EDR is Not Enough.

Stop Responding. Start Preventing.

deep instinct™
www.deepinstinct.com

Background

EDR tools have become popular based on the perception that they can stop and remediate a wide range of cyber threats. But EDR tools have proven to be not enough to prevent today's sophisticated attacks — a point driven home by the skyrocketing frequency of damaging breaches. EDR tools are *not* the only answer to defend against advanced attacks.

8 Reasons Why EDR is Not Enough

1. "Assume Breach" mentality is flawed.
2. EDR is a reactive approach.
3. EDR is not winning against ransomware.
4. EDRs produce high false positives.
5. ML weaknesses lower EDR's efficacy — and can be exploited.
6. EDR is only as good as its visibility across every endpoint.
7. EDR blocks post-execution, it doesn't prevent pre-execution.
8. XDR only makes EDR less effective.

Learn why fresh thinking around EDR tools is overdue.

Read our free eBook: 8 Reasons Why EDR is Not Enough.