SOLUTION BRIEF

Absolute Endpoint Data Discovery

Seamlessly identify at-risk data residing across your endpoints

With the emergence of work-from-anywhere, breaches of sensitive corporate and customer data have been on the rise. Given the reduced visibility and control IT teams face, it's challenging for them to enforce data security policies effectively across their remote endpoints. Although every endpoint represents a potential target for cybercriminals, those containing sensitive data—such as Personally Identifiable Information (PII) and Protected Health Information (PHI)—pose a more serious threat. If a device containing such information is compromised, the potential damaging implications to the organization multiply exponentially.

How big of an issue is this? One might think that this information is highly restricted to a limited number of devices. Unfortunately, that assumption is misguided. Since workforces are now highly distributed, mobile workers are consistently connecting into various databases containing sensitive information from a variety of locations and networks. This inherently increases the likelihood of workers storing data locally (on the endpoint itself). This locally stored sensitive data increases the potential attack surface. **Absolute's analysis** found that more than three fourths (76%) of enterprise devices contained sensitive data, on average.

Challenges Identifying Sensitive Data

Typical challenges IT teams face in identifying and protecting at-risk data include:

- Accumulation of sensitive files containing corporate or customer data on endpoints, thereby heightening the organization's data risk exposure.
- Remote endpoints going dark periodically, thereby limiting visibility to stored sensitive data.
- Employees being lax in their usage of work devices by storing personal files or PII.
- Identifying and protecting sensitive corporate data such as intellectual property (IP) being stored on devices used by external parties, contractors, or consultants.
- Inability to reliably enforce data protection policies across remote devices due to lack of visibility and control.
- Legacy data loss prevention (DLP) tools being either ineffective or arduous to set up correctly in a remote environment.

IT and security teams today are expected to keep a handle on the accumulation of sensitive files across their remote endpoints. Many industry standards and government regulations (e.g., PCI DSS, HIPAA, CCPA, GDPR) set stringent guidelines when it comes to the handling of sensitive data. Thus, not being able to identify any potential risk exposure can lead to major audit gaps, data leaks, and massive financial repercussions.

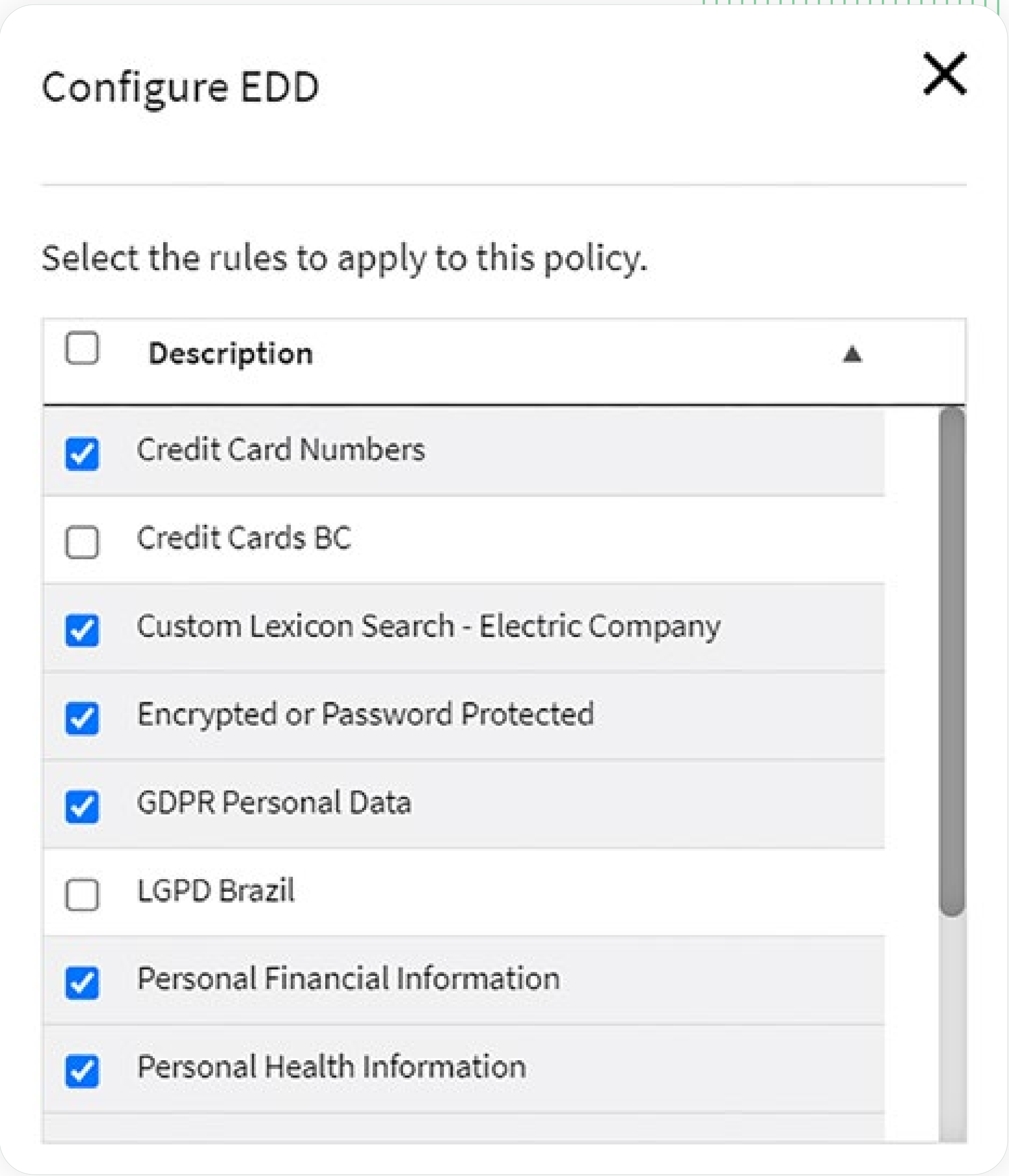
Remote Identification of Sensitive Files Across Your Devices

The first step in protecting sensitive data is to proactively identify where it resides. Absolute Endpoint Data Discovery enables IT and security teams to seamlessly track the accumulation of sensitive files across their remote endpoint environment.

Absolute Endpoint Data Discovery allows you to set policies to scan your managed devices for data-at-risk — either periodically or on demand, thereby providing reliable data visibility across your devices to monitor and ensure your organization's data risk exposure is below an accepted threshold.

Key Capabilities

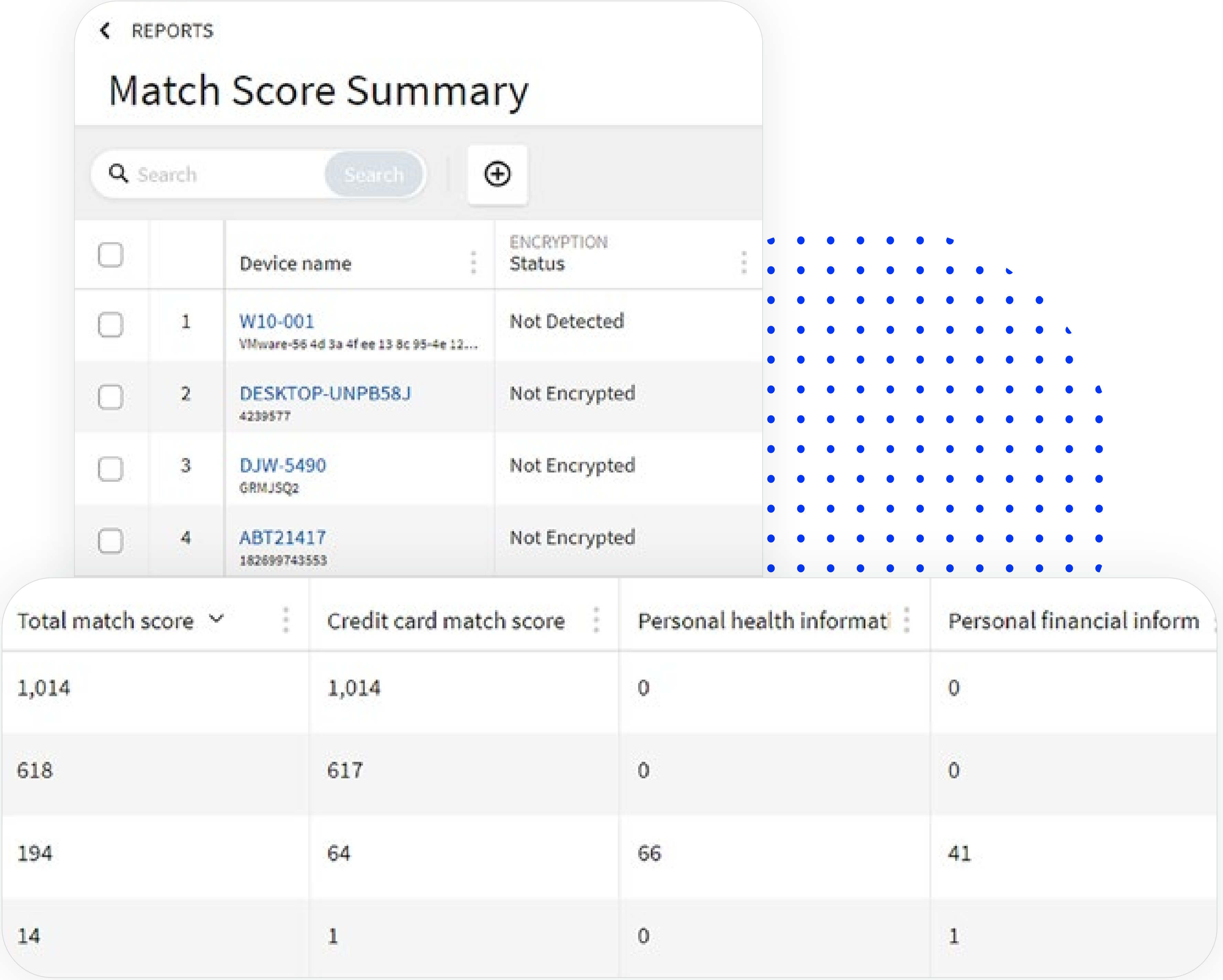
- Seamlessly scan for sensitive personal, corporate, or customer data across your endpoint fleet.
- Leverage pre-built rules or build custom ones to identify files containing specific keywords such as social security numbers, health terms, financial terms, or intellectual property among others.
- Run full scans when required or periodic delta scans to limit the impact on the end user experience.
- View integrated and customizable reports through the Absolute Console to assess your organization's data risk exposure and identify potential compliance gaps with regulations by frameworks such as GDPR.
- Once at-risk data is identified, utilize security actions available through the Absolute Console such as Device Freeze and/or Data Delete to mitigate the risk.



Configure EDD

Select the rules to apply to this policy.

☐	Description ▲
☑	Credit Card Numbers
☐	Credit Cards BC
☑	Custom Lexicon Search - Electric Company
☑	Encrypted or Password Protected
☑	GDPR Personal Data
☐	LGPD Brazil
☑	Personal Financial Information
☑	Personal Health Information



< REPORTS

Match Score Summary

Search Search ⊕

□		Device name	ENCRYPTION Status
□	1	W10-001 VMware-56 4d 3a 4f ee 13 8c 95-4e 12...	Not Detected
□	2	DESKTOP-UNPB58J 4239577	Not Encrypted
□	3	DJW-5490 GRMJSQ2	Not Encrypted
□	4	ABT21417 182699743553	Not Encrypted

Total match score	Credit card match score	Personal health informat	Personal financial inform
1,014	1,014	0	0
618	617	0	0
194	64	66	41
14	1	0	1

Key Benefits

- Proactively monitor at-risk data accumulated across remote devices to ensure your organization's risk of data exposure is minimized.
- Ensure adherence with industry standards or regulatory mandates (e.g., GDPR, HIPAA, and CCPA).
- Protect sensitive data such as PII, corporate IP, customer order details, financial information, and health records from falling in the wrong hands.
- Avoid unnecessary and exorbitant financial penalties and reputational damage that result from a data breach or data leak. Maintain the trust of your customers, partners, and key stakeholders.

Getting Started

For more details about Absolute Endpoint Data Discovery, please check out the **Absolute Endpoint Data Discovery FAQ**. Absolute Endpoint Data Discovery is available with all Absolute Secure Endpoint service tiers (Absolute Visibility, Control and Resilience).

ABSOLUTE®

Trusted by nearly 21,000 customers, Absolute Software is the only provider of self-healing, intelligent security solutions. Embedded in more than 600 million devices, Absolute is the only platform offering a permanent digital connection that intelligently and dynamically applies visibility, control and self-healing capabilities to endpoints, applications, and network connections — helping customers to strengthen cyber resilience against the escalating threat of ransomware and malicious attacks.

Request a Demo

Nasdaq | ABST   TSX | ABST