APPGUARD

The Malware Disruptor

The Malware Disruptor

DEFENDING YOUR ENTERPRISE FROM HARM

Agenda

- AppGuard Background
- Endpoint Security Challenges
- Why Prevention on Endpoints is Key
- AppGuard Technology Overview
- AppGuard Value & Benefits
- Q&A

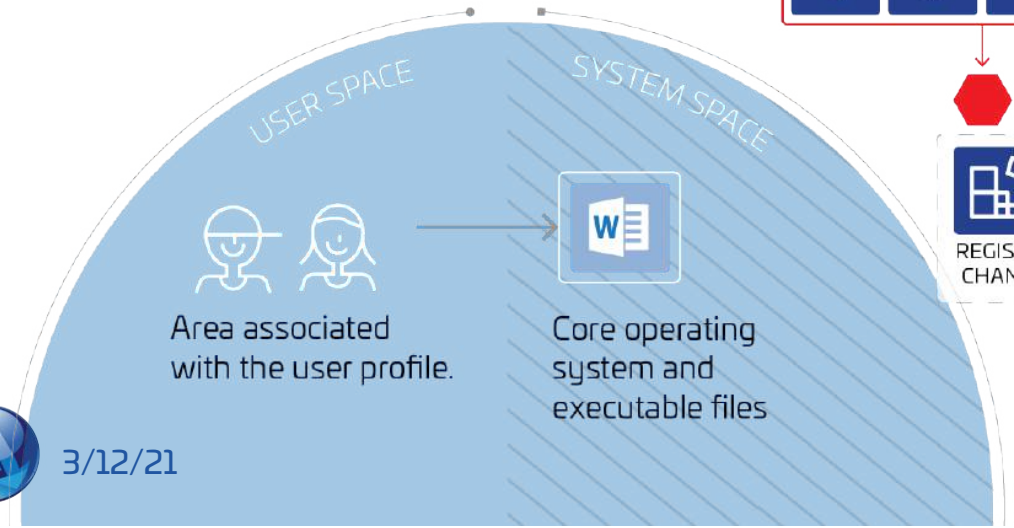
Prevent Breaches with 3-Point Policy Protection

LAUNCH POLICY | POST-LAUNCH POLICIES

Zero Trust Space
LOCATION-BASED POLICY

Key operating system folders are separated into System Space. **Applications and utilities can only launch from the System Space** unless a "trusted" exception is granted.

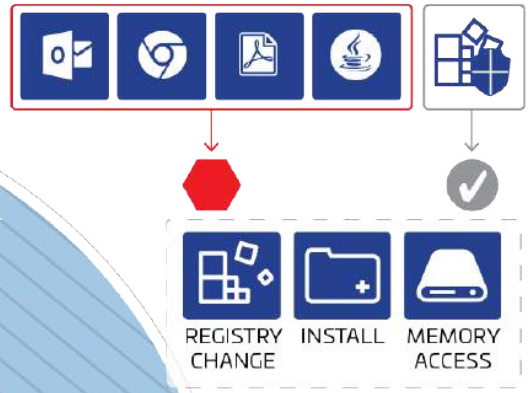
User Space is "untrusted" territory, where executables are blocked from launching.



Isolation
OS INTERACTION POLICY (PATENTED)

Applications in System Space are grouped into **high-risk** and "normal" applications.

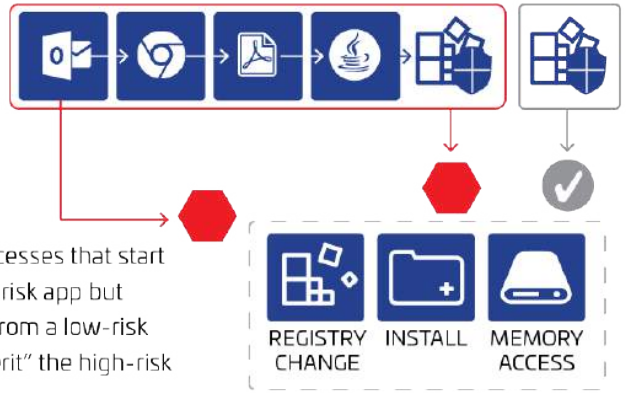
High-risk apps are blocked from executing processes malware requires to cause harm.



