware that requires skills and headcount to maintain
- establishes a highly abstracted and manageable infrastructures that require less personnel
- enables IT managers to deploy more effective strategies, policies, and procedures around access control and monitoring HER/EMR usage.

Embracing digital transformation is a gradual process. Throughout this operation, healthcare IT and security teams need to plan for maintaining legacy systems in conjunction with new ones, all without compromising security.

Here are some of the key things IT and security leaders in healthcare should consider.

Safe storage for EMRs

While software-defined and hyperconverged infrastructures present obvious improvements in costs and agility, they may also create **compliance challenges**. Many of these issues revolve around **the storage of patient data** in the public or private cloud.

The constantly expanding attack surface

Digital transformation puts to rest old security challenges but surfaces new ones. The main concern is that **traditional security solutions are not designed to act as an enabler** for these highly abstracted infrastructures.

3 The Value of Data report

From cloud storage to BYOD to medical trackers and other connected devices, the attack surface expands steadily. To safely deploy and operate the new setup requires a change in the approach towards security.

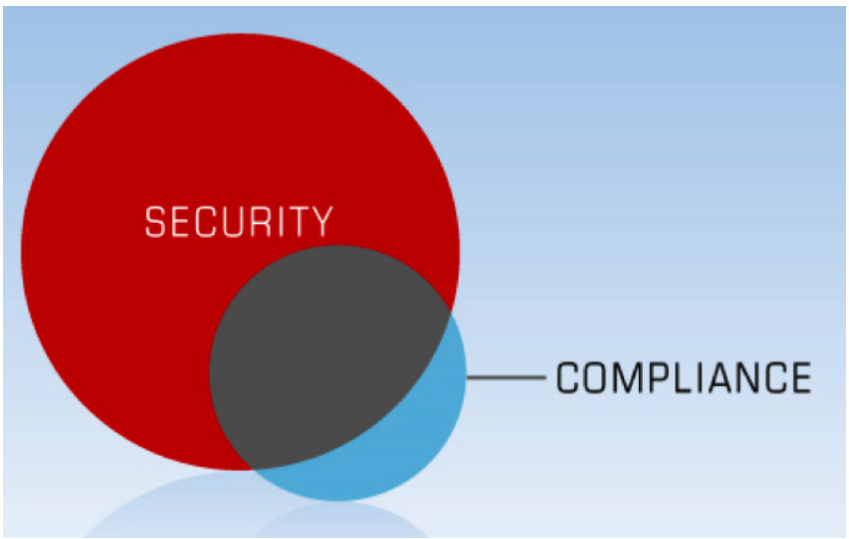
A richer threat context and more visibility

Healthcare organizations should also factor in **deploying additional security layers** that can protect from zero-day vulnerabilities and sophisticated attacks. This is especially important if those security layers are tightly integrated with bare-metal technologies such as hypervisors.

Memory introspection solutions are the perfect example of such technologies, as they can **identify memory manipulation** techniques associated with zero-day vulnerabilities. This enables them to effectively stop threat actors during the first stage of attack.

Both the volume and the diversity that define attacks against healthcare organizations make multi-layered security imperative.

Almost every surveyed **healthcare organization (83%[4]) confirmed an increase in cyberattacks** over the last 12 months. What's more, **45%** of these organizations mentioned they came across **attacks focused on data destruction** over the same period of time.



Business trends in healthcare

Three key transformations are changing the way healthcare organizations operate on every level. They all have in common on key concern for IT and security leaders: protecting patient data.

BYOD becomes inevitable

Medical staff will often bring their own devices, such as smartphones or laptops, to the hospital. This happens either because hospital hardware may not allow for portability or because personal hardware is more performance-driven that currently deployed devices.

This poses both privacy and security challenges:

- **privacy**: doctors could use personal devices to store and transfer confidential patient data
- **security**: IT needs to manage BYOD to avoid potential breaches caused by their compromise.

Strictly from a financial perspective, allowing BYOD on premise does save on costs associated with equipment acquisition or upgrades. The downside is that it places more strain on IT and security teams that may already be overburdened and understaffed.

4 Hackers are stealing personal medical data to impersonate your doctor

More connected equipment leads to new workflows

The need to provide new online and digital services to clinicians and patients has led to the increased adoption of medical equipment and the digitization of healthcare medical records.

The use of PACS (picture archiving and communication systems) for storing and accessing images from multiple machine types eliminates the need for traditionally handling film jackets.

