

Bitdefender With Advance Threat Defense

The fact that modern-day organizations are faced with **advanced threats** to their data is no hidden knowledge. There is a cyberattack on networks and computers every [39 seconds](#) – affecting one in three North Americans each year.

MSPs particularly headline such cyberattack agendas, providing access to various organizations that they work with. This is why **endpoint protection** has emerged as a key service differentiator in the MSP industry.

With the demand for specialized protection against cyber threats continues to rise, MSPs need to integrate leading **endpoint security tools** within their network – such as **Bitdefender ATS**.

What Is Bitdefender?

Bitdefender ATS, short for Advanced Threat Security, is a modern EPP (**endpoint protection** software) solution that deploys an entire spectrum of technologies to prevent malware and cyberattacks.

From authorization checks to machine learning, Bitdefender utilizes industry-leading standards to prevent the execution of an attack on the endpoint infrastructure of your customer networks.

With a machine learning process that has developed over ten years, Bitdefender offers a proven security suite that is designed keeping MSPs in mind. This allows you to pick up on the most elusive of threats, comfortably managed with a single multitenant console and monthly licensing cycle.

Bitdefender's Key Point - Advanced Threat Protection

A layer of protection that defends your customers against targeted ransomware attacks not only reaffirms your client's trust in your service but the simplified management console allows you to be more proactive and efficient – resulting in a better service offering.

So, what are the features that help distinguish Bitdefender as a leading endpoint solution?

HyperDetect

This feature has been introduced recently into the security suite, exclusively operational in the pre-execution phase. It utilizes local machine learning models as well as advanced heuristics to detect potential threats to a network.

The cutting-edge machine learning system allows it to expand beyond an advanced **antivirus** solution to safeguard against the continuously evolving cyber threats. Here's an impressive list of its capabilities:

- Spot hacking tools
- Discover network exploits and malware obfuscation techniques
- Block sophisticated threats before execution
- Detect malware delivery techniques
- Identify sites that host such exploit kits
- Stop traffic from suspicious websites accessing the network

Additionally, HyperDetect also allows security administrators to utilize their expertise and customize defense strategies according to the risks that are most likely to be associated with each particular business.

The 'report-only' feature is specifically designed to allow security admins to deploy and monitor any upgrades or alterations to the defense policy before they roll it out across the system. This helps detect errors and bugs beforehand and saves valuable business time.

To round it off, **Bitdefender HyperDetect** offers a blend of high visibility and aggressive security measures by allowing users to set their protection levels at a normal or permissive level.

The software will continue to report things on an aggressive mode, providing early indications of any threats or issues that may arise in the future.

Endpoint Integrated Sandbox Analyzer

This powerful component combines machine learning with behavioral analysis to examine any suspicious file in depth. To make it happen, the **Bitdefender GravityZone Sandbox** detonates such payloads in a contained virtual environment and then analyzes their behavior to identify malicious intent.

When integrated with the GravityZone Endpoint agent, the Sandbox Analyzer comprehensively analyzes every file and submits anything that looks malicious to the Endpoint Security HD. This allows Bitdefender to block that file across the network, on all systems, ensuring foolproof security.

However, Bitdefender has reserved the right to monitor or block a file for the administrator. If you opt for blocking a potentially malicious file, that file remains inaccessible until Bitdefender verifies that is safe for use.

The complete array of Bitdefender comprises of multiple aspects that help form a reliable wall of defense against the **advanced threats** faced by companies.

Advanced Patch Management Capability

Organizations have evolved from a static workstation centric environment to a more flexible and dynamic environment. This allows each individual to increase productivity through a variety of devices and applications.

However, the increasing number of devices means an increased possibility of unpatched systems, and inevitably increases the risk of malware outbreaks and data breaches.

This is why a core component of the Bitdefender security offering is the patch management solution across the entire range of devices – including workstations, physical servers, and virtual servers.

Patch management requires customizing security updates across different operating systems and applications to allow for a completely secure network. Bitdefender excels in this – and more. Here's what it can do for your clients:

- Automatic and manual patching options for different operating systems
- Patching management solutions to the largest collection of software applications
- Detailed information centering patches; Bulletin ID, Patch Severity, CVE to name a few
- Ability to segment different schedules for security and non-security updates
- Rapid deployment for missing patches
- Automatic reports for missing patches in devices

Bitdefender ATS – #1 Ranked MSP Security Suite

Bitdefender provides layered next-gen protection technology for MSPs, adding much-needed value to their security offerings.

When compared to leading **endpoint protection** software and antiviruses, Bitdefender stands tall among its competitors.

What differentiates Bitdefender from its rivals? Here's a list of reasons that elevates **Bitdefender ATS** above other EPP and **antivirus** solutions.

Upgraded Security Efficacy

With advanced protection measures that help detect threats evading traditional endpoint security, Bitdefender can allow you to prevent such incidents in the pre-execution stage.

Built on an adaptive layered architecture, there is no chance of a false positive. While traditional endpoint security limits itself to **antivirus** diagnosis, Bitdefender allows you to detect any threats that may evade common measures.

Immediate And Effective Response

With cybercriminals continuously on the lookout for opportunities, data breaches have become an inevitable part of doing business. Bitdefender assists in setting policies that allow security administrators to take immediate action.

The system provides further feasibility by terminating the said malicious program and preventing major losses from taking place.

Deeper Insight

The proven machine learning algorithm allows Bitdefender to pitch suspicious files to its Sandbox system, which detonates the payload to examine it for security purposes.

Additionally, the system also provides additional context to help understand the threat better and take relevant action.

As businesses continue to grapple with advanced threats in the online world, MSPs can utilize Bitdefender's ATS to provide enhanced protection to their clients. Its advanced features, coupled with an easy billing cycle, making it the perfect addition to your service.

List Of Keywords

- Antivirus
- Endpoint protection
- Advanced threat
- Endpoint security tools
- Bitdefender ATS
- Bitdefender GravityZone sandbox
- Bitdefender HyperDetect

CONFIDENTIAL