Malwarebytes combines seven distinct but complementary technologies to break attack chains, from pre-execution to post-execution.

1. Application hardening
   - Enhances application hardening and process monitoring to catch and block malicious attempts.
   - Prevents access to malicious websites, bots, and PUPs.

2. Web protection
   - Provides real-time protection against known and unknown ransomware.

3. Exploit mitigation
   - Monitors and detects common attack vectors to mitigate exploit-based attacks.
   - Blocks known and unknown exploit-based attacks.

4. Application behavior protection
   - Prevents known and unknown malware from executing.
   - Blocks known and unknown malware campaigns.

5. Anomaly detection
   - Identifies viruses, malware, and PUPs with behavioral rules.
   - Prevents ransomware from executing.

6. Behavior monitoring
   - Detects and mitigates malicious scripts, macros, and malicious websites.
   - Protects against web injection attempts.

7. Payload analysis
   - Identifies and removes malicious and suspicious payloads.
   - Detects and removes malicious ADs.

One size fits none

The "one-size-fits-all" approach to antivirus is no longer sufficient. Malwarebytes Layered Protection technology uses next-gen computer security that empowers your firewall to protect your home or office from both known and unknown ransomware.

It's an arms race

79% of security professionals believe a security breach is inevitable today.

40% of businesses experience a security breach at least once a year.

Malwarebytes detected ransomware before it caused damage.

Layer up

The most effective way to counter the multiplicity of attack chains is to combine multiple technologies in your endpoint defenses. Some malware is now distributed using Microsoft Office document macros while exploit kits leverage banner ads on legitimate websites to deliver ransomware.

Back on the chain gang

Cybercriminals are constantly changing their methodologies and deployment vectors to fool your endpoint defenses. Some malware now becomes as dynamic as the malware itself.

Breaking the attack chain

Understanding the Depth of the Global Ransomware

Source: Osterman Research, August 2016.

So what if malware successfully executes? The Malwarebytes Endpoint Protection套件 uses behavioral heuristics to detect and block ransomware before it spreads on the endpoint.

Between IT teams and cybercriminals. It's an arms race.

Remote cleanup and restore, when and where you need it.

Interested in a free business trial? malwarebytes.com/business