Medical devices that perform X-ray scans, computed tomography (CT), or even magnetic resonance imaging (EMR) now enable timely delivery and efficient access to images and patient data for any medical practitioner. They effectively eliminate the physical barriers associated with traditional film-based distribution, enabling healthcare professionals to diagnose and treat more patients.

The use of Patient Data Management Systems is especially beneficial as it allows medical practitioners to have complete patient charting history at right at their bedside.

The use of such systems enables:

- increased mobility
- better diagnostics based full medical history
- immediate access to all clinical documentation from a single point of access.

The caveat is that **security implications of such systems are often disregarded in favor of usability**.

Both EHR and PACS systems are often deployed using a centralized production database that is tied into various types of applications servers and client software, often accessible through desktop applications or virtual desktops.

IT and security leaders know that enabling medical practitioners to access patient data from any device or location involves an underlying infrastructure that is often a complex bundle of servers, storage area networks, and operating systems. **This setup makes it challenging not just to deploy and manage it, but also to secure it.**

The sum total of these backend infrastructures that are necessary to enable performance, scalability, and mobility for PACS and HER systems raise unique security challenges. These issues can only be addressed by technologies that are not just **operating system agnostic**, but also **optimized and fine-tuned for any type of environment** (physical or virtual).

Unusual devices that require non-traditional security

The rise of IoT (internet-of-things) and related applications in medical devices adds extra security pressure. Most of these smart devices used for monitoring patient data are not governed by the same strict security policies.

The convergence of IoT with healthcare adds a new "physical" element to security concerns, as implantable medical devices (IMD) - such as internet-connected pacemakers and insulin pumps - may have security vulnerabilities that put patient lives at serious risk.

The FDA has issued several warnings[5] regarding vulnerabilities found in IMDs, the latest involving around 465,000 pacemakers manufactured by Abbott, known to be vulnerable to hackers.

While there have been no in-the-wild attacks on such devices, **fixing known security vulnerabilities and updating them is a cumbersome process**, forcing patients to visit their doctors for the updates.

In light of these trends, hospitals need to rethink their security strategies for both digital patient data stored in the cloud as well as for their infrastructure when exposed to new devices that may have access to EHRs/EMRs.

Healthcare IT trends

One can look at healthcare security from a multitude of angles. No matter the stance, it's importance for our society is undeniable. Healthcare is so deeply embedded into the fabric of our lives that keeping these systems safe is not optional.

Just as people with chronic disease or emergencies cannot postpone a doctor's visit, so technology leaders must act on their responsibility to ensure attackers are prevented from putting these systems out of order.

This walkthrough of the biggest trends in healthcare technology provides a comprehensive overview of the most important factors to monitor in a security program.

Reconciling hyperconvergence with legacy systems

The adoption of hyper convergence is said to bring cloud-like scalability to enterprise data centers at around 22% of the cost, according to a recent study by IDC[6].

Rapidly embracing virtualization and the SDDC technologies are transforming the healthcare industry by ripping out physical desktops and replacing them with virtualized desktops and applications.

Accessibility is the main driver for datacenter modernization, as it increases user productivity while keeping IT infrastructure costs down.

While there are many moving parts to making the transition, organizations can break down challenges to focus on modernizing IT infrastructure while automating service delivery. The result is a deep transformation of their IT operations.

The goal is to be able to look at the infrastructure as a single system that can be managed holistically, an objective that can be achieved through **hyperconvergence.**

5 FDA Recalls 465,000 Pacemakers Due to Cyber Security Concerns

6 The Business Value of Modernizing Infrastructure with Hyper-Converged Systems

Multifaceted compliance and the risk of high-profile breaches

HIPAA[7] (Health Insurance Portability and Accountability Act) is probably one of the best-known pieces of legislation for safeguarding medical information and ensuring data privacy. Since it took effect in 1996, it has changed the way the healthcare industry addresses the privacy and security of EHRs/EMRs from a technology perspective.

The two major components of HIPAA – the HIPAA Privacy Rule and the HIPAA Security Rule – are designed to enforce a series of standards around disclosing patient data, particularly in terms of:

- how that information flows between healthcare providers and hospitals
- how that information is stored and transported between parties.

In essence, while the HIPAA Privacy Rule addresses confidentiality, the HIPAA Security Rule addresses the technical and non-technical safeguards for protecting the integrity of medical data from unauthorized access or tampering.

Organizations that fail to comply with HIPAA may face criminal prosecution and fines estimated at around **$50,000 per violation**.

