White Paper

Bitdefender®

Threat Intelligence: Shrinking the Cybersecurity Data Gap

Prepare, React, Resolve and Learn

Contents

Executive Summary

Cybercrime is on the rise with more devastating consequences than ever. For example, a Ponemon Institute and IBM study reported the average cost of a data breach continues to grow year after year, reaching $3.92 billion in 2019. At the same time, security teams are struggling to keep up with evolving threats and an abundance of false positives. Lack of automated security processes combined with a shortage of security professionals trained in the latest cybersecurity technologies further stretch resources.

To overcome these challenges, some of today's most successful enterprises are embracing threat intelligence services to gain insight on how adversaries operate, the tools and techniques they use or understand better the threat landscape that surrounds their organizations. Not only do threat intelligence offerings dramatically reduce false positives, but they increase efficiency by triaging and prioritizing security alerts. The result is quicker and more accurate detection of potential or active breaches and recommendations for corrective action.

More companies worldwide are taking note and adopting threat intelligence. According to Mordor Intelligence, the threat intelligence market will grow from $4.49 billion in 2018 to $11.83 billion by 2024 with a compound annual growth rate of 17.5%.

At Bitdefender, the #1 ranked provider of advanced cybersecurity solutions, our threat intelligence offering, Bitdefender Advanced Intelligence (ATI), is critical to supplementing existing security systems with actionable, real-time threat-hunting insights. Bitdefender ATI benefits from our nearly 20 years of experience in developing award-winning, innovative cybersecurity solutions and networks and collaborating with governments and law enforcement agencies on solving cyber-attacks worldwide. Bitdefender's threat intelligence differentiators include top-quality data sources, easy-to-consume formats, and streamlined integration with existing security systems, among other capabilities.

In this white paper, we explain the growing importance of threat intelligence, Bitdefender's approach to threat intelligence with Bitdefender ATI, as well as the roadmap for threat intelligence advancements.

Threat Intelligence: The Missing Link

Data. It permeates almost every aspect of our online lives—whether we're shopping, navigating directions, looking for a job, checking in for a flight and so much more. With each click, we accomplish tasks and get closer to our goals, but we're also putting data at risk for capture by cybersecurity thieves.

Challenges for today's enterprises, especially medium-sized and large enterprises and managed security service providers (MSSPs) are intensifying as cybersecurity thieves up their game with more sophisticated attacks. Advanced persistent threats (APTs), phishing and ransomware attacks can cost enterprises millions of dollars from revenue losses, brand damage, compromised intellectual property and regulatory fines. A Ponemon Institute and IBM study reported the average cost of a data breach continues to grow year after year, reaching $3.92 billion in 2019. The study also revealed mean time to identify a breach was, on average, 197 days.

Meanwhile, security operations centers (SOCs) struggle to stay ahead of fast-changing threats with stretched resources. False positive alerts overwhelm security teams, increasing the risk of missing true positives and forcing a reactive approach. Further, many security operations and processes are not fully automated or integrated. There also is a shortage of security professionals skilled in next-generation cybersecurity solutions, such as endpoint detection and response (EDR) and network traffic analytics.

To address these challenges, today's high-performing companies are embracing threat intelligence for an array of use cases, such as security data augmentation, phishing investigations, incident response, vulnerability management or detailed malware analysis. With threat intelligence, security teams can improve security defenses of their enterprises by triaging and prioritizing alerts while increasing efficiency and productivity. Often integrated with security information event management (SIEM) or EDR solutions, threat intelligence correlates data gathered from inside the enterprise with indicators about external threats. By narrowing threats marked for investigation, threat intelligence can identify more quickly and accurately the risk of a breach or one that is penetrating your infrastructure.

> **"Today's security teams are overwhelmed with massive amounts of data which leads to a side-effect of an exponential increase of false positives. By connecting dots between activity in your enterprise and relevant external threats, threat intelligence narrows and triages areas for investigation. That way, security teams can prepare, react and learn more quickly and effectively."**
>
> **Sorin Dudea**
>
> **Vice President, Cyber-Threat Intelligence Labs**
>
> **Bitdefender**

It's no surprise that enterprise adoption of threat intelligence is mounting. According to Mordor Intelligence, the threat intelligence market will grow from $4.49 billion to $11.83 billion by 2024 with a compound annual growth rate of 17.5%. One of way of observing this trend is by analyzing reported software vulnerabilities. According to Bitdefender's annual Global Mid-Year Threat Landscape Report, reported vulnerabilities have increased for the third year in a row. (Figure 1). A vulnerability describes a weakness, such as a flaw in software code or hardware design, that increases the risk of an attack and compromised information.

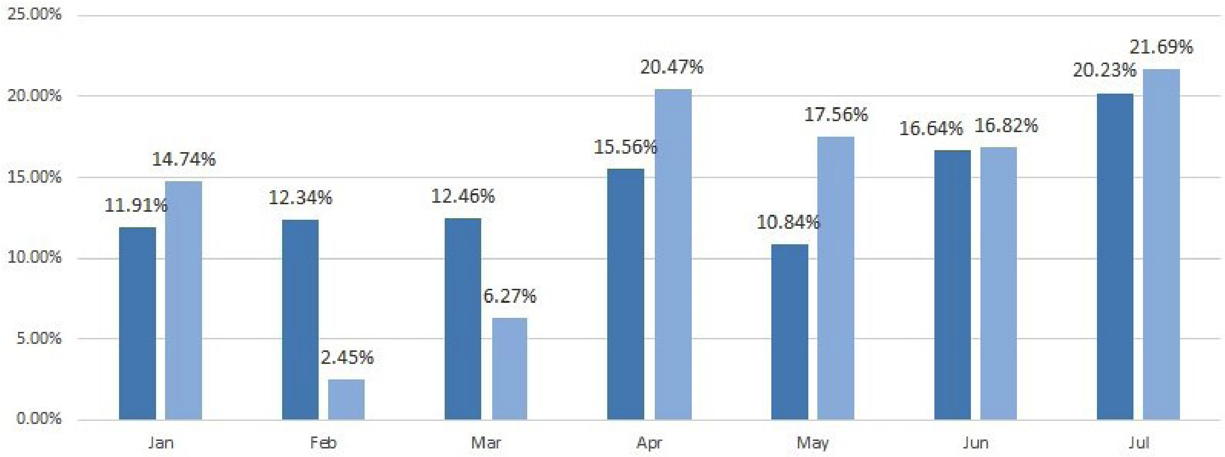


Figure 1. Reported software vulnerabilities in 2018 and 2019

Bitdefender, the #1 ranked provider of advanced cybersecurity solutions, recognizes that threat intelligence is critical to supplementing existing security systems with actionable, real-time threat-hunting insights. With high quality data sources and easy-to-consume formats, Bitdefender ATI helps security teams reduce the burden of false positives while narrowing their targets for investigation and corrective action.

Threat Intelligence Defined

Today's cybercriminals continue to find innovative ways to circumvent the most advanced security solutions. They use sophisticated programs to exploit vulnerabilities in security software or operating systems and extricate data from key systems and access directories with credentials to capture even more data. The scariest part: these exploits can remain undetected for months or even years as private, proprietary data is stealthily captured.

EDR, SIEM and other advanced cybersecurity solutions advise about potentially high-risk activity in your enterprise, but security teams must analyze and correlate vast volumes of ever-changing data and alerts. Threat intelligence connects the dots between weak spots in your enterprise and fast-moving threats sweeping the globe by providing evidence-based context, mechanisms, indicators and other relevant data. This information helps security teams make more informed decisions.
With increased visibility enabled by threat intelligence feeds, enterprises are fortifying their security defenses and refining their forensics and threat-hunting capabilities. Ultimately, they can transform their security posture from reactive to proactive, while spotting and responding to threats sooner and with less internal resources.

Why Threat Intelligence?

- Gain a proactive approach to security
- Increase visibility into latest threats
- React to attacks and expose undetected threats faster
- Reduce false positives
- Automate SOC processes for increased efficiency
- Decrease time chasing false positives

Bitdefender Advanced Threat Intelligence

Strategic Threat-Hunting Insights Protect Your Assets

At Bitdefender, we’ve spent nearly 20 years investing in cybersecurity R&D and developing threat detection technologies and solutions that have consistently won industry awards and pushed the threshold for cybersecurity innovation. The outcome of this investment is reflected in our approach to threat intelligence through our Advanced Threat Intelligence service, which provides SOCs, MSSPs and other security firms with powerful strategic threat-hunting insights. (Figure 2)

