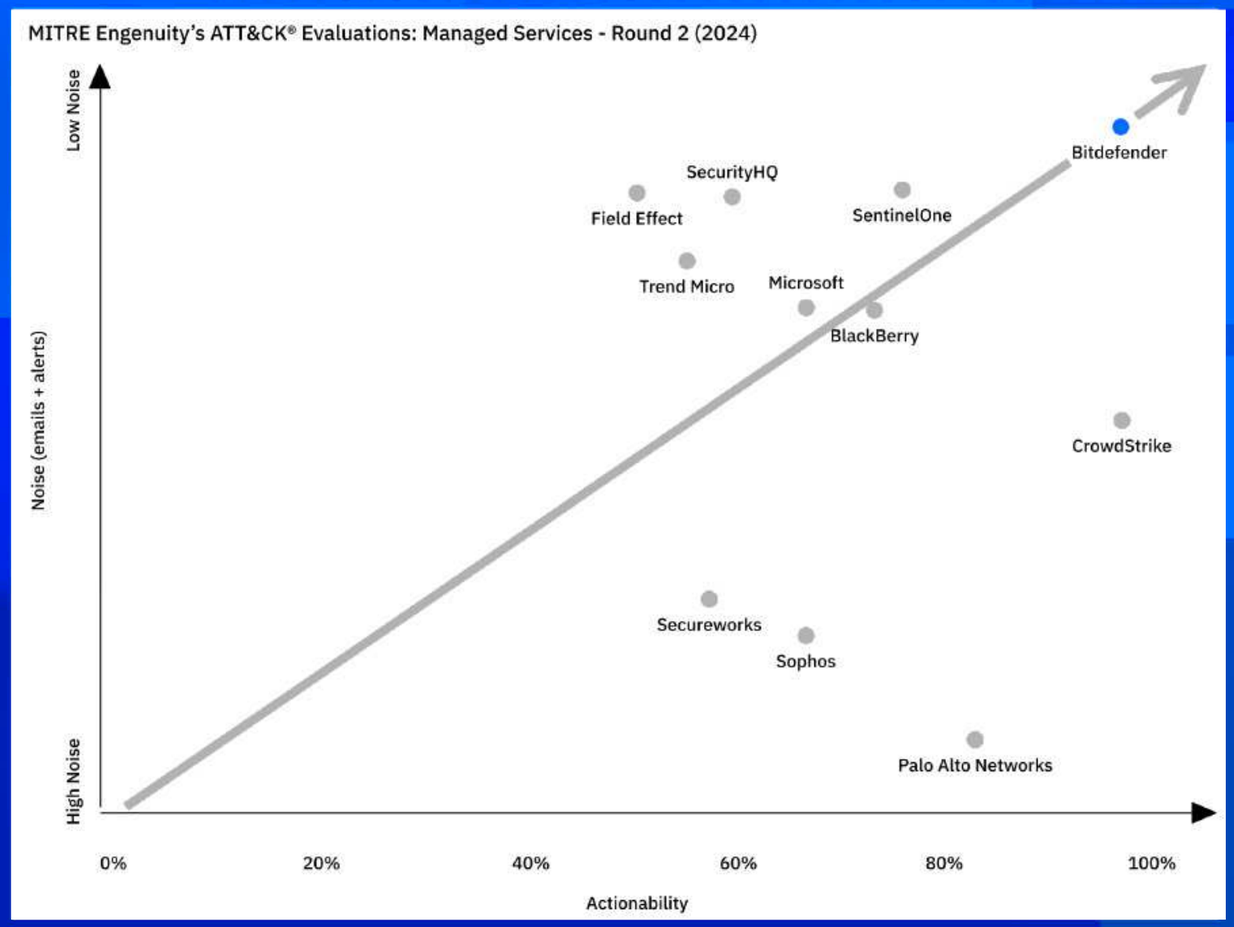
Bitdefender Global Leader In Cybersecurity

