NeuShield®

How much is your data worth?

Beyond EDR

COST EFFECTIVE PROTECTION AND RECOVERY BEFORE MALWARE INVASION

© 2024. All rights reserved. NeuShield, Mirror Shielding and Data Engrams are trademarks of NeuShield, Inc.
All other trademarks and registered trademarks are the properties of their respective holders.

Cost Effective Protection and Recovery Before Malware Invasion

Endpoint security has evolved over decades from primitive antivirus software to more sophisticated next-generation platforms, Endpoint Detection and Response (EDR). Multiple incidents have shown that EDR can be evaded, calling for real- time data protection tools that complement EDR in the battle against cyber criminals.

TEST OUR RANSOMWARE PROTECTION PROMISES WITHOUT OBLIGATION.

For questions about this paper and to find out more about how NeuShield works:
Sales@neushield.com or call **+1 510-239-7962**

© 2024. All rights reserved. NeuShield, Mirror Shielding and Data Engrams are trademarks of NeuShield, Inc. All other trademarks and registered trademarks are the properties of their respective holders.

EDR Purpose

Gartner states that EDR must provide the following four primary capabilities:

1. Detect security incidents.
2. Contain the incident at the endpoint.
3. Investigate security incidents.
4. Provide remediation guidance.

Many of the security vendors in Image 1 market themselves as effective EDR offerings, including those not represented in Gartner's EPP Magic Quadrant[1] that profess to offer a leading EDR tool but in fact only include limited EDR capabilities.

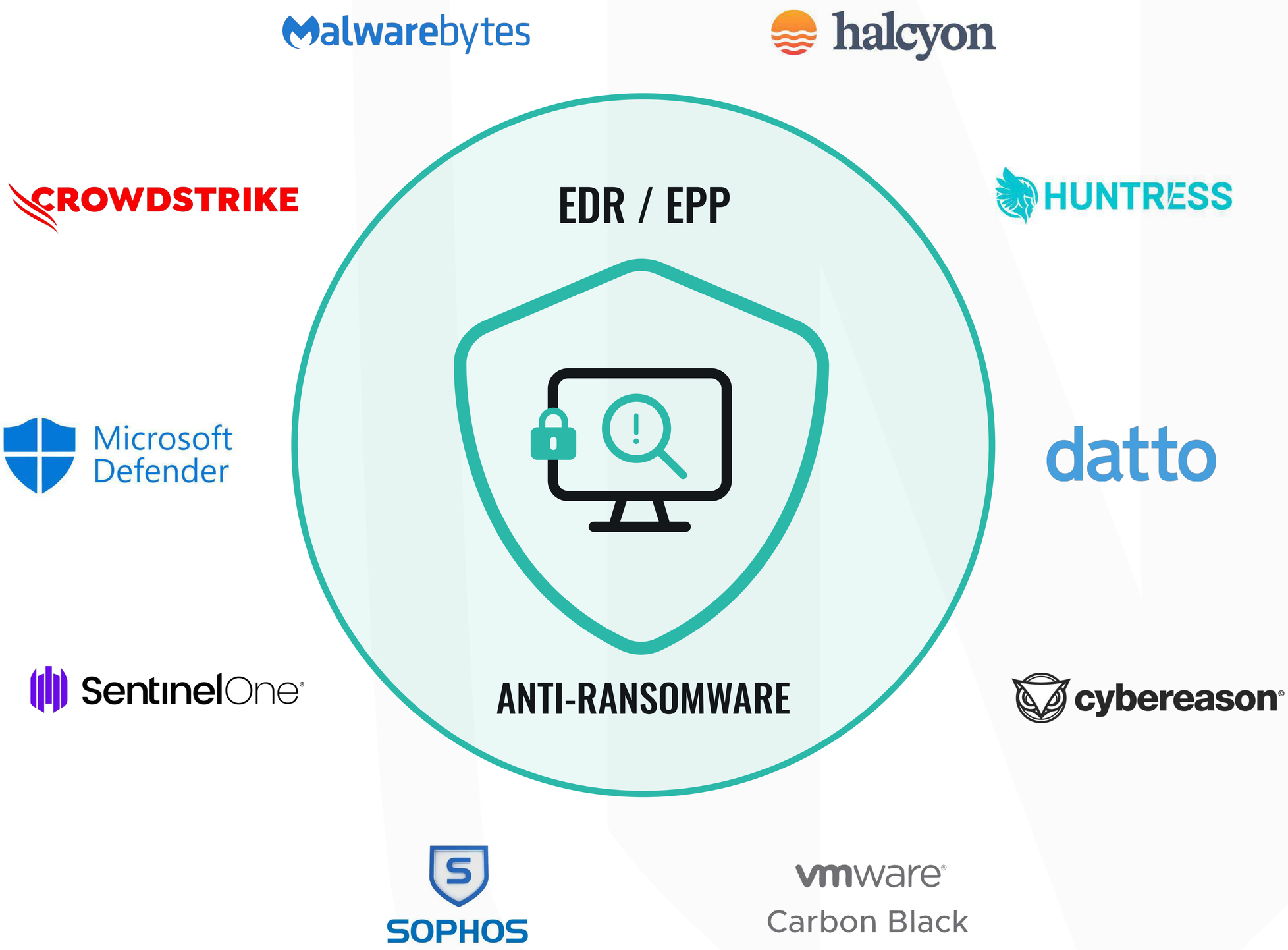


IMAGE 1 - EDR & ANTI-RANSOMWARE VENDORS:

Some vendors in Image1 stretch reality in their marketing messaging to promote their awareness and consideration for specific malware or anti-ransomware detection and remediation.

