



SOLUTION BRIEF

Endpoint Protection that Works Anywhere

Ziften Zenith maintains endpoint protection plus visibility when endpoints are on-the-network, off-the-network, or completely offline.

We live in a highly mobile world. The days of work being contained to “9-to-5 at the office” are now pure nostalgia. Today’s reality is that employee and contractor machines are in use anywhere, anytime – corporate office, home office, local coffee shop, airplanes and hotels. And, since those endpoints can run into security or operational issues anywhere, it stands to reason you need the same endpoint protection, visibility, tracking, and control capabilities – regardless of whether the user is down the hall, or half way around the world.

While some endpoint protection platforms only work when the employee is connected to an internal network domain, Ziften draws no such artificial boundaries. Protection plus visibility for endpoints on-the-network, off-the-network, and even offline.

Endpoints On-the-Network

The first and most obvious location is when the endpoint is directly connected – wired, wireless, or via VPN – to a corporate network domain. This scenario is straightforward and affords full Ziften protection, visibility, and control.

Endpoints Off-the-Network

Second is when the endpoint is connected to the Internet in an off-premises environment. In this scenario, Ziften steps beyond other endpoint protection platforms and retains full protection, visibility and control through the Zenith endpoint agent. Full and continuous endpoint protection, streaming visibility, and remote access to the machine is fully preserved. No compromises.

Endpoints Offline

Zenith still works even if the endpoint in use is not connected to the Internet. In this scenario, it is obvious there is no way to query from afar or push any type of communication or instruction out. However, with Ziften, the Zenith agent can still provide local threat prevention and detection, and all monitoring functions are cached locally meaning full data capture is still intact. The moment the machine reconnects to a network – either a corporate domain or the Internet – all visibility data is uploaded and full visibility and control functionality immediately ensues.

With Ziften, security operations teams always have the most effective endpoint protection plus visibility and control possible no matter where the endpoints reside or their “state of connectedness”.

The Ziften Zenith difference is clear.

Endpoint Protection that Works Anywhere

