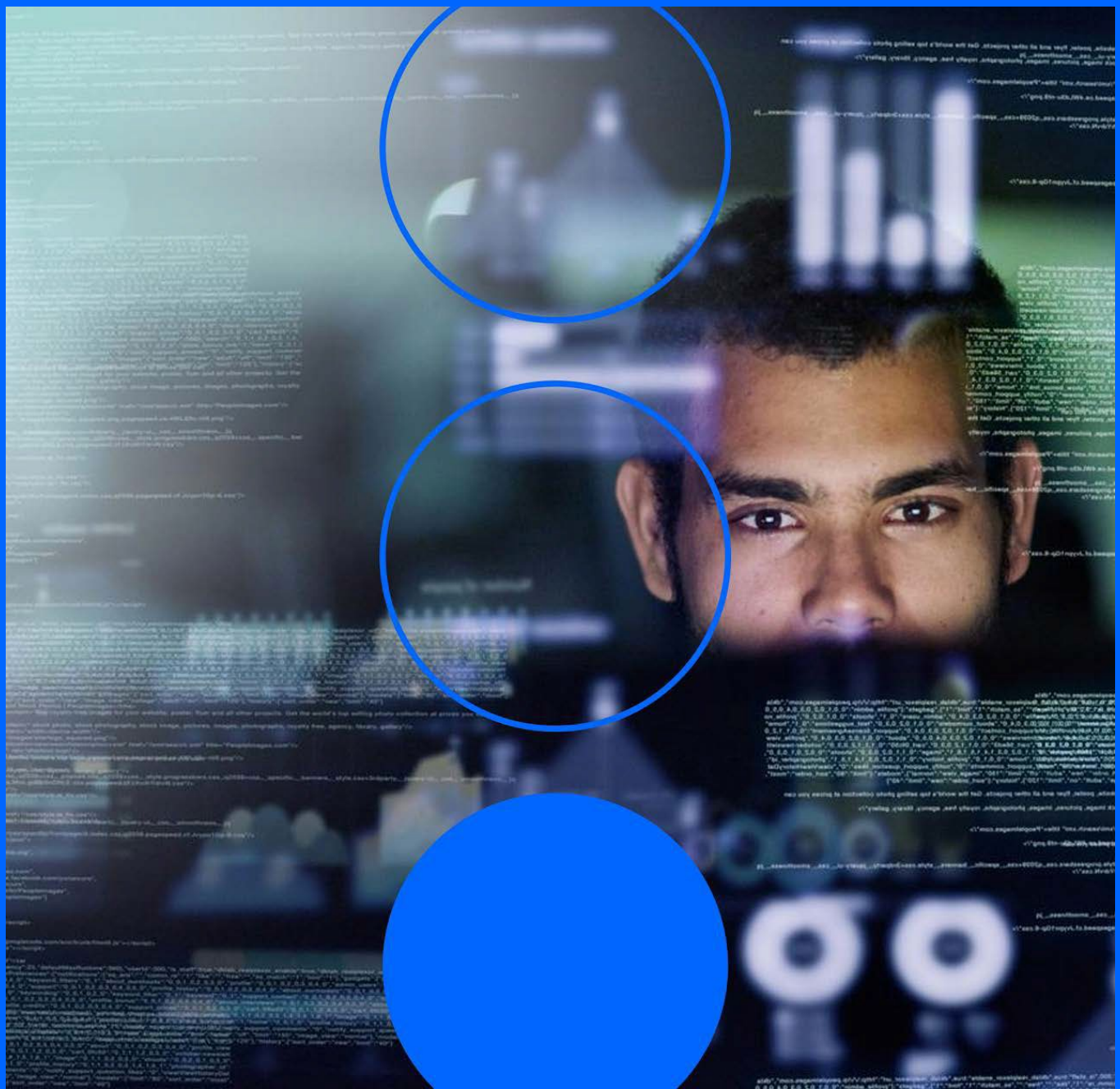
Telefónica Tech

APPGUARD®

Achieve Zero Trust Endpoint/Server Protection



APPGUARD

Prevention without detection

Prevent zero-day threats, vulnerabilities and application exploits from harming your business

Modern Endpoint (and server) Detect and Response (EDR) technologies focus on identifying threats through signatures, scans and behavioural algorithms, incorporating machine learning and AI in an attempt to defeat cyber criminals.

