SentinelOne

6 Things Your NGEP Must Do

Looking at Next Gen Endpoint Protection? Here are 6 Must-Haves

1

Known Attack Detection

Couple known threat intelligence with additional security layers to preemptively stops known threats and bad sources before they execute. Your NGEP must...

Use cloud intelligence to keep it lightweight

Uses a collection of reputation services rather than one vendor's

2

Dynamic Exploit Detection

Hackers often use exploits to target code-level vulnerabilities so they can breach systems and execute malware. Drive-by downloads are a common vector for carrying out exploit attacks. Your NGEP must...

Detect exploits to prevent application & memory-based attacks

Detect exploit techniques rather than using static methods

3

Advanced Malware Detection

As thousands of variants are created each day, your security must prevent unknown malware and targeted attacks - even those that do not have static indicators of compromise. Your NGEP must:

Monitor behavior of OS activities and processes

Look at the full execution context

Detect attacks whether device is on or offline

4

Mitigation

Detecting threats is necessary, but with detection only, many attacks go unresolved for days, weeks, or months. Your NGEP must:

Provide automated mitigation during the attack inception stages

Provide policy-based options covering many use cases

5

Remediation

During execution, malware often creates, modifies, or deletes system file and registry settings and changes configuration settings. These changes, or remnants that are left behind, can cause system malfunction or instability. Your NGEP must:

Restore an endpoint to its pre-malware, trusted state

Log what changed and what was successfully remediated

6

Forensics

Since no security technology claims to be 100% effective, the ability to provide real-time endpoint forensics and visibility is a must to be able to take steps. Your NGEP must:

Provide clear and timely visibility into malicious activity organization-wide

Give a real-time audit trail of what happened during an attack