Inheritance
PROCESS EXECUTION FLOW POLICY (PATENTED)

Inheritance ensures that isolation rules are automatically adapted for more precise controls with less management burden.

Advanced malware cannot hide its actions using a normally unrestricted application.



Child processes that start in a high-risk app but execute from a low-risk app "inherit" the high-risk policies.

Values & Benefits

HOW APPGUARD BENEFITS YOUR BUSINESS & CYBER STACK

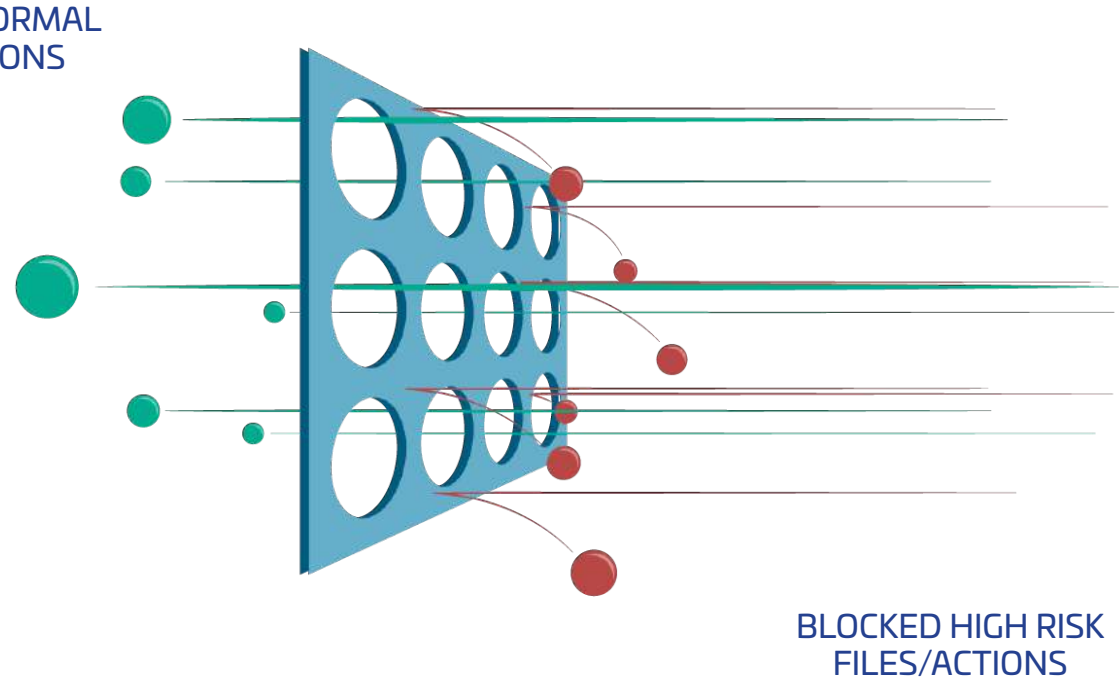
Worldwide Credibility

AppGuard Targets the Source

93%

of successful cyber attacks occur because a **vulnerable application or utility targets an endpoint** operating system using a small number of actions, regardless of the form it takes.

AppGuard restricts applications from performing the high-risk actions that malware must use to cause harm.



SMBs Are Not Immune to Attacks

- Every 19 seconds a small UK business is hacked (Hiscox)
- 63% of SMBs reported a data breach in 2019, up from 58% and 54% in 2018 and 2017.
- COVID-19 remote work trend and BYOD introduce greater risk/greater attack surface.
- