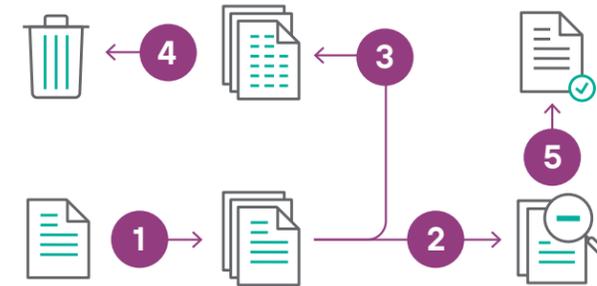


How Zero Trust CDR Can Boost Your Current Cyber Defenses

Is malware still getting through your defenses? Find out how you can stop it for good!

How does it work?



1. Rather than identifying known malware, Zero Trust CDR takes the data and extracts the useful information from it.
2. The extracted information is transformed into an intermediary format and verified.
3. This advanced threat protection process makes sure no threats or attacks can reach the next stage.
4. The original data is stored or discarded along with malware, known or unknown.
5. Brand new data is then built in a normalized way, containing the verified information. The new data replicates the original data, without the threat of embedded malware and is now guaranteed safe.

Anti-malware defenses must:

- › Always deliver safe and fully functional content so users can have utter confidence in the files they receive from outside the organization.
- › Stop zero-day threats without the need for the latest patches or signatures to shore up the defense.

Attack vectors to protect:

Web browsing	Web downloads
Web mail	Social media
File uploads	Mail
Web applications	File sharing

Deployment options

	Built into applications AX ↓	Web browsing Upload and Download GX ↓	Email and File Transfer IX ↓
Setup	seconds	minutes (<60)	hours (<2)
Delivery	API key & example code	virtual machine software & integration guide	virtual machine software & setup instructions
Customer	use example code & API key to clean data	install & connect to a supported forward or reverse proxy	install & clean files, emails or web services

It's time!

It's time to pivot from detection to prevention. Many detection-based defenses still let malware in. Forcepoint Zero Trust CDR makes incoming files and data safe without using detection, preventing attacks and ensuring you are protected from the latest threats.

Zero trust, zero hassle

Enhance user experience without compromising on security. With no delays for scanning or sandboxing, **Zero Trust CDR delivers threat-free, pixel perfect, fully revisable and usable files and data to users in near real-time.**

Highly versatile

Zero Trust CDR works with your existing security estate. Add it your boundary defenses to ensure a wide range of files and data flows including the Office files, images and PDFs favoured by attackers are threat-free.

Choice of deployment

Choose from on-premise, virtual and cloud-native deployments and for unparalleled protection and peace of mind.

- ✔ Malware free data
- ✔ Zero false positives
- ✔ Zero latency
- ✔ Stop zero-day threats
- ✔ Free up the SOC team
- ✔ Enhance user experience
- ✔ Quick & simple installation
- ✔ Pixel-perfect, fully revisable files

Forcepoint

forcepoint.com →