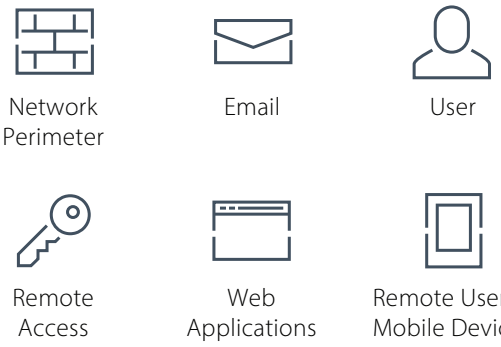
Barracuda
Your journey, secured.

Barracuda Advanced Threat Protection

WHITE PAPER

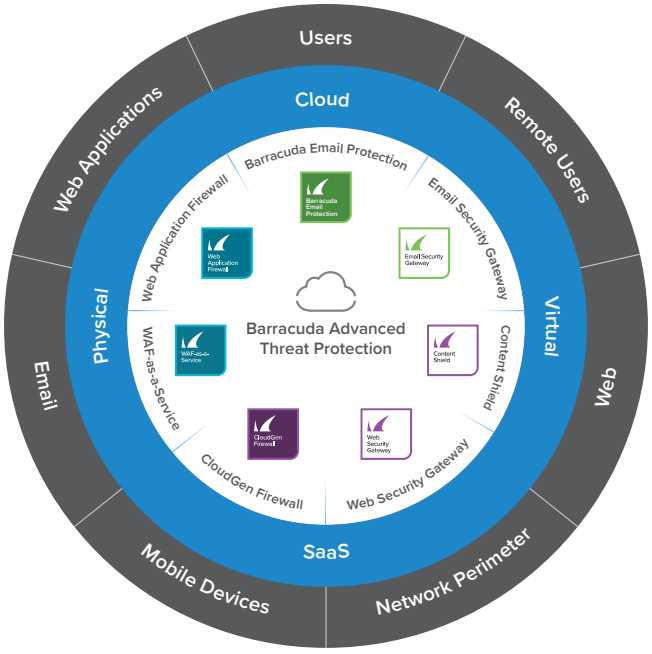
Modern threats need layered threat protection

The polymorphic nature of modern cyber threats renders traditional signature-based defense mechanisms inadequate. On the other hand, in-depth defense techniques like sandboxing are expensive and come with performance overheads. Comprehensive, reliable protection against attacks like ransomware and advanced persistent threats require a layered approach with progressively sophisticated defense techniques that balance accurate threat detection with fast response times. Also, the architecture should provide protection from all threats across all the threat vectors and across multiple deployment surfaces like physical and virtual infrastructures, SaaS services, and public cloud platforms.



The 6 most common internet threat vectors

Barracuda Advanced Threat Protection (BATP) is a cloud-based service that provides in-depth defense against ransomware, malware, and advanced cyber attacks. It consists of multiple layers of detection, including signature, static, behavioral analysis—all the way to comprehensive sandboxing to provide accurate detection of a variety of polymorphic attacks. This cloud-based service has been integrated with all Barracuda security solutions, protecting specific threat vectors—like web, users, network, email, and applications—across any deployment surface. BATP is automatically connected to a global threat intelligence network that gathers threat data from diverse sources around the world, providing real-time protection across all threat vectors.



Barracuda Advanced Threat Protection (BATP)

Advanced threats evade traditional detection techniques

Modern attacks are rapidly growing in volume and sophistication. New malware strains like ransomware are designed to evade traditional detection techniques and are often propagated through targeted, zero-hour attacks.

According to leading industry analysts, we can expect over 200 new strains of ransomware per quarter through 2023.[1] For attackers, this is a huge business opportunity, and they are just getting started: Ransomware alone will pull in over $1 billion in revenue for these criminals in 2017. And while that's great news for them, it leaves many scrambling to figure out how to best protect themselves from these new types of attacks.

Threats like ransomware exploit multiple threat vectors

More than ever, threat actors are deploying modern malware exploits across multiple threat vectors to gain maximum efficiency and effectiveness. Email is by far the preferred method of delivery, especially for phishing and spear phishing attacks. In fact, IDC estimates that "more than 90% of ransomware infections are known to be delivered through malicious email attachments."[2]

1 *Analyst, Michael Osterman 2016*

2 *IDC ANALYST CONNECTION: Why SaaS-Based Productivity Tools Require Additional Threat Protection - 2017*

Users can also be enticed into downloading malicious payloads through social engineering, spoofing, hacked websites, tampered URLs and other techniques. Furthermore, a gateway firewall, by itself, may not be enough with so many workers being mobile and with networks becoming more dispersed.

Remember: A comprehensive security strategy should address all threats across all threat vectors. Additionally, an effective threat protection framework should cross-pollinate diverse threat intelligence gathered across all the vectors.

Sandboxing, by itself, isn't efficient

Sandboxing is the method of choice for detecting zero-hour threats. It usually consists of 'detonating' file attachments in a virtual 'sandbox' that emulates endpoint environments that are susceptible to attacks.

While sandboxing can be effective (because of the high processing requirements), it can be a time-consuming operation if applied to every attachment. To avoid large delays in content delivery, organizations either require very large and expensive sandboxing appliances, or risk exposure to attack by allowing the delivery of some attachments before they are fully scanned. Some advanced threats are designed to detect sandboxing environments that are purely based on virtual machines. To evade the sandbox, these threats mask any malicious activity, thereby rendering the sandbox useless.

Also, premises-based sandboxing solutions are typically deployed at a corporate HQ, and requires remote and satellite locations to backhaul attachments to the sandbox. On-premises sandbox solutions cannot scale as organizations add more traffic, locations, and users. To complicate matters, organizations are moving their infrastructure to the cloud; therefore, they have to extend their security posture into the cloud, which adds burden to the premises-based sandbox.

Defense-in-depth with Barracuda Threat Protection

To address these challenges, Barracuda has leveraged its decades of experience dealing with advanced malware to build a cloud-based platform that provides comprehensive protection against all types of malware without compromising performance, coverage, accuracy or security.

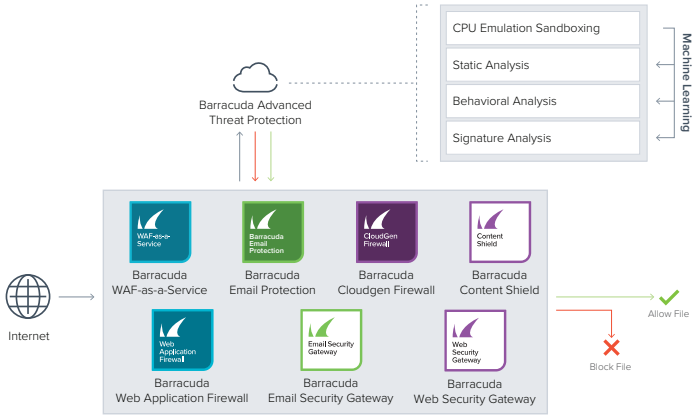
Layered protection

Barracuda Advanced Threat Protection (BATP) is an integrated cloud-based service that consists of multiple layers of threat detection, combined with machine learning techniques. Each detection layer is designed to progressively eliminate threats at different levels of severity and complexity. By pre-filtering threats as they move through the layers, BATP can respond very quickly to any type of attack with minimal delays in the data path and without requiring any compromises to security policies. Also, the various threat detection layers automatically share analysis results with each other, so the overall service gets better and faster at responding to new threats as it processes more data. This ensures that repeated instances of threats can be caught quickly at the lower layers while leaving the more resource intensive layers, like sandboxing, free to operate on emerging threat variants.

