Adding a sandbox stops almost 100% of malware from the web with URL filtering and antivirus. The remaining 20% is zero-day and reaches endpoints, requiring cleanup.

Most organizations block only 80% of malware from the web with URL filtering and antivirus. The remaining 20% is zero-day and reaches endpoints, requiring cleanup.

URL filtering and antivirus don’t stop zero-day malware from the web, leaving security teams overwhelmed and organizations at risk. A new approach is needed.

Adversaries know security technology—and avoid it with custom malware.

The web delivers more criminal malware than any other vector.

When malware gets through—expenses go up. 31 days at $20,000 a day for a large organization to clean up and remediate malware infiltration.

What could you do without the costs of cleaning up zero-day malware?

URL filtering and antivirus aren’t enough to stop zero-day malware from the web, leaving security teams overwhelmed and organizations at risk. A new approach is needed.

Adversaries know security technology—and avoid it with custom malware.

The web delivers more criminal malware than any other vector.

When malware gets through—expenses go up. 31 days at $20,000 a day for a large organization to clean up and remediate malware infiltration.

What can be done to stop malware from the web?

Adding in-line file and code emulation prevents zero-day malware, bringing the total to 99.5%.

McAfee Labs, Q2 2016
Verizon’s 2015 Data Breach Investigations Report (DBIR)
Verizon’s 2016 Data Breach Investigations Report (DBIR)
2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2014
McAfee performance testing. Actual figures will vary in individual organizations.

Change to: McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC.