BREAKING THE ATTACK CHAIN

See how Malwarebytes defeats multiple attack chains with seven different technologies.

It's an arms race

Between IT teams and cybercriminals. And guess who's losing?

79%

Businesses surveyed suffered a security-related breach in the previous 12 months.*

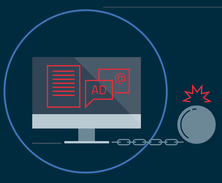
Source: *Understanding the Depth of the Global Ransomware Problem*, Osterman Research, August 2016.

One size fits none

The "one size fits all" signature-based approach to endpoint security used by traditional AV companies and single-layer technology used by some next-gen companies are getting businesses like yours in trouble every day.

40% Businesses surveyed were hit by ransomware in the last year.*

Source: *Understanding the Depth of the Global Ransomware Problem*, Osterman Research, August 2016.

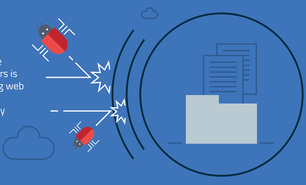


Back on the chain gang

Cybercriminals are constantly changing methodologies and deployment vectors to fool endpoint defenses. Some malware is now distributed using Microsoft Office document macros while exploit kits leverage banner ads on legitimate websites to deliver ransomware. The evolution of malware distribution is becoming as dynamic as the malware itself.

Layer up

The most effective way to counter the multiplicity of attack chains and vectors is through diversification. An interlocking web of matching and signature-less technologies work together to not only block malware execution, but its deployment on the endpoint.



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

1 Application hardening

Reduces vulnerability surface and proactively detects fingerprinting attempts used by advanced exploit-based attacks. **Especially effective against advanced exploit kits.**

2 Web protection

Prevents access to malicious websites, ad networks, scammer networks, and "bad" neighborhoods. **Especially effective against malvertising, phishing emails, botnets, PUPs, and malware servers.**

3 Exploit mitigation

Detects and blocks attempts to abuse vulnerabilities and remotely execute code on the endpoint. **Especially effective against exploit-based attacks.**

4 Application behavior protection

Prevents applications from being leveraged to infect the endpoint. **Especially effective against exploit-based attacks, spearphishing, and social engineering.**

5 Anomaly detection

Identifies viruses and malware proactively through machine learning. **Especially effective against zero-hour malware.**

6 Payload analysis

Identifies entire families of known malware using heuristic and behavioral rules. **Especially effective against new zero-hour variants of existing malware families.**

7 Behavior monitoring

Detects and blocks ransomware via behavior monitoring technology. **Especially effective against known and unknown ransomware.**

1ST

So what if malware successfully executes? The Malwarebytes Linking Engine removes the primary payload or infector and related artifacts. In a AV-Test.org test of the top 17 security products, Malwarebytes was the only one to completely clean and repair the infected machine.

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

Malwarebytes