The layers include:

1. Advanced Threat Signatures: Barracuda collects threat signatures from over 250,000 Barracuda endpoints (appliances and services across the web), as well as information from honeypots, crawlers, downloads, viruses, malware spyware, email attachments, network, and application data. This all comes together to create a massive threat intelligence signature database that ensures that any new threat seen anywhere under Barracuda's purview is immediately shared across all its security products and subscribers in real-time.
2. Behavioral and Heuristic Analysis: Behavioral and heuristic analysis is a process where the execution of certain programming commands of a questionable piece of code or script is conducted in a controlled environment. The resulting behavior is analyzed for common viral activities such as replication, file overwrites, and attempts to obfuscate the suspicious file. Other suspicious activities might also include excessively long timers, programming loops that run for days, or code that tries to access the registry or memory functions.
3. Static Code Analysis: Static analysis consists of examining parts of an executable file without actually executing it. Malicious code writers attempt to obfuscate the malicious code to subvert the malicious code detectors, such as anti-virus software. The static analysis layer analyzes and de-obfuscates any questionable code constructs. This layer is a highly effective, fast method of pre-filtering malware before sending questionable files up to the sandboxing layer.

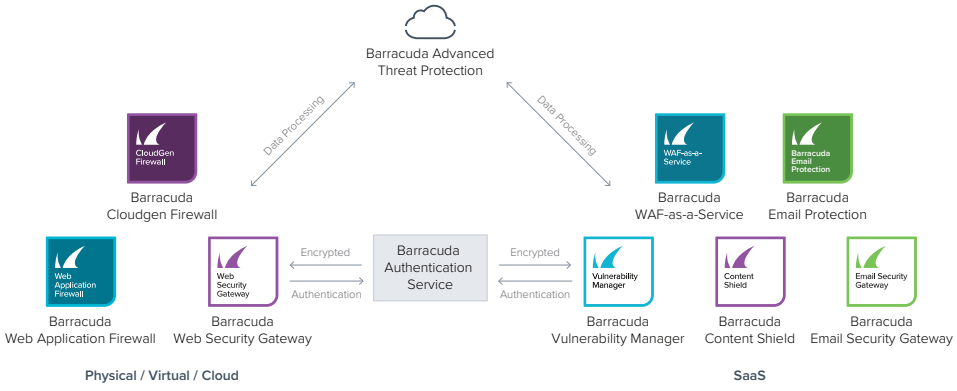
4. CPU Emulation-Based Sandboxing: The last layer of defense is a comprehensive CPU emulation-based sandbox that will comprehensively 'detonate' any attachment that is not conclusively analyzed by the preceding layers. By using CPU emulation techniques, the sandbox can detect threats that are designed to evade traditional virtualization-based sandboxes. Also, by pre-filtering the files through the other layers, BATP ensures that the sandbox is able to process the really complex threats with minimal delays.



Layered threat protection

Distributed, scalable cloud service

BATP fully leverages the benefits of a globally distributed, highly scalable cloud micro-services architecture. It is used by Barracuda's entire portfolio of security products that include network, web application, email, and web security solutions. The service can be automatically expanded for performance and coverage to handle increasing traffic volumes from Barracuda customers around the world. It uses highly secure communication channels to ensure the privacy and security of data transmission.