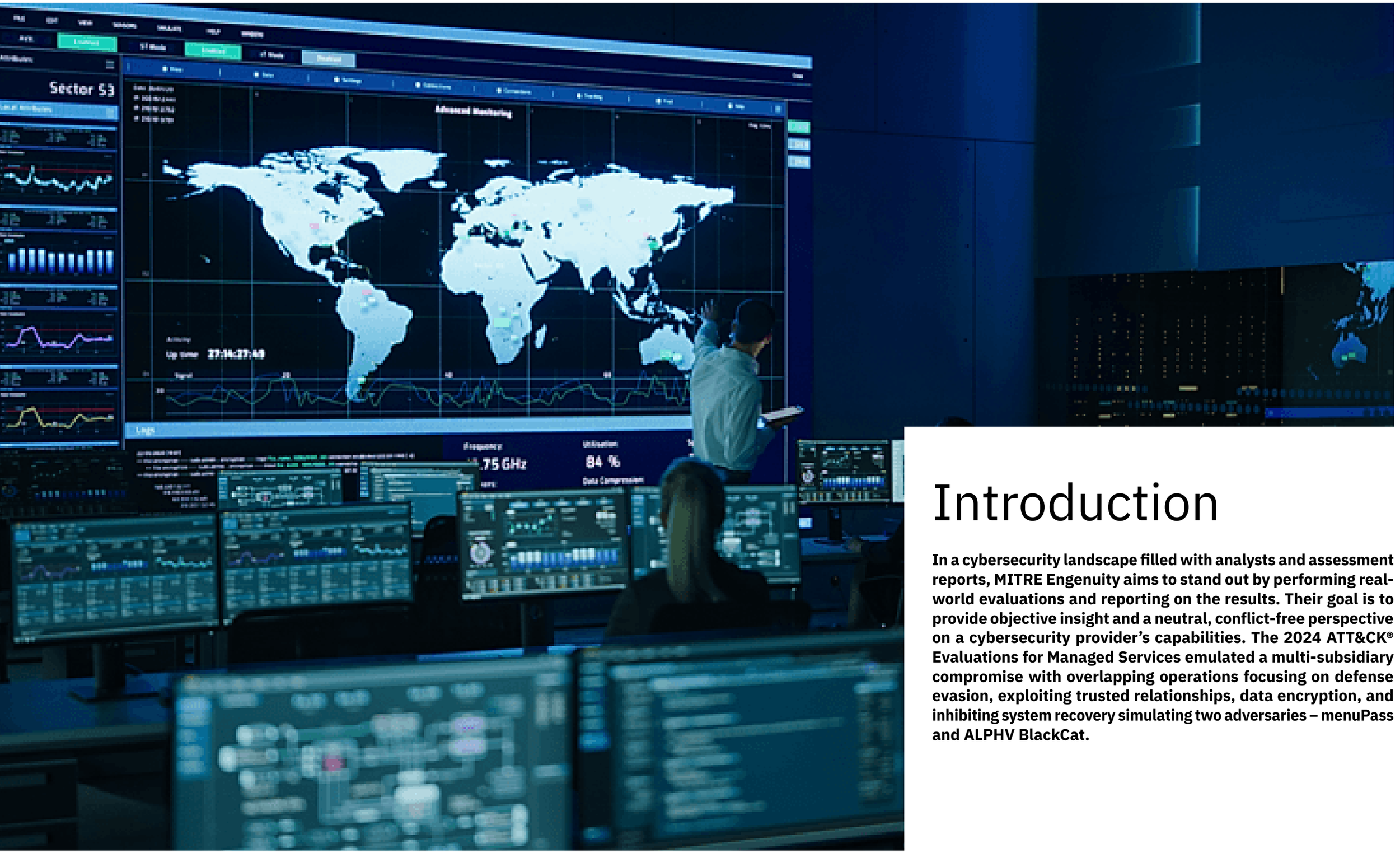


A guide to the 2024 MITRE ENGENUITY ATT&CK® EVALUATIONS

for Managed Services

Table of contents

Bitdefender® Global Leader In Cybersecurity



Introduction

In a cybersecurity landscape filled with analysts and assessment reports, MITRE Engenuity aims to stand out by performing real-world evaluations and reporting on the results. Their goal is to provide objective insight and a neutral, conflict-free perspective on a cybersecurity provider's capabilities. The 2024 ATT&CK® Evaluations for Managed Services emulated a multi-subsidiary compromise with overlapping operations focusing on defense evasion, exploiting trusted relationships, data encryption, and inhibiting system recovery simulating two adversaries – menuPass and ALPHV BlackCat.

What are the MITRE Engenuity ATT&CK® Evaluations?

Founded in late 2019 as part of the MITRE corporation, MITRE Engenuity is a tech foundation supporting the cybersecurity industry through a variety of services including special research projects, research and development collaboration, grant-funded studies, capture the flag competition, the ATT&CK® Evaluations and more. Not to be confused with the MITRE ATT&CK® Framework itself, MITRE Engenuity works as a separate entity and these evaluations are not a validation of the ATT&CK ® Framework's accuracy or completeness.

The ATT&CK® Evaluations began as a test of enterprise cybersecurity tools back in 2018. There have been five since the initial evaluation, with only 2020 being skipped due to COVID-19. The enterprise evaluations focused on cybersecurity products such as endpoint detection and response (EDR) or extended detection and response (XDR) solutions involving a series of simulated attacks to measure the tools' ability to detect, investigate, and remediate threats. In 2022 MITRE Engenuity introduced the first evaluations of Managed Services in which they simulated real world threats to test services beyond just security tools. These evaluations focused on the service provider's abilities to monitor and detect threats and how they communicate and support customers, rather than a test of the tools themselves. These evaluations, despite the limitations of any controlled test, remain one of the most accurate and comprehensive tests for managed services. Let's dive in and see what makes these evaluations so different.

How Did They Evaluate Managed Services?

This evaluation was an attempt to simulate a real-world attack and see how each vendor participant performed. It was a closed book test in that none of the participants were made aware of the type of attack techniques or attacker profiles that would be used during the evaluation. Participants were given a realistic on-prem environment to install their security tools and sensors on and then MITRE Engenuity acted as customers/red teamers performing a series of attack techniques and steps as part of a threat simulation. Each participant's configuration – software tools and sensors used – are listed on the MITRE Engenuity site by clicking the configuration settings button under each participant. For example, Bitdefender used our own GravityZone Platform and EDR sensor and detailed information on our setup can be found here.

Adversary and Attack Simulation

This evaluation simulated both menuPass and ALPHV BlackCat adversaries. MenuPass has been publicly active since 2006 and is suspected to be sponsored by the Chinese Ministry of State Security (MSS). They are known for targeting various industries globally, with a focus on stealing sensitive information like intellectual property. ALPHV BlackCat is a well-known Ransomware-as-a-Service (RaaS) operation that provides flexible ransomware strains written in Rust to other malicious actors allowing them to quickly and easily target any platform.

Evaluation Criteria

During the testing period, participants were evaluated based on their alerts and reports sent via email or posted in the participants portal. Participants could communicate with the “customer” via chat, but these would not be counted as part of the evaluation criteria. MITRE Engenuity evaluated participants across four primary metrics:

1. **Mean Time to Detect:** The average time from when the red teamer initiated a behavior or event and when the participant alerted on that behavior across all steps.

2. **Alert Volume:** The combined total number of alerts sent by the participant via email and inside the portal. Used to assess a participant’s ability to reduce noise and alert fatigue.

3. **Detections (and their Actionability):** How MITRE classified whether a participant successfully detected the attack step or substep (technique). They assigned three possible statuses and distinguished how actionable the alerts were.

    - **Not Applicable (N/A):** Execution failed, so nothing to alert or report on.
    - **Not Reported (Visibility Only):** Vendor did not notify, alert, report, or provide sufficient evidence they detected a behavior.
    - **Reported:** Vendor provided sufficient notification and evidence of the activity being evaluated
    - **Actionability:** A separate distinguisher on the “reported” status to denote if enough information was provided with the alert/notification rather than just noise. Was there enough context and detailed information about what, where, when, who, and why to act. This metric can act as a reasonable interpretation for how the participant would have responded in a real-life scenario.