While adherence to HIPAA is mandatory, other healthcare rules and regulations have been drafted to help critical infrastructures maximize their cybersecurity resilience against cyberattacks.

Marked as optional, the FDA and NIST (National Institute of Standards and Technology) have drafted under The Internet of Medical Things Resilience Partnership Act[8] (2017) a series of security best practices to which any organization, including those in the healthcare sector, can use as guidance.

Besides data security best practices and recommendations, the NIST Framework for Improving Critical Infrastructure Cybersecurity[9] also includes technical security solutions aimed at securing both physical and virtual environments, as well as methods for detecting anomalous behavior and events at the network and endpoint level.

Basically, instead of focusing just on reactive security controls, these regulations focus on:

- **proactively establishing a baseline** of network operations and expected data flows
- **aggregating/correlating events from multiple sources** in order to detect potential cybersecurity events, malware, or unauthorized access
- **creating a response plan** that mitigates potential security breaches as timely as possible.

The proposed cybersecurity mantra focuses on **a continuous cycle of identifying, protecting, detecting, responding, and recovering from potential cybersecurity incidents**. The key objective is to constantly improve the overall security posture of the organization.

The Health Information Technology for Economic and Clinical Health[10] (HITECH) Act is also one of the toughest healthcare security standards that US healthcare organizations have to abide by when it comes to **privacy and disclosing medical data**.

However, the recent GDPR[11] regulation is much tougher than HIPAA or any previous US legislation, as it broadens the definition of personal data to include anything that's considered identifiable information that can lead to singling out individuals.

More than that, GDPR also places strain on healthcare organizations as they now have to set up mechanisms through which patient data can be irrevocably deleted, if the patient should chose to exercise his **right to be forgotten**[12]. This is something that's never been implemented in US healthcare as medical data is usually stored indefinitely.

Two other important aspects that GDPR requires are the need for **encryption** and the obligation to **inform patients of a data breach within 72 hours** of discovery, unlike the 60-days timeline enforced by HIPAA.

7 HIPAA for Professionals

8 Internet of Medical Things Resilience Partnership Act Bill Introduced

9 Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

10 HITECH Act Enforcement Interim Final Rule

11 The EU General Data Protection Regulation (GDPR)

12 Everything you need to know about the "Right to be forgotten"

However, while regulations are easily expressed in draft form, the technical challenges of actually implementing them cause grievances for IT and security teams.

Strengthening security on a (stagnating security) budget

The biggest issues revolve around security budgets which, in healthcare, are below the industry standard. According to Forester[13], US industries spend an average of **10 percent** of their IT budget on security while **healthcare only dedicates 6% or less[14] of their funds on average** to the same.

A large number of surveyed healthcare organisations plan to spend more on cybersecurity over the next 12 months - about **66%[15]** of them. Unfortunately, the increase doesn't match the necessities.

While expected to increase slightly over the next 12 months - by **roughly 5%** - healthcare security budgets continue to stagnate.

A large chunk of those budgets will be spent on upgrading security technologies, and on securing cloud instances and services.

The changing nature of IT threats that are both internal and external as well as the increasing complexity of IT environments place healthcare security decision-makers in a difficult position. They must secure their infrastructure against an ever-increasing attack surface while relatively maintaining the same security budgets.

Security technologies that **leverage the hypervisor to perform memory introspection** on virtual workloads present an added benefit. That is because they allow IT and security admins to defend against advanced and sophisticated threats that leverage unpatched or unknown vulnerabilities to plant malware.

An added benefit of hypervisor introspection technologies is that they are **completely compatible with existing security solutions**, while at the same time fully integrating with software-defined and hyperconverged infrastructures.

These technologies may prove to be viable solutions for the CISO who has to make the most of his security budget while meeting compliance prerequisites and fighting off increasingly persistent attacks.

13 Are You Spending Enough on Cybersecurity?

14 2018 Healthcare Information and Management Systems Society Cybersecurity Survey

15 EY Global Information Security Survey 2018-2019

The deepening cybersecurity talent gap

Tackling these multifaceted challenges requires capable specialists who can leverage technology to advance healthcare security.

Disruptive cloud technologies, mobile, and analytics have huge potential for improving healthcare. In the trenches, it's decision-makers who have the difficult task of carefully calculating the risks associated with integrating all of these in their current infrastructure.

BYOD and remote working, coupled with the need to maintain legacy systems in conjunction with new ones, **overburden an already understaffed IT department**.