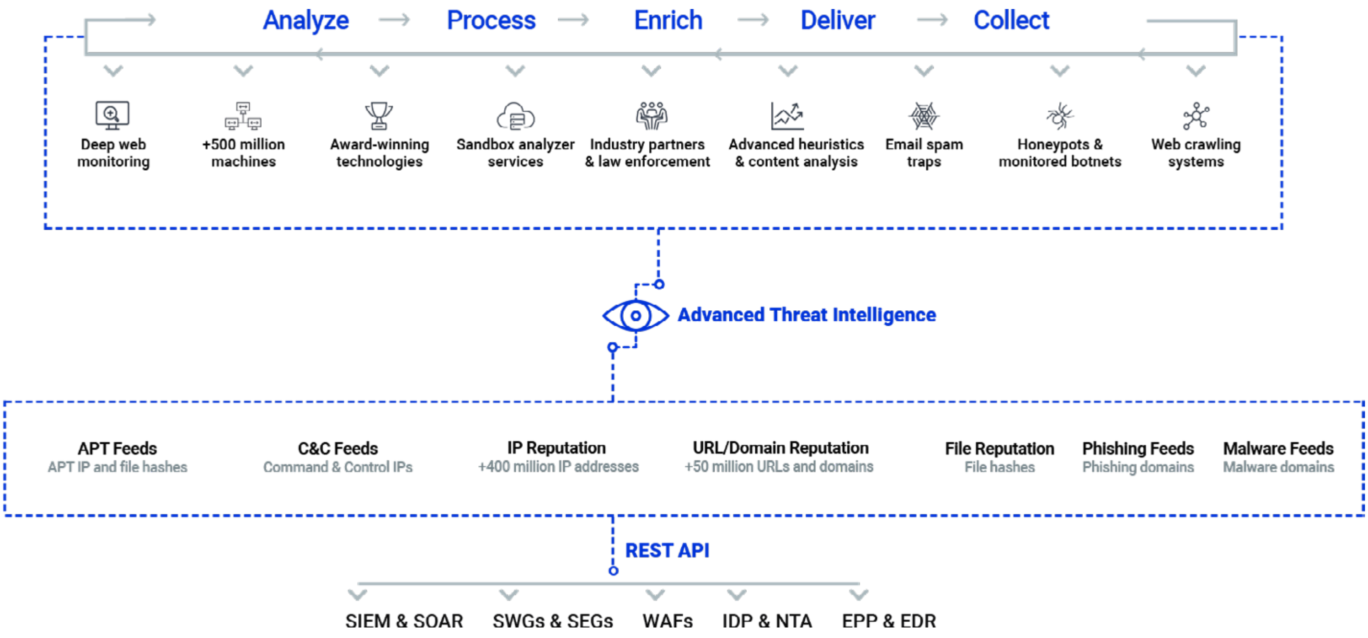


Figure 2. Bitdefender Advanced Threat Intelligence

Bitdefender ATI offers compelling advantages over other threat intelligence solutions, including

- Threat feeds with close to zero false positives and high confidence scores
- Digital forensics, human intelligence (HuMinT) and a global sensor network
- In-depth threat intelligence lab and real-world expertise
- Dark web analysis
- Well-organized, curated consumable data formats and reports
- Accurate and continuously updated indicators of compromise
- Compliance with STIX/TAXII standards
- Isolated Sandbox Analyzer infrastructure for running live threats and obtaining indicators
- Easy integration with existing security systems and tools

Actionable Threat Intelligence in Real Time

Instead of spending countless hours manually correlating open-source threat data with internal activity, SOC managers use the Bitdefender ATI offering's accurate, comprehensive data sources to proactively respond to advanced attacks pre-emptively or after they affect the enterprise. To provide actionable threat intelligence in real time, ATI continuously identifies and updates the latest IoCs, including malicious URLs, file hashes, domains, APTs and command and control (C&C) IPs, using data from Bitdefender's Global Protective Network (GPN) of 500 million installed machines. (Figure 3)