4. **Enrichment of the After-Action Report:** Every participant was required to submit a full report summary of the attack simulations. MITRE Engenuity specifically looked for participants to include the following in their AAR:

    - Chronological breakdown of adversary’s activities
    - Technical details
    - Recovery or remediation recommendations
    - Attribution
    - MITRE ATT&CK tactics and techniques mapping

How Did MITRE Engenuity Present the Results?

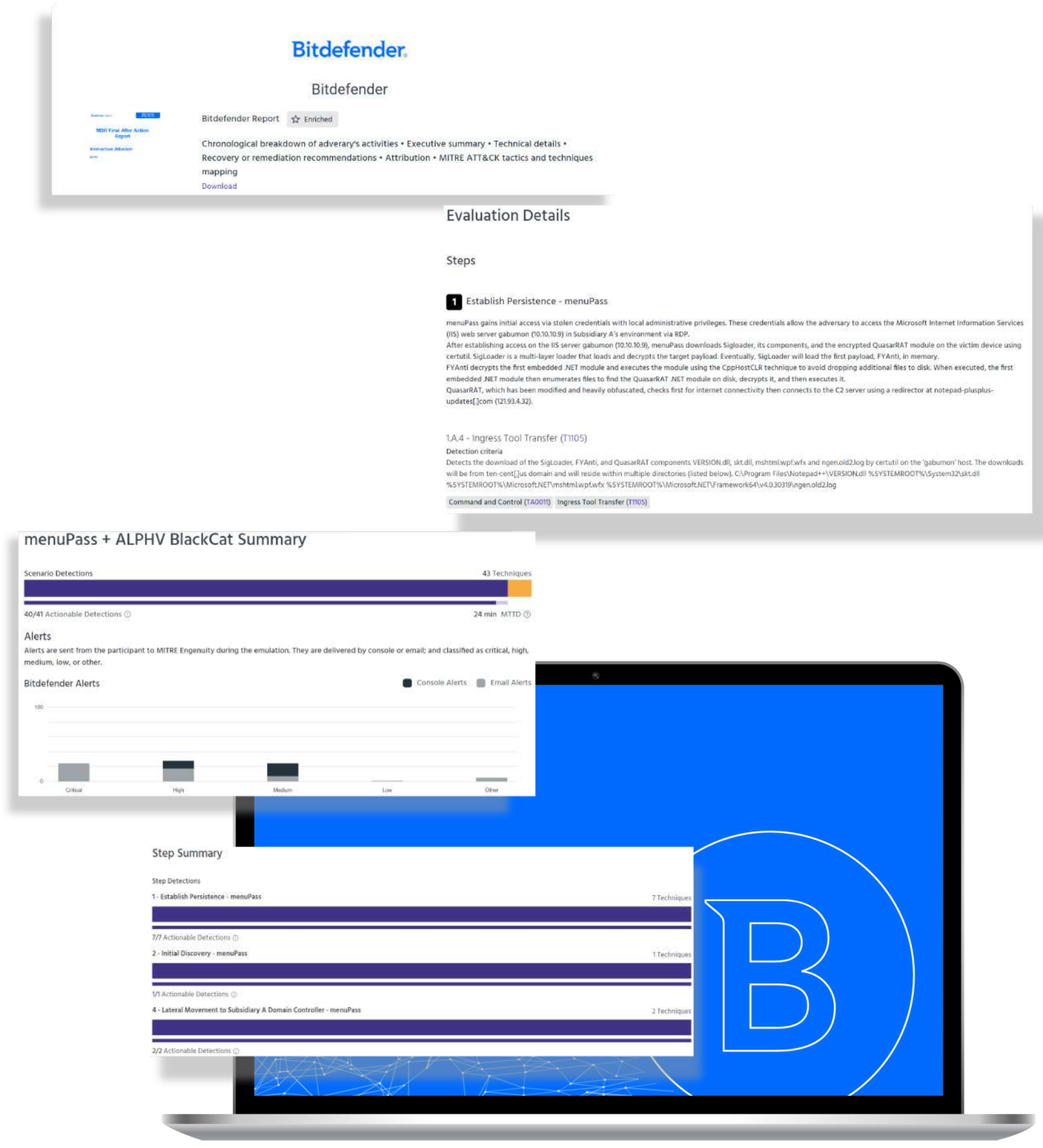
First it should be noted that MITRE Engenuity evaluations and results are available to everyone for free and can be accessed at any time through their website.