Consequently, the consensus is to focus on mandatory compliance first, then move to optional security practices.

Although IT and security leaders are eager to try and adopt new technologies, the lack of trained personnel and staff is yet another obstacle that hinders them.

Substantially more diverse attack vectors

Internal actors are considered one of the biggest threats to the healthcare vertical, as most incidents involve error and misuse, according to a 2019 Verizon Data Breach Investigation Report[16].

With **60% of security incidents caused by internal threat actors** and **83% of actor motives being financially fueled,** the healthcare industry faces another big problem: medical practitioners mishandling data.

Aside from malicious or careless insiders, there is a range of attack vectors that healthcare CISOs could benefit from monitoring.

Healthcare is one of the few sectors where **ransomware** continues to be a growing threat. In fact, ransomware incidents plaguing healthcare account for **85% of all malware**[17] that's been targeting the industry.

The high number of reports could be based on the fact that HIPAA requests ransomware incidents to be treated as data breaches.

In fact, security reports agree that ransomware seems to be targeting individuals and end users less frequently. Instead, cybercriminals are focusing on organizations as they are the ones most likely to give into their demands because of the risks posed by potential downtime issues. For healthcare organizations, the recovery process can even endanger patients' lives, which makes them a more appealing target for ruthless cybercriminals.

One of the most common attack vectors for healthcare remains **phishing**, accounting for "59% of significant security incidents across all organizations, and 69% of incidents at hospitals," according to the 2019 HIMSS Cybersecurity Survey . Alongside it, the **theft of assets,** such as tablets, phones, and laptops containing patient or healthcare date, is also considered a major contributing factor to security issues.

Recently, malicious hackers have started to take a closer interest in **third-party service providers for healthcare organizations**.

For example, the debt-collection firm American Medical Collection Agency (AMCA) announced its customers that their data had been illegally accessed between August 1, 2018 and March 1, 2019.

This led to LabCorp and Quest Diagnostics - two of AMCA's clients - to notify relevant US authorities that their patients' EMRs had been leaked as a consequence. Both healthcare organizations unwittingly exposed 11.9 million[18] EHRs because of this third-party provider breach.

The compromised information included customer names, their dates of birth, addresses, phone numbers, balance information, and even payment-account details, if the patient had tried to pay their outstanding medical bills.

16 Verizon 2019 Data Breach Investigations Report

17 ENISA Threat Landscape Report 2018

18 Healthcare Breach Expands to 19.6 Million Patient Accounts

Needless to say that this is the golden treasure attackers seek to get their hands on.

Data breaches and their long-term ripple effects

The past couple of years have been riddled with data breaches impacting the healthcare industry. These compromises ended up leaking hundreds of millions of healthcare records, potentially exposing users to fraud, phishing and other types of threats indefinitely.

In fact, **955**[19] **major security breaches** have occurred in the past three years alone, resulting in **135,060,443 compromised records** and more than **41%** of the US population having their medical data exposed.

By far, one of the largest data breaches involving the exposure of personal information is the Anthem data breach[20], which affected **78.8 million** people. The stolen information ranged from names, birthdays, and medical IDs to social security numbers, email addresses, and physical addresses. Details following the investigation have revealed that the breach occurred due to a phishing email with an infected attachment, allowing the attacker(s) to move laterally across the infrastructure and compromise at least 90 systems, including the organization's database.

The Premera Blue Cross data breach in 2015 that spilled **11 million patients' healthcare records** onto the web is considered the second-largest healthcare data breach, according to the U.S. Department of Health and Human Services Office for Civil Rights[21]. Everything from clinical information to bank account numbers, social security numbers, birthdates, and other personal information was reportedly accessed and stolen by threat actors.

19 Security Breaches in Healthcare in the Last Three Years

20 Anthem medical data breach

21 U.S. Department of Health and Human Services Office for Civil Rights - Breach Portal

The third most notorious data breach involved the leak of personal medical data belonging to more than **10 million** patients that was managed by Excellus BlueCross BlueShield. While **the financial losses were estimated at around $17.3 million**, experts say the final losses may be as high as $3.6 billion[22], as some studies have estimated costs per record at $363.

All this sensitive personal information has led to a surge in development for the cybercrime economy. Not only do malicious actors engage in transacting this highly valuable data, but they also use it to execute subsequent attacks that range from identity theft to extortion.

The negative long term effects are undeniable, impossible to estimate in terms of financial impact and, sometimes, permanent.