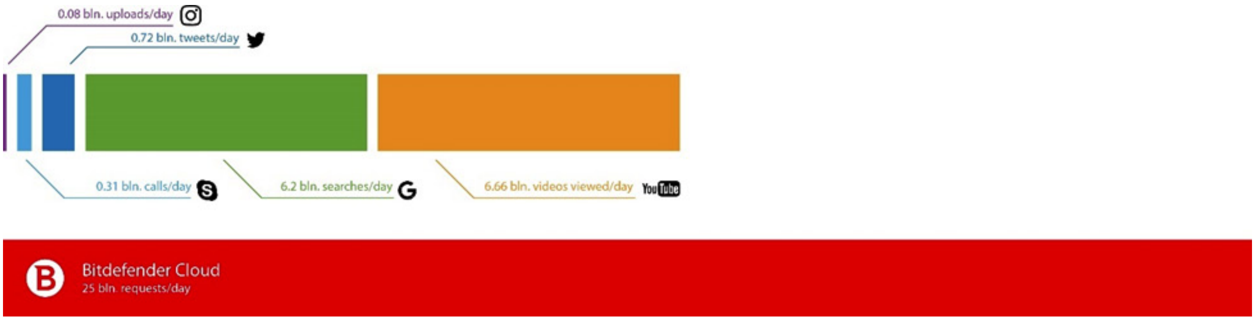


Figure 3. Bitdefender Daily Global Protective Network volume

Bitdefender GPN receives and filters 25 billion requests daily and differentiates between safe and malicious IOCs. Bitdefender GPN is one the most comprehensive, up-to-date and diverse databases of threat intelligence indicators.

Bitdefender ATI provides a powerful continuous feedback loop generated by 500 million users and sensors across Bitdefender's customer base and other security detection databases. As soon as a customer downloads a malicious URL, anonymized data with the customer's permission is relayed to the Bitdefender cloud and future customers that attempt to download the URL will be blocked.

Further, Bitdefender's ATI will tag customers attempting to download the URL by category, such as geographic location or vertical industry and correlate this data generated by a customer's SIEM or EDR system. (Figure 4) Any alert will be validated in an automated fashion with a machine learning algorithm or by Bitdefender's security experts, significantly reducing the volume of false positives.

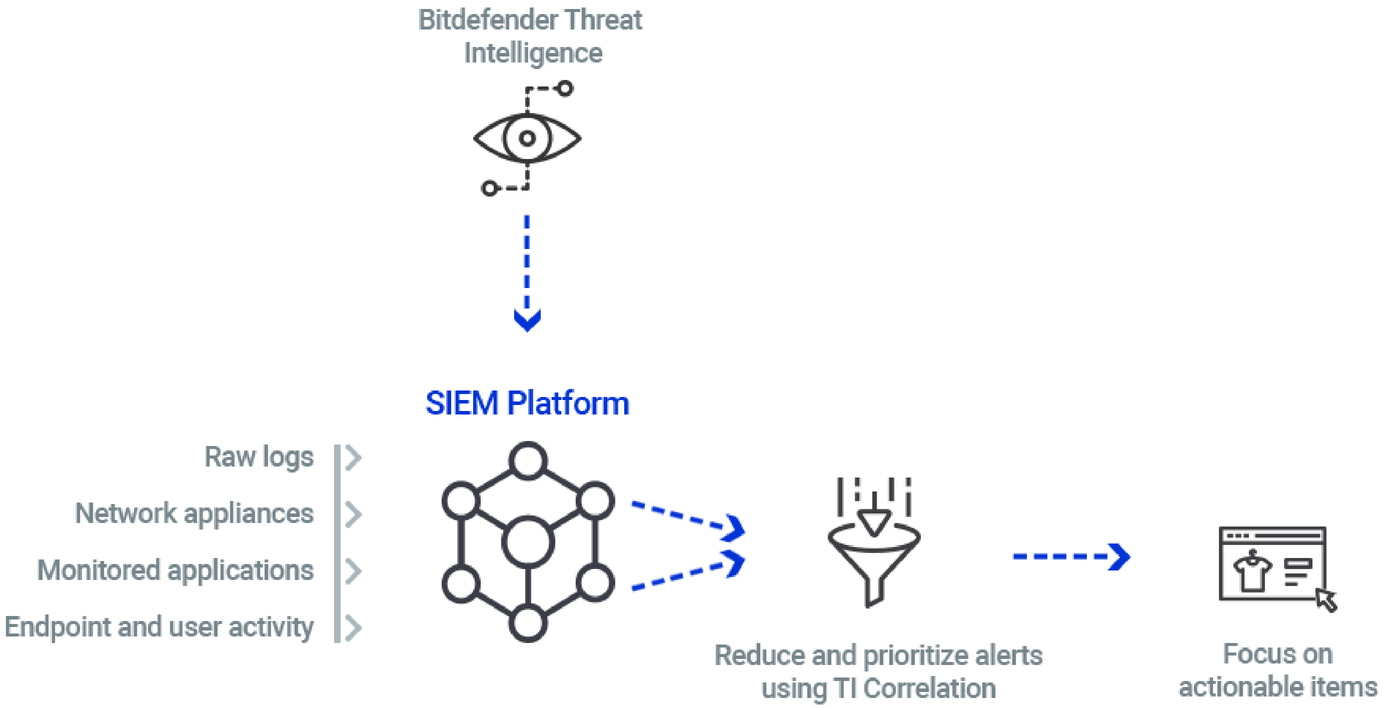

Bitdefender Threat Intelligence
SIEM Platform
Raw logs
Network appliances
Monitored applications
Endpoint and user activity
Reduce and prioritize alerts using TI Correlation
Focus on actionable items