There are two primary ways to view the results. First is the webpage which is a curated summary overview of the key findings including a couple of snapshots and details from the evaluation. The JSON file, which can be downloaded per participant, serves as the authoritative source of truth for the evaluation, providing a comprehensive and granular view of the results. Let's go over each section of the webpage and how the information is grouped:

Vendor Info and AAR: Brief company info and the ability to download their AARs. You will also see buttons in the top right to view configuration info of the partner's security setup as well as the button to download all results data as a JSON file.

Results Summary: This section has two parts. An overall summary showing total scenario detections and alerts, the actionability rating, and the average MTTD. Under is the individual summary of each of the 15 high level steps and their subsequent substeps underneath.

Evaluation Details: This final section is where the meat of the data lives. It provides detailed information of each step and substep with included screenshots and information from the vendor.



Testing Limitations

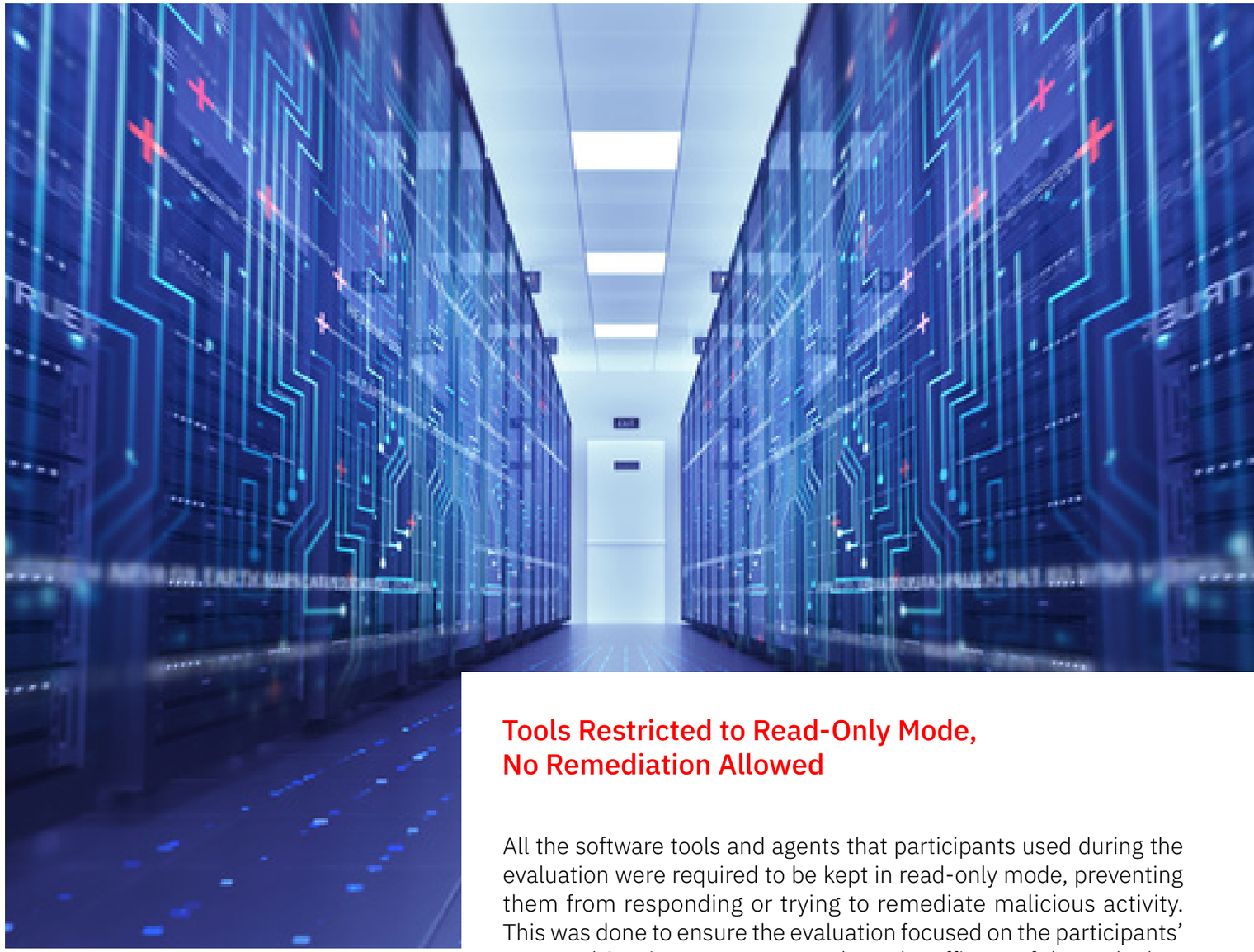
With any evaluation, there will be limitations to what is being measured because certain factors could impact other parts of the evaluation. Let's explore some of these considerations.