[1] Gartner, Magic Quadrantfor Endpoint Protection Platforms, 31 December2023, Evgeny Mirolyubov, Max Taggett, Franz Hinner, Nikul Patel.

© 2024. All rights reserved. NeuShield, Mirror Shielding and Data Engrams are trademarks of NeuShield, Inc. All other trademarks and registered trademarks are the properties of their respective holders.

Defense in Depth

Unfortunately, even with the latest EDR products deployed, hackers still breach organization's defenses, causing chaos and operational disruption.

Complementary tools - from EDR and niche malware/ anti-ransomware providers - attempt to fill gaps using other external or mitigation offerings when the primary EDR product has been evaded.

WINDOWS VOLUME SNAPSHOT SERVICE (VSS)

EDR providers include this as a bolt-on feature to help recover compromised data. It is not a core part of an EDR function. Unfortunately:

- VSS is not part of your 3-2-1[2] policy that caters for data recovery.
- VSS can consume vast [additional] amounts of storage 'just in case' of an incident.
- VSS is limited in the amount of data it can backup (in its settings or physical hard disk). If the user has 100GBs of data and only 30GBs of free space, when 100GB is unlawfully encrypted, 30GBs would not be sufficient to recover all the data.
- Recovery using VSS is only viable if a) the malware is blocked, and b) the malware has encrypted data in-part or fully prior to being blocked.

ENCRYPTION KEY CAPTURE

The software claims to capture the decryption key and deliver immediate decryption defense. Unfortunately:

- These products are not EDR tools. They respond after the data is compromised.
- Even if the product is able to capture the key, decrypting the encrypted data is slow.
- Ransomware may only perform partial file encryption. Having the key is not enough to decrypt, you need to know what part of the file was encrypted.
- Symmetric encryption (single shared key) may expose the decryption key, but smart hackers may utilize asymmetric encryption.
- As with EDR programs, if the Encryption Key Capture software cannot detect the threat it may not be able to capture the decryption key.

WRAPPING CYBER WARRANTY

Incident remediation can cost $100k - $millions to re-establish your operations. EDR and other security product vendors wrap Cyber Warranty and Insurance policies promising $1m-$5m to help recover mitigation costs. Unfortunately:

- This does not negate the chaos and disruption during an attack or protect infrastructure and data.
- Policy exclusions restrict payouts to specific effected devices, invalidating claims if the incident was not directly targeting the company or is not the cause of the security vendor's product providing the warranty/insurance coverage.
- Existing cyber insurance policies may invalidate any product wrapped warranty coverage.

[2] https://www.synergysixd.com/Results - Is 3-2-1 still fit for purpose in today's "always available" world?

© 2024. All rights reserved. NeuShield, Mirror Shielding and Data Engrams are trademarks of NeuShield, Inc. All other trademarks and registered trademarks are the properties of their respective holders.