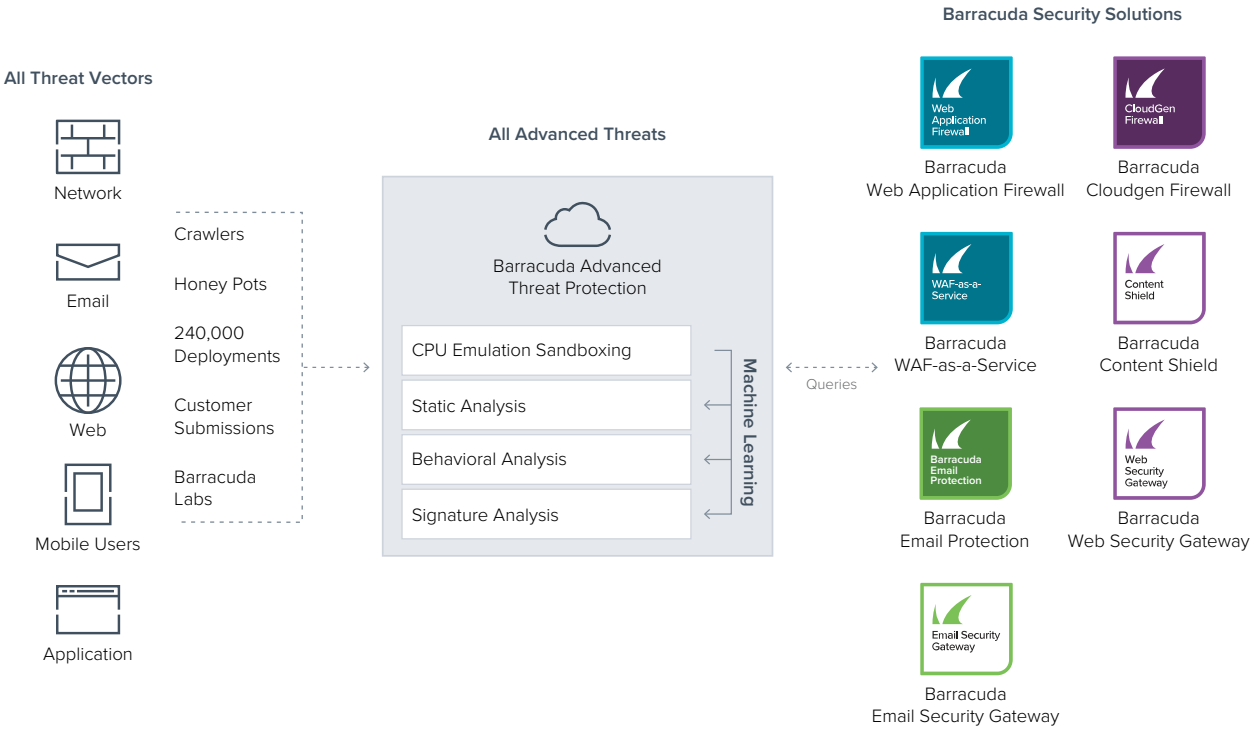


Barracuda BATP architecture

Global threat intelligence network

As a result or extending protection across multiple threat vectors, BATP leverages a powerful global threat intelligence network that ingests vast amounts of diverse threat information from over 50 million deployed collection points around the world. Barracuda's ATP infrastructure utilizes a hardware-accelerated machine-learning farm that analyzes this data by looking at over 900 attributes per artifact.

All Barracuda products that are covered with BATP become a part of this highly diverse network that shares threat intelligence across all the threat vectors for real-time protection for its subscribers. For example, a threat that is first propagated over email will be detected by BATP, and the protection will instantly be extended to all other threat vectors that are secured through the service. Additionally, once that new threat is identified and a signature is created, the information is pushed to Layer 2; so the next time that threat attempts to enter your network, it will be blocked, thereby eliminating the need to send it to the sandbox again. In a 2016 independent test conducted by MRG Effitas and AV-Comparatives, the Barracuda CloudGen Firewall, with Barracuda Advanced Threat Protection technology enabled, was the only solution tested to achieve 100-percent effectiveness, along with a zero-percent rate of false positives.



Conclusion

Architecting a comprehensive security approach to defend against today's advanced threats is a multi-dimensional challenge. Barracuda Advanced Threat Protection combined with Barracuda's portfolio of purpose-built security solutions provides an easy, economical, scalable, and powerful way for organizations to conquer this obstacle.

Barracuda®
Your journey, secured.