Environment Simulated On-Prem Only

It's obviously difficult to set up a testing environment that mirrors the full setup of real-world environments of most organizations. Having the testing environment only focus on on-prem systems (servers and endpoint hosts) means they left off a large portion of cloud-based services that most organizations use including IaaS (Infrastructure as a Service) environments, SaaS (Software as a Service) applications, and Identity management systems.

Managed service organizations must be able to support these cloud-based services and be highly proficient in detecting and responding to threats in them. It is important to keep this in mind when reviewing the results, and we encourage customers to do additional research to ensure that the security service they choose to invest in can support and monitor all aspects of their environment.

Software tools and agents that participants used during the evaluation were required to be kept in read-only mode, preventing them from responding



Tools Restricted to Read-Only Mode, No Remediation Allowed

All the software tools and agents that participants used during the evaluation were required to be kept in read-only mode, preventing them from responding or trying to remediate malicious activity. This was done to ensure the evaluation focused on the participants' Managed Service component and not the efficacy of the tools they used. This meant that each attack, and every step, substep, and TTP used would be successful requiring each participant to prove they can detect each activity and alert the customer.

For organizations reviewing the MITRE Engenuity results should make sure they do additional due diligence to verify the participant's ability to respond and remediate threats.

How To **Interpret** the Results

MITRE Engenuity is not an analyst firm and as such performs these evaluations to foster competition and collaboration across the cybersecurity community rather than assessing vendors to discover a definitive winner. This evaluation is a means for security vendors to test themselves against a set of standardized metrics with the ability to review the objective resulting data.

		Bitdefender	BlackBerry	CrowdStrike	Field Effect	Microsoft	Palo Alto Networks	Secureworks	SecurityHQ	SentinelOne	Sophos	Trend Micro	Mean	Median
Coverage Quality	Visibility (data collected)	43	42	43	41	43	43	43	43	43	43	43	43	43
	Reported (not actionable)	41	35	42	25	37	38	25	33	38	36	36	35	36
	Reported (actionable)	40	30	40	20	27	34	23	24	31	27	22	29	27
	Were any Red Team activities missing from incident reports?	No	Yes	Yes	Yes	Yes	No	No	Yes	No	No	Yes	N/A	N/A
Speed	MTTD (minutes)	24	48	4	11	24	24	33	93	47	72	65	41	33
Noise	Emails + Alerts	82	394	579	196	385	1119	878	200	189	942	310	479	385
	Total Emails	54	307	326	98	162	37	51	125	32	24	138	123	98
	Total Alerts in Console	28	87	253	98	223	1082	827	75	157	918	172	356	172

**This table is a compilation of data from each participant's results in the JSON files*

Very few were able to do so in a manner that showcased the value and benefit of their managed service offerings.

We previously covered the evaluation criteria and metrics MITRE Engenuity used above -- MTTD, alert volume, Actionability, and AAR enrichment – and wanted to showcase those metrics in more granular detail. This table zooms in on those metrics including a breakdown of the actionability of reporting into two distinct rows and including overall visibility.

- ✓ **Visibility:** Did the tool or service have visibility over the attack step or technique used.
- ✓ **Reported and Actionability:** How many of the steps and substeps (techniques) the participant successfully reported on. This is split showing how many of these reported alerts/notifications were deemed actionable by the MITRE Engenuity.
- ✓ **Not Reported:** Did the participant miss any of the steps or techniques performed?
- ✓ **MTTD:** The average time in minutes it took to detect an activity after the activity was executed by the red teamer.
- ✓ **Number of Alerts:** Total number of alerts sent to the "customer" broken down by how they were sent (email or inside the console)

While many participants successfully detected and reported on the threat and adversary tactics, very few were able to do so in a manner that showcased the value and benefit of their managed service offerings. Here are some key points to focus on when interpreting these results to better assess each participant.

Mean Time to Detect

MTTD helps highlight how fast organizations can detect suspicious activity. A key benefit of any managed service offering is to reduce the MTTD to better mitigate threats as early as possible. While some vendors had incredibly low MTTDs, it was often paired with an abundance of alerts which in a real-world scenario would translate to alert fatigue for their customers. Organizations comparing vendors should ensure they are not looking at MTTD in a vacuum but rather in conjunction with the other metrics to get a clearer picture of the capabilities and benefits the participant is trying to showcase.

A high number of alerts combined with low actionability indicate a high likelihood of alert fatigue

Noise Reduction

A key reason organization's look to managed service providers is the lack of security expertise or time to properly investigate alerts and suspicious activity. Managed service providers help alleviate that burden by investigating events, filtering out false positive or benign activity, and only notifying and acting on actual malicious activity.

Participants with a low number of total alerts but high percentage of reported attack steps demonstrate their ability to reduce noise while still detecting and responding to threats quickly and effectively. On the flip side, a high number of alerts combined with low actionability indicate a high likelihood of alert fatigue requiring the customer to do more manual investigations. Organizations assessing participants should download the JSON file to review how they handled alerting and communication.

Actionability

The addition of actionability in this evaluation helps to distinguish participants for how they communicate and how they would respond to a threat in a real-life scenario. It's important for Managed Service providers to be able to communicate clearly and concisely what is occurring within the environment while also demonstrating the expertise, knowledge, and experience to respond effectively.

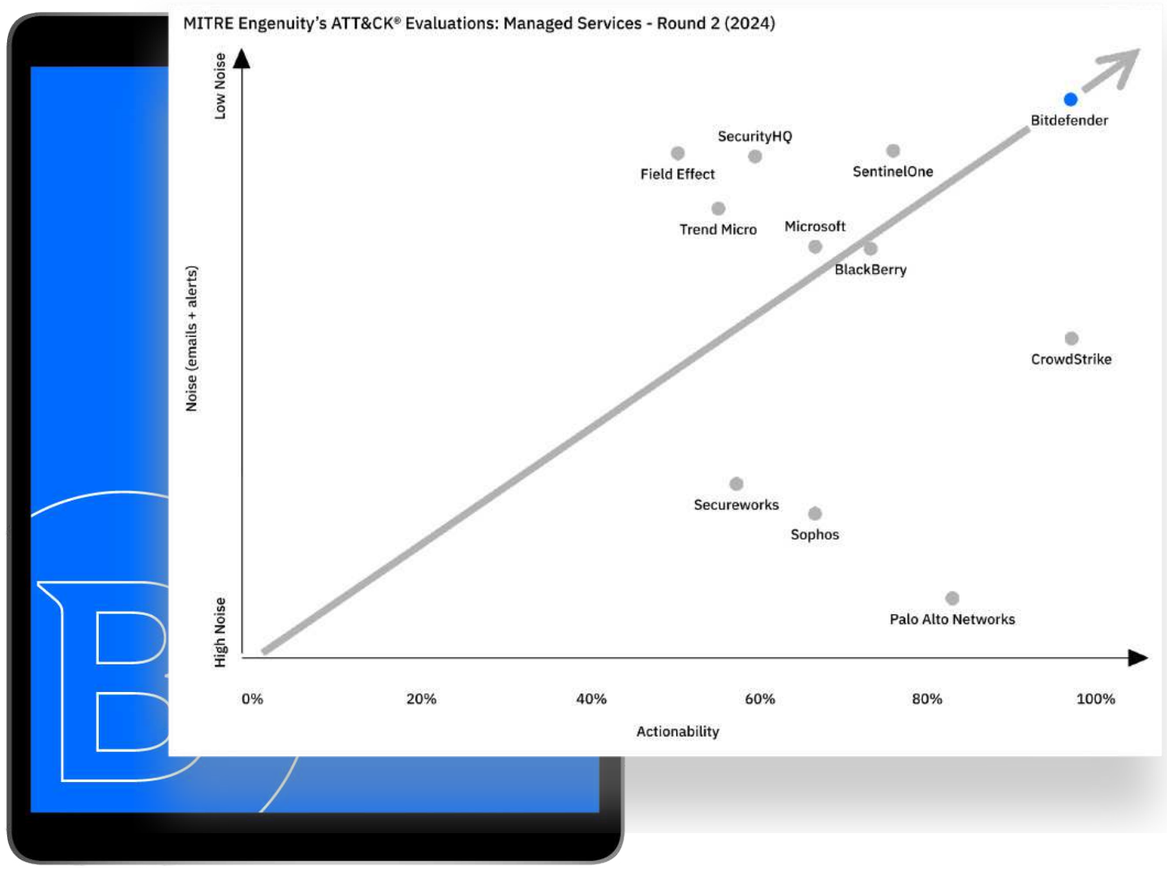
The After-Action Report

Participants were required to submit an After-Action Report (AAR) that provided a clear summary of the attack simulation. While MITRE Engenuity did not directly include this report in part of its evaluation metrics – only whether the report included required information to be deemed an "enriched report" – it remains one of the best treasure troves of information and datapoints that can be used to better evaluate and assess each participant. The AARs help demonstrate or provide examples for how the participant handles threat intelligence and research, communication, security expertise and how they identify and detect threats, and how they would respond or handle remediation.

Organizations reviewing the participant AARs should pay close attention to the type of info provided to get a sense of how organizations would respond to a threat. Beyond the recommendations or suggested actions, how a participant explains and describes the attack steps can indicate how well the vendor understands what is going on to mount a proper and timely response. Also, did the participant go above and beyond what was required of them? Bitdefender was able during the attack execution window to create and provide a script that would be able to decrypt files encrypted by the ransomware being used.

It's important for Managed Service providers to be able to communicate clearly and concisely what is occurring within the environment while also demonstrating the expertise, knowledge, and experience to respond effectively

Bitdefender – Timely Detection and Response... Without the Noise



The MITRE Engenuity evaluations are valuable because they delve into a range of interconnected metrics, providing a more nuanced picture of a vendor's capabilities. It's important to consider the data provided in context, as some vendors might choose to focus on specific metrics to their advantage. No one metric tells the whole story, and organizations must consider their own needs and what they are looking for in a Managed Service Provider.

Looking at all the metrics together and in context, Bitdefender came out as one of the strongest vendors in the evaluation. Bitdefender had 100% visibility over the entire attack chain and provided the highest percentage – 93% – of actionable reporting with the least number of notifications sent – 82 total and over 100 alerts less than the second lowest – demonstrating our ability to help reduce noise without compromising our detection and response capabilities.

We were also able to detect the malicious activity within 24 minutes of the event occurring while heavily reducing the number of alerts sent to the customer. Our focus lies in striking a balance between timely detection and minimizing unnecessary noise. We prioritize delivering high-fidelity alerts that provide actionable insights, allowing your security team to respond efficiently to genuine threats.

This evaluation helped highlight Bitdefender's ability to understand the attack occurring, and provide information about the w hat, where, when, who, and why demonstrating our security expertise and ability to effectively respond to the attack if this were a real customer and a real threat. If you're looking to partner with a trusted security provider, reach out to us today to learn how Bitdefender can help secure your organization. broken down by how they were sent (email or inside the console)

Bitdefender® Global Leader In Cybersecurity

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Trusted. Always.

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.