Figure 4. Correlating advanced threat intelligence with SIEM and EDR

Solving Cybercrimes Yields High-Value Threat Intelligence

Bitdefender collaborates closely with law enforcement and government agencies to identify and crack tough-to-solve cybercrimes, such as APTs and ransomware, as well as government-sponsored attacks on other countries. Such attacks can shutter businesses for hours, days or weeks or even close them permanently. In the nation-state realm, they can weaken government infrastructures or compromise election security. Bitdefender's in-depth research into dark web threats combined with its vast sensor network have proved valuable in solving these crimes and increasing the quality of our threat intelligence offering.

For example, Carbanak group targeted APT cyberattacks in the financial industry, compromising 100 banks worldwide and stealing up to $1 billion. Following an investigation by law enforcement agencies and cybersecurity companies, Carbanak's leader was apprehended in 2018. Unlike most forensic investigations, which focus on a technical analysis of payloads, Bitdefender's research chronicled the full timeline of the Carbanak attack.

Bitdefender also worked with Europol, national cybersecurity agencies and other law enforcement agencies to counter GandCrab, file-encrypting ransomware that has resulted in hundreds of millions of dollars in losses worldwide. Bitdefender developed a free GandCrab decryption tool, which 42,000 victims used to avoid $60 million in decryption fees, as well as restore data and operations more quickly.

Law enforcement agencies regularly engage Bitdefender, due to its in-depth cybersecurity expertise and high success rate in solving cybercrimes. For these projects, Bitdefender Cyber-Threat Intelligence Labs creates an infrastructure to scan and uncover hidden services on the dark web, and then ingest, classify and analyze the data in real-time, providing valuable information for dark web investigations.

Global Reach with Vertical and Geographic Precision

Bitdefender's ATI solution offers a comprehensive, global approach to cybersecurity with 38% of the world's security solutions incorporating Bitdefender's advanced technology. With 150 technology partners worldwide, Bitdefender captures threat intelligence inside and outside of the U.S. from sources in English and numerous other languages. With 50-plus percent of revenue generated by U.S. customers, Bitdefender also has built a fast-growing customer base across Canada, Europe, Middle East, Africa, South America and Asia.

In addition, the Bitdefender ATI solution can be queried to interrogate data for a specific geography or vertical industry. For example, a bank's security team can interrogate file hashes, registry keys, emails, vulnerabilities and other IoCs in their infrastructure that are specific to the financial sector and correlate them with ATI feeds. If there is a match, the security team knows immediately to take corrective action.

Partnership and Employee Talent Drive Value

Bitdefender employing some of the world's best threat researchers and cybersecurity analysts along with its partners are essential to developing high-value threat intelligence.

For example, Bitdefender exchanges telemetry, IOCs, hashes, files and other data with security partners, security software vendors and international crime agencies, such as Europol and INTERPOL. In addition, Bitdefender exchanges a vast array of threat data feeds with other security firms.

Backed by Bitdefender technologies, 800 Bitdefender forensics researchers and engineers analyze, select and prioritize threat data from numerous feeds and sources to be included in the ATI offering. The forensics team is trained to extract accurate data by investigating attack sources, such as malicious files, as well as how threats propagate. Bitdefender also uses this intelligence to continually enhance its own sensors to detect threats faster and more accurately.

Threat Intelligence Spotlight Expands

As cybercrime episodes proliferate, Bitdefender is moving fast to enhance and broaden the array of proactive and defensive solutions to keep up with evolving cybersecurity threats.

Expanding the breadth of ATI data available to customers is another strategic focus for Bitdefender. Knowing how a malware-infected email attachment takes advantage of software vulnerabilities in specific protocols is one example of data that will help enterprises better understand how to protect themselves and respond to attacks.