The importance of seeing it all, with clarity and detail

One of the major security pain points in healthcare security is **the lack of visibility across infrastructures and endpoints**.

Whether the assets are physical, virtual, private or in the cloud, IT and security teams need to understand how everything connects, where they're located, and how to manage them.

Having **complete, single-pane-of-glass visibility** across infrastructures not only allows **consistent policy enforcement** but also helps with **early identification, containment, and remediation** of potential security incidents.

Having a capable security solution that can secure physical endpoints and mobile devices is mandatory. It's also imperative for it to **scale using a virtual container architecture** and be **compatible with any virtualization platform**.

IT and security leaders know that the performance of virtual workloads must not be negatively affected by the in-guest security solution. Otherwise, it will defeat the performance and scalability benefits offered by virtualization.

EDR (Endpoint Detection and Remediation) tied together with a strong **EPP** (Endpoint Protection Platform) solution can offer **contextual awareness** into the security posture of the organization and also give IT and security admins **greater visibility into security incidents** that might escalate into full-blown data breaches.

Since healthcare organizations have understaffed and overworked IT and security departments, alert fatigue caused by traditional EDR solutions may become aggravating. The ideal EDR solution needs to discern which alerts are critical and worth investigating and which not to enable **strategic security decision-making**.

In light of recent healthcare data breaches that stemmed from advanced and sophisticated attack techniques, digitized healthcare organizations should also consider adopting new **security layers designed to protect virtual workloads** from zero-day vulnerabilities and potentially state-sponsored actors.

Security technologies designed to work with the hypervisor to offer complete visibility into advanced threats targeting virtual workloads considerably reduce the risk of potential data breaches.

BYOD should not be neglected either, especially since medical staff needs portable access to patient data and health history. Controlling and managing smartphones and tablets that have access to sensitive business information is both mandatory, according to healthcare regulation, and a good security practice.

Financial costs are also a main constraint when IT and security teams plan on deploying new security technologies for security data centers.

Balancing security budgets with adequate security controls should involve carefully walking senior managers and boardroom members through the security and financial implications of a potential security breach.

A security strategy that's based on risk assessment and carefully identifying the best technologies for securing critical data should help board members understand the value of security and its priority for business growth.

22 Cost of the Excellus BlueCross BlueShield Data Breach Reaches $17.3M

Building security around compliance

While healthcare organizations may be more interested – at first – in building compliance, getting certifications, and taking the minimum steps necessary for ensuring business operations, building security operations around compliance should be more than just good practice.

In the long run, a robust security setup saves costs, reduces risk, and provides support for business continuity and growth in an industry that is critical for our societies.

Integrating security solutions that offer layered and adaptive security for any type of environment – including compliance with healthcare regulations – should be assessed for their **protection, performance, and manageability**.

Compliance may cover the fundamentals, but **centralized visibility** across all managed devices and the entire infrastructure helps healthcare organizations save more money by avoiding financial fallout caused by an undetected data breach.

The financial costs associated with investing in beefing up compliance with additional security technologies may pale in comparison to fines and lawsuits resulting from undiscovered compromises.

Given the importance and value of EHRs/EMRs, healthcare providers and organizations should look to solutions that help with:

- compliance in virtualization and cloud environments
- streamlining security operations
- eliminating point solutions.

Layered next-generation security is mandatory in protecting healthcare infrastructures against breaches and advanced threats. However, healthcare digitization should consider looking towards solutions that offer **best-in-class security with minimum performance impact** and low management overhead.

These objectives are both attainable and accessible for IT and security leaders. These challenges can be overcome through collaboration and finding the right partners to share experience and information with.

Securing healthcare data and organizations is a cross-industry effort we are all invested in.

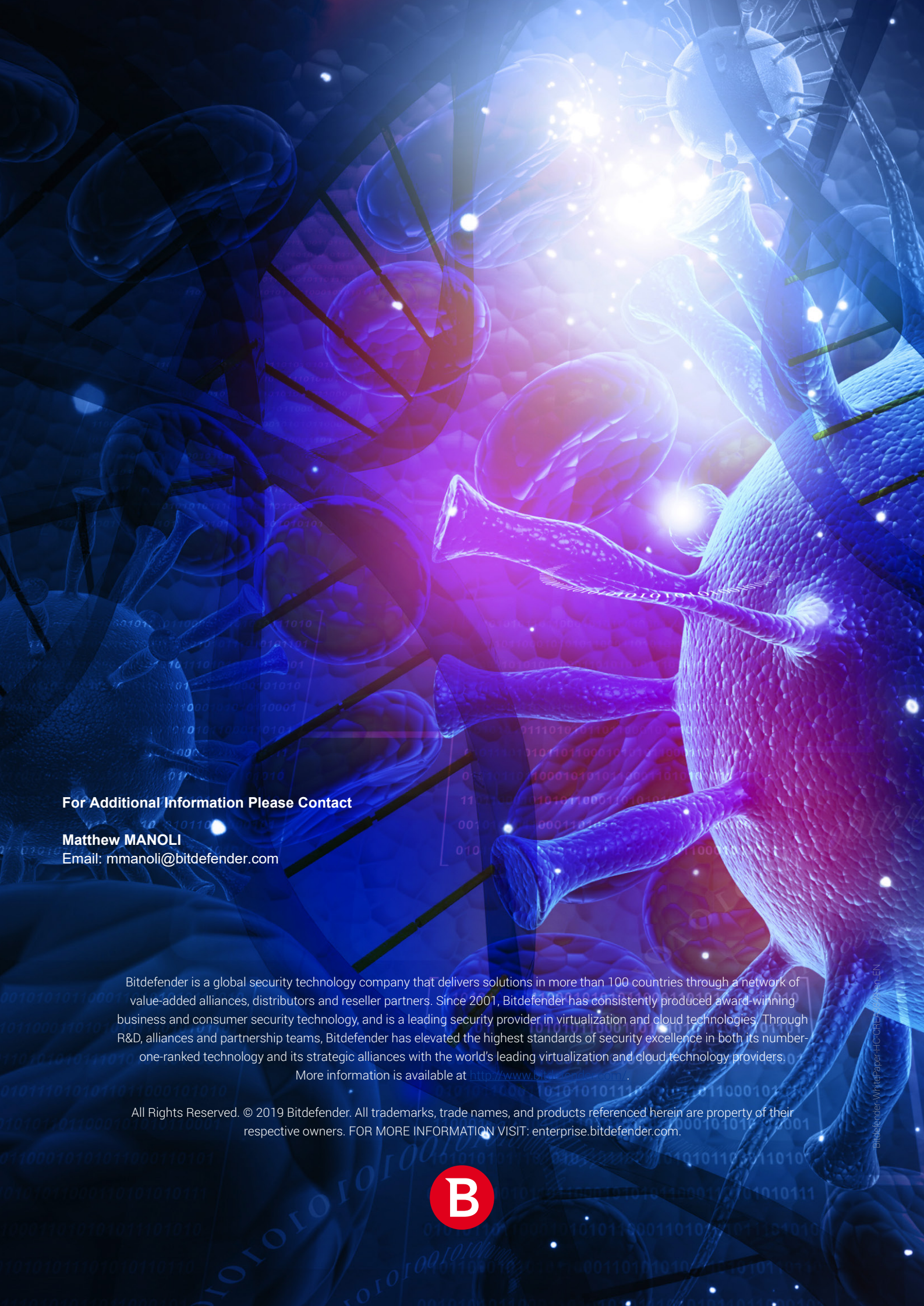
This whitepaper is brought to you by Bitdefender®, the creator of:

- **Bitdefender GravityZone™ Ultra Security,** the world's most effective endpoint security suite that integrates 30 layers of protection. Its low overhead Endpoint Detection and Response (EDR) and Endpoint Risk Analytics (ERA) are built into a single agent with a unified console architecture. GravityZone™ Ultra Security enables IT and security leaders to protect the wide range of devices used by medical personnel across the organization.

- **Bitdefender GravityZone™ Network Traffic Security Analytics (NTSA),** a plug-and-play, out-of-band solution that comes with flexible deployment options. NTSA accurately detects the most sophisticated malware and Advanced Persistent Threats (APTs) with high accuracy. GravityZone™ NTSA's real-time breach detection and automated triage ensures IoMT and expensive specialized medical devices run safely and productively to ensure optimal patient care.

- **Bitdefender GravityZone™ Security for Virtualized Environments (SVE),** the next-generation data center and cloud workload security platform that delivers award-winning protection, while promoting the operational efficiency and performance. GravityZone™ SVE enables deep integration with software-defined (SDDC), hyperconverged, and cloud infrastructures. This enables healthcare organizations to transition to the cloud safely, maintaining a constant level of protection throughout the entire process.

› This page was left blank intentionally



For Additional Information Please Contact

Matthew MANOLI
Email: mmanoli@bitdefender.com

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/.