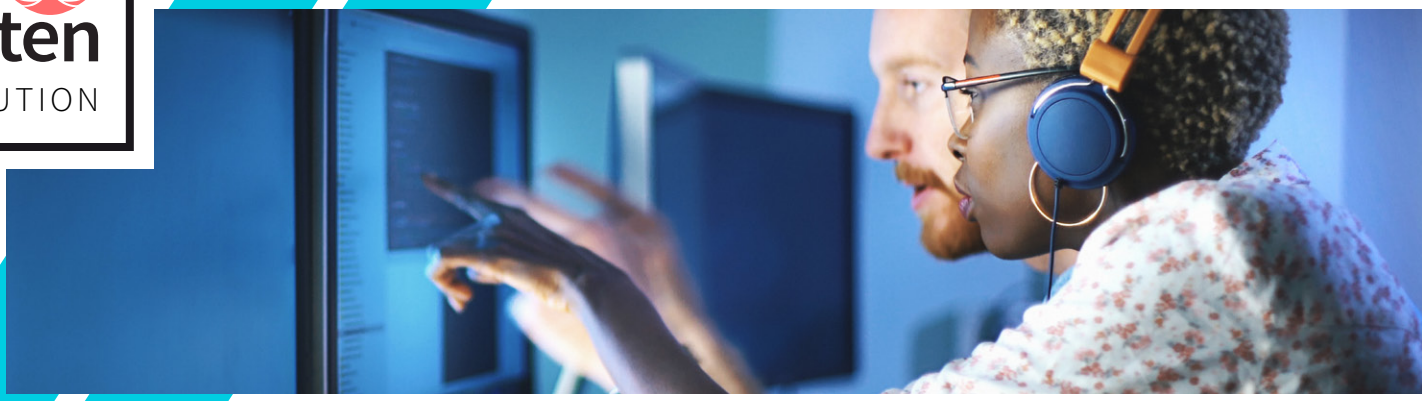
ziften SOLUTION



SOLUTION BRIEF

Multi-Vector Protection, Built from AI

Proprietary algorithms detect multiple attack vectors to prevent file-based, fileless, and in-memory attacks before system infection and damage can occur without daily signature file updates.

Attackers love your endpoints. And they'll use any way they can to gain access to these critical assets. And why not, traditional antivirus (AV) won't stop attackers. And let's face it, users aren't great at patching and even sometime disable the security controls. But with Ziften Zenith endpoint protection you can stop file-based, fileless and in-memory attacks with the power of the cloud and artificial intelligence (AI).

Stop Known File-Based Malware

Can you use Zenith to replace your existing AV? You bet you can. With Zenith's Advanced AV capability, you can intercept and prevent attacks before they can execute, eliminating or at least minimizing the need for post-infection investigations, forensics, and incident response.

But stopping known file-based malware is not enough against determined attackers.

Block Unknown and 0-Day Malware

Most malware in use today uses new variants to get around traditional AV signatures. And when these new cyber-attacks first show up, it can take 2 weeks for security solutions that rely on signatures and heuristics to recognize and block them. This "Protection Gap" is unacceptable.

Ziften's AI-based endpoint protection improves threat detection by learning to recognize the basic, general features of malicious code, rather than looking for specific kinds

of threats. In this way, we can detect and block never before seen threats, preventing unknown and zero-day malware attacks with no need for rigid heuristics, out of date signatures, or rudimentary “on/off” control features.

Don’t expose your enterprise endpoints to the traditional endpoint “Protection Gap”.

Prevent Fileless Attacks

But that’s not all. More and more, attackers are moving to fileless based attacks. In fact, a recent study found that 77% of successful breaches involved the use of some type of fileless attack. So let’s get beyond only stopping file-based malware.

Ziften’s proprietary algorithms detect and prevent multiple attack vectors including fileless weaponized documents, script and macro-based attacks, and in-memory attacks before system infection and damage can occur. These are all fairly tricky attacks that are designed to circumvent the protections of traditional endpoint security, but Ziften’s AI-based endpoint protection is able to prevent these threats from breaching an organization.

Ziften helps you get beyond traditional endpoint protection and ahead of attackers.

The Ziften Zenith difference is clear.