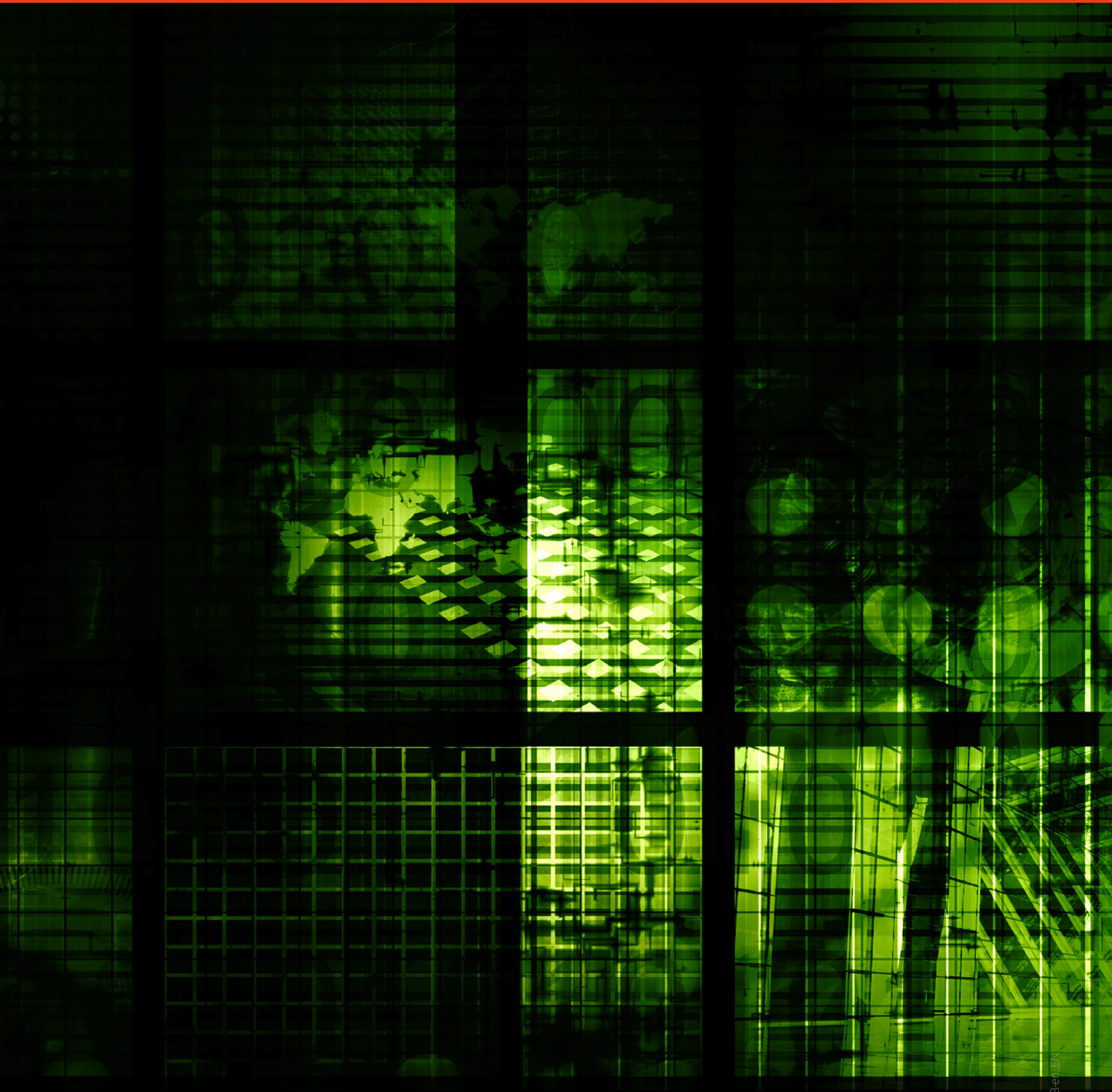
Bitdefender remains committed to increased sharing of threat intelligence across enterprises, security firms and government and law enforcement agencies. We will continue expanding the exchange of threat data specific to industry sectors, geographic regions and threat actors. Advocating that threat intelligence is captured and shared using standard, easy-to-consume formats also will be a priority.

In addition, Bitdefender views development of a unified interface to extract and analyze data, as well as conduct investigations as a long-term priority for the cybersecurity industry. This is an advancement that will enable security teams to more efficiently and effectively consume and analyze advanced threat intelligence and take corrective action with optimal results.

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.

This page is left blank intentionally

This page is left blank intentionally



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/.