They parse infinite possibilities, requiring more tools, more personnel, and more skills every year. EDR relies upon monitoring and investigating vast, diverse volumes of detection and indicator data from multiple perspectives at multiple stages of malware attacks: before and after compromise.

And those who think machine learning will help them scale are finding that the single most pervasive characteristic in enterprise IT , '**change**', is also machine learning's greatest adversary.

Having a 99% detect rate sounds impressive. Yet with over a billion pieces of malware in circulation, it would still mean millions of potential threats going unchallenged. Because of this, relying on detection alone no longer works. A far different approach is needed, one that uses zero trust principles at its heart to protect core assets and company data, ensuring the effects of breaches on endpoints and servers are nullified.

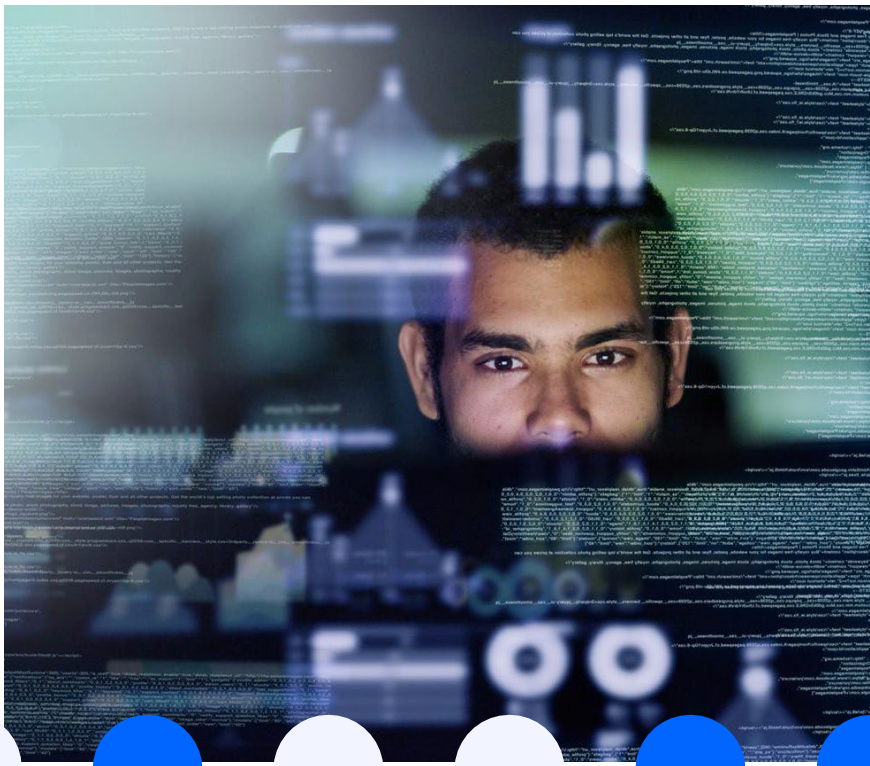
AppGuard's Approach

Rather than trying to scale to parse more, AppGuard's zero trust for endpoint takes the opposite approach: drastically reducing what needs to be monitored and analysed.

It does this by avoiding the predicament of telling "good" from "bad" and "normal" from "abnormal" by instead blocking those actions malware needs to take to execute.

This replaces analysing an infinite amount of data with suppressing hundreds of actions within an endpoint that years of industry research have revealed are necessary for adversaries to attain their goals.

With AppGuard, malware recognition is not required. Alternatives only succeed when they are able to recognise every piece of malware.



APPGUARD

AppGuard's Approach

Data security and governance has never been higher up the agenda. AppGuard provides the missing piece of the operational resilience jigsaw, ensuring that if threat actors bypass all detection technology and methodologies, application vulnerabilities cannot be exploited and the effects of malware are neutralised.