Active Data Defense: NeuShield + EDR

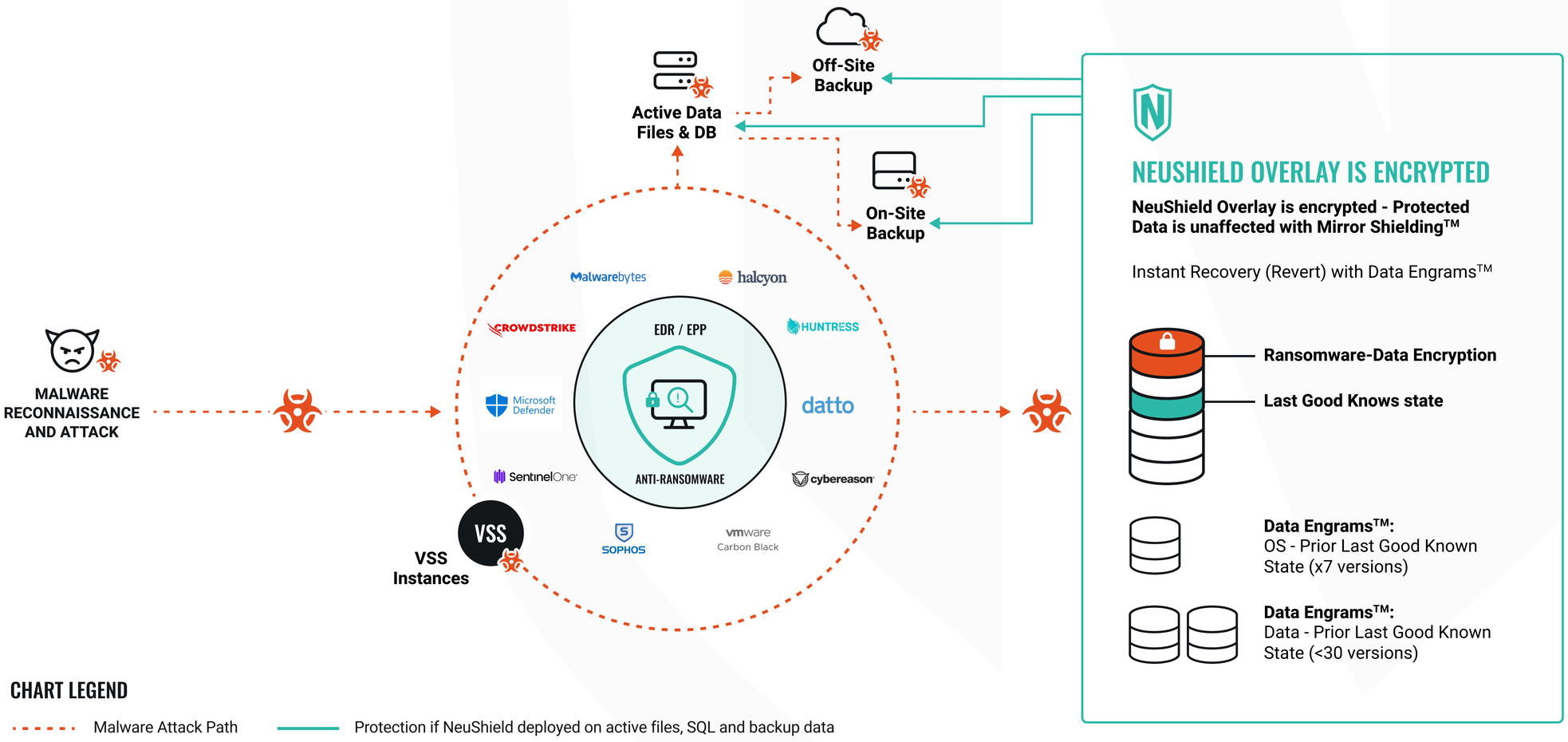
EDR products depend on malware engines[3], using signatures, AI, and machine learning to detect malware, such as: SamSam, REvil, RagnarLocker or fileless malware, such as: Cobalt Kitty, Ursnif, Sodinokibi.

NeuShield should never be considered an EDR. That said, although NeuShield has no requirement for a malware engine, its value comes from the file validation and verification checks performed. At the time data is written to the NeuShield Overlay it will be immediately checked for validity. The IT administrator will be alerted to suspicious data file modifications, such as encryption.

NeuShield protects your active data in real-time using its patented Mirror ShieldingTM and Data EngramsTM technology. NeuShield's architecture employs an Overlay barrier for data on every device of operation. Mirror ShieldingTM is an impenetrable defense that protects active data from compromise when other security tools have been evaded. NeuShield complements EDR as your 'last line of defense' against data compromise.
NeuShield can always recover compromised data and OS even if the threat is not detected or not detectable (file or fileless malware and Zero-day attacks).

NeuShield's recovery is achieved 99% faster than current techniques at no additional cost (see our report referenced below). Remediation is a simple process that deletes the compromised data on the Overlay and immediately reverts (recovers) the protected data from an appropriate Data EngramTM to its 'last known good state'. This is possible without the need to use your backups.

DETECTION AND RESPONSE (BLOCK, DETECT & RECOVER)



[3] EDR vendors use multiple engines, which will be a combination of their own plus that of other security vendors to increase their detection capabilities.

READ OUR REPORT

How NeuShield can supercharge existing backup strategies'.

© 2024. All rights reserved. NeuShield, Mirror Shielding and Data Engrams are trademarks of NeuShield, Inc. All other trademarks and registered trademarks are the properties of their respective holders.

NeuShield®
How much is your data worth?

Contact us today to actively protect your data and deliver instant recovery. Re-establish operations faster without additional costs.

NeuShield Data Sentinel does more than just detecting and blocking ransomware. We're the only anti-ransomware solution that can recover encrypted data from any known, unknown or zero-day threat. No matter how much data is encrypted NeuShield can get it back instantly from any laptop, desktop or server. NeuShield is an endpoint agent that works locally to recover data without using a backup or internet connection.

sales@neushield.com

NeuShield, Inc
200 Brown Road, Suite 306
Fremont, CA 94539
Main: +1 510-239-7962
Toll Free: +1 888-999-0965 (U.S.)

WWW.NEUSHIELD.COM