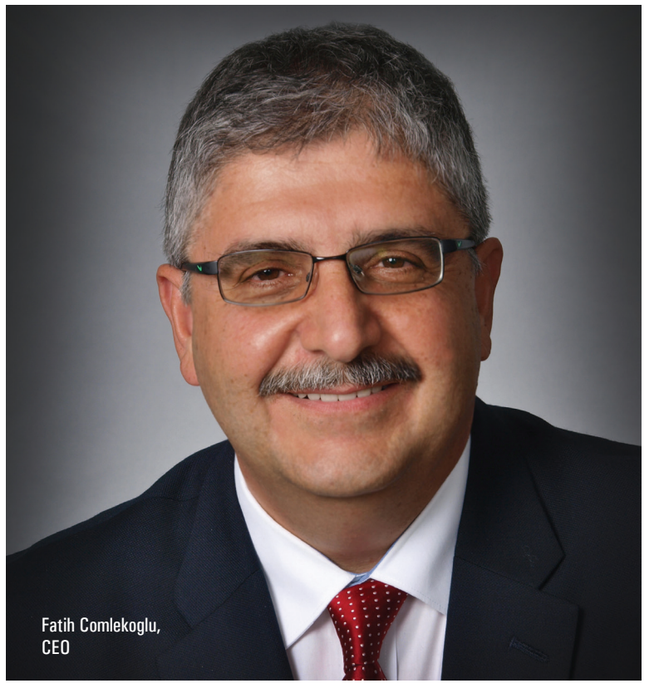
ZERO TRUST ENDPOINT SECURITY
SOLUTION COMPANY OF THE YEAR 2024

AppGuard®

Securing Endpoints Via Compartmentalization Within


Fatih Comlekoglu, CEO

The firm's security can be compared to national defense, where endpoints represent vulnerable border forts—far from the capital's protection and the first to be breached. This analogy highlights that an enterprise network cannot be secure without securing its endpoints.

AppGuard® addresses this issue by transforming each endpoint into smaller, compartmentalized fortifications. The approach turns a single target into a robust stronghold, creating multiple barriers that stop attacks in real-time, which detection-based defenses either miss entirely or detect too late.

COMPARTMENTALIZATION COMPLETES ZERO TRUST ARCHITECTURE (ZTA)

Most cyber incidents and breaches originate at the endpoint. AppGuard applies compartmentalization within endpoints to implement ZTA at a micro-level for an enterprise. Turning endpoints into well-fortified strongholds against malware attacks ensures the safety of the broader organization.

"AppGuard is controls-based endpoint protection software that avoids the chronic shortcoming of detection-based endpoint protection software, which strives to tell bad from good. Instead, AppGuard compartmentalization does not allow malware to do what it needs to do. Hence, AppGuard stops attacks without having to recognize the malware itself, making it the ideal complement to detection-based defenses," says Fatih Comlekoglu, CEO of AppGuard.

Applying ZTA principles to each computing process restricts what can run and what the running can do. It also has a macro effect on the entire enterprise network. Stopping what detection-based defenses miss at the endpoint in real-time alleviates the pressure across the cyber stack, decreasing operating expenses and vastly reducing incident response alerts. It also reduces remediation work, such as restoring endpoints to a pre-attack state and resetting credentials.

SECURITY THROUGH CONTROLS BASED PROTECTION

AppGuard compartmentalization is implemented through three fundamental controls: launch, contain, and isolate. Through the launch control, untrustworthy executables, script files and/or dynamic link libraries cannot launch or load. The compartmentalization of high-risk applications restricts what they can do to the rest of the host. Isolation controls protect select, important parts of the host from the rest of the host. Many malware techniques fail because AppGuard containment or isolation prevents malware from adding or altering something. It's a default deny approach.

To allow legitimate system changes, AppGuard allows for select IT tools to be designated as power apps. This ensures that AppGuard won't interfere when users install software, patch applications, or make other necessary system changes.

CONTAINMENT ALLEVIATES PATCH MANAGEMENT FAILURES

Attackers prowl for unpatched or unpatchable (aka, zero-day exploits) application vulnerabilities. By exploiting them, they can hijack an application to perform extremely harmful actions, such as downloading malicious files, injecting malicious code into memory and/or instructing operating system utilities to execute malicious instructions.

One common example is hijacking an application and using a process hollowing technique where malicious code is injected into a common application. So, while it might look generic on the surface, it's a Cobalt Strike Beacon™ that gives the adversary remote access to the endpoint with a library of hundreds of malicious tools to do great harm. AppGuard's compartmentalization principles shine in this scenario. It restricts what vulnerable applications can do, blocking potentially harmful actions.

USABILITY VS. SECURITY; PRAGMATIC VS. IMPRACTICAL

AppGuard respects the balance between usability and security.

"When a user's activity is hindered by a security tool, an enterprise would either under-utilize it or uninstall it. We make tradeoffs based on risk and usability. We do not strive to replace all other endpoint protection tools. Instead, by adding AppGuard, we either stop what others miss entirely or stop what they detect too late," says Comlekoglu.

> AppGuard complements AV, EDR, and XDR. Instead of trying to detect malware, it doesn't let malware do what it needs to do

One such client is an airline with tens of thousands of endpoints. It had found that antivirus and endpoint detection and response solutions required too much operational effort for too little risk mitigation. They used AppGuard to implement their "Security by Design" philosophy, which fills the gap they saw in ZTA frameworks. After years of searching for applicable tools, they opted for AppGuard because it uniquely achieved the needed risk mitigation without imposing impractical operations and usability issues. Since deploying AppGuard in 2019, they have experienced no successful malware attacks, a significant feat in mitigating malware threats and improving overall security.

AppGuard has proven its mettle wherever it has been implemented, be it in finance, government, healthcare or any industry that suffers from similar problems. It ensures that whenever the scourge of malware attacks strike, it is there to fight back, providing an additional layer of protection. The war in the cyber-sphere is ever-raging, but AppGuard stands tall as a force of good against the relentless tide of threats. ES