Barracuda
Your journey, secured.

How Barracuda Application Protection can protect you from ransomware

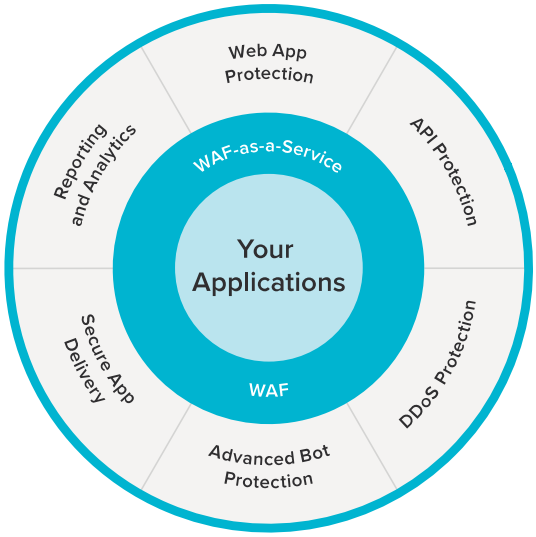
An increasing number of ransomware groups are using web apps for initial access. Stop them in their tracks with Barracuda Application Protection.

As more organizations' email systems become more protected against phishing attacks, attackers are more frequently exploiting web and API applications to gain entry into networks. In addition, many of these applications offer direct access to the credentials and data that these attackers are looking for — making it much easier and faster for them to compromise these organizations. It is more crucial now than ever to take every possible measure to ensure your web applications and APIs are well protected.

Protecting your web apps and APIs from ransomware

Web Application Protection

Barracuda Application Protection stops web application attacks, including OWASP Top 10 attacks and zero-day attacks. Its Smart Signature engine is very efficient at stopping new attacks, with low false positive rates. Machine learning-powered risk-based security ensures that advanced attacks are detected based on behavior, so sneaky advanced attacks are detected and blocked.



The Smart Signature engine is our highly efficient take on attack signatures. Each signature in this engine can handle more than 40 individual attacks, with all the variations in encodings and patterns that attackers use to try to bypass traditional signatures. The biggest benefit of this approach (over exploit-specific signatures) is the early detection of zero-days, which are now being exploited by ransomware groups like they were in the MoveIT breaches, with low false positives.

Machine learning-powered risk-based security learns about the access patterns of the application and looks at each access and user from the perspective of risk. Each access is validated by specifically tuned models that then assign a risk score. As riskiness increases, actions are implemented to validate and eventually block attackers.

API Protection

Attackers are targeting APIs more, and this is because APIs are extremely under-protected. A significant part of the problem is that many defenders do not know that APIs have been deployed in their environment — so-called shadow APIs. Barracuda Application Protection uses machine learning to first detect these unknown API endpoints and then automatically turns on security for them, ensuring comprehensive security for your JSON and GraphQL APIs.

Advanced Bot Protection

Advanced persistent bots are increasingly used for everything from application DDoS attacks to account takeover attacks. Barracuda Application Protection uses machine learning to identify and block these bots and their low and slow attacks. The built-in Credential Stuffing Protection can identify credential attacks by matching incoming credentials against our leaked credential database and prevent these attacks. Privileged Account Protection uses machine learning to identify anomalies in user behavior and detect and block compromised accounts where the credentials have not been leaked yet.

Stolen credential attacks are among the most commonly used methods of gaining initial access. These attacks could happen using credentials from a previous breach (such as the ones floating around from the LinkedIn breach) or using credentials from a new attack — typically a phishing attack that uses a reverse proxy such as EvilGenix to steal fresh valid credentials.

Barracuda Application Protection uses multiple layers to identify and block these account takeover attacks. The first layer is preventing credential stuffing attacks. The solution has its own updated database of known leaked credentials running in the cloud. All incoming logins are validated to ensure that no known leaked credentials are being used to login. To ensure security of credentials in transit, only partial hashes of username and password pairs are used for validation — these cannot be reversed to gain the complete username and password.

However, this type of protection does not work for “freshly” stolen credentials. This is where the Privileged Account Protection capability comes in. Privileged Account Protection uses machine learning to profile each incoming authenticated user and their behavior. This profile is then used to validate user behavior across the application. Any anomalous behavior causes the system to validate and send alerts to admins to identify and block any malicious access and stop attackers in their tracks.

Conclusion

Ransomware attacks continue to evolve, becoming more complex every day. No organization can ever be fully protected from ransomware by a single layer of security. That’s why a defense-in-depth strategy is best for protecting against ransomware attacks. Barracuda can help you build a winning strategy against ransomware, providing solutions that help your organization detect, prevent, and recover from ransomware attacks.

NEXT STEPS

Don’t be the next ransomware victim.

Does your ransomware protection have teeth?

Barracuda is uniquely qualified to protect your business from ransomware because we can help you defend against every stage of a ransomware attack — including the new, more sophisticated AI-powered attacks. We provide the email, network/application, and backup solutions required to defend your business against ransomware.

FIND OUT MORE ↗

Don’t wait to get protected.

The best time to fight ransomware is before it strikes. Barracuda’s comprehensive approach to ransomware protection provides the solutions essential to securing your business from critical attack vectors. If you’re concerned about ransomware, we can help you build a ransomware protection plan.

GET IN TOUCH ↗

Barracuda®
Your journey, secured.

SOLUTION BRIEF • US 1.0 • Copyright 2024 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com