AppGuard potentially reduces insurance premiums. Some clients adopting AppGuard have questioned the need for it at all. Why? By taking AppGuard into your infrastructure, you are saving any potential costs associated with trying to recover from the effects of a breach: be they downtime, loss of custom, reputational damage, or recovery related. Their view being – it's better to spend money preventing an attack happening in the first place, than trying to mitigate the costs of a breach.

Prevention without detection

Failed conformance controls such as whitelisting, HIPS, and sandboxing require too much endpoint state information that needs to be revised following changes such as application updates/patches.

AppGuard's zero trust for endpoint approach is based on patented higher abstractions that simplify policy formulation and automatically adapt to lifecycle changes. For example, app containment begins with its parent executable and automatically extends to any resulting process from the app's operation. This means very little state information is required for policy formulation, and updates/patches do not necessitate policy updates. Further, it accounts for the unanticipated.

Containment is enforced uniformly to all at-risk apps, avoiding the app-specific policy dilemmas of alternatives.

Customers praise AppGuard's real-time protection effectiveness. Endpoint zero trust defeats malware without having to detect it, resulting in better protection and fewer operations. Other cyber defence layers see substantially lower alert volumes because malware attacks are stopped at endpoints in real time.

APPGUARD®

The Endpoint Zero Trust Approach

Key Features

Use Case	How zero trust mitigates risks & accomodates legitimate use
Unpatched app or zero-day exploit	Does not allow an app or any process it spawns to install malware or steal/alter the memory of other app/OS processes. This alleviates patch/vulnerability management pressure. For AppGuard, containing an app is as simple as adding a song to a playlist.
Drive-by download	Scripts and executables are not allowed to launch unless proven trustworthy via validated digital signature or other means; those allowed to launch are not allowed to do harmful actions.
Server with mission-critical app has mysterious, malicious process running	Any malware that somehow gets onto a server cannot read/write the memory, directories, executables, or data files of the “isolated” mission- critical app. IT/Sec-Ops can usually safely run the app until a maintenance window.
Pass-the-hash/ticket attacks	Blocks credential thefts by granting access to trustworthy processes only. No IT/Sec-Ops actions are required; eliminates alerts that other tools would otherwise make.
Non-malware attacks	Prevents unauthorized actions by built-in tools yet allows limited use by end-users and full-use by IT/Sec-Ops. This requires fewer than a dozen deployment-specific policy rules that rarely require adjustment later.
Code injection attacks	Blocks clearly untrustworthy app process changes and ensures the app’s processes cannot do harmful actions in case they ever do run malicious code. Spares IT/Sec-Ops from the false-positive/negative quagmires of behavior analytics and other tools.
Remote code execution attacks from other endpoints	These built-in capabilities (e.g., Remote PowerShell, PsExec-like, SSH/shell, etc.) are locked/unlocked to ensure only IT/Sec-Ops can use them on demand, even if adversaries somehow steal elevated privilege credentials.

About Telefónica Tech

Telefónica Tech is the leading company in digital transformation. The company offers a wide range of services and integrated technological solutions in Cyber Security, Cloud, IoT, Big Data and Blockchain.

With our worldwide presence and strategic hubs in Spain, Brazil, the UK, Germany, and Hispam, our capabilities reach more than 5.5 million B2B customers in 175 countries every day.

We unlock the power of integrated technology for all businesses, bringing together a unique combination of the best people, with the best tech and the best platforms, supported by a dynamic partner ecosystem and strategic agreements with all market leaders. We do this in a simplified manner, to facilitate and accelerate tech adoption and make a real difference every day, to every business.

Telefónica Tech
We're here to **help**.

Visit **telefonicatech.uk** for more information.

@TefTech_EN Telefónica Tech Telefónica Tech

About Telefónica Tech

Telefónica Tech UK&I is a key holding of the Telefónica Group. The company offers a wide range of integrated technology services, reaching more than 5.5 million customers in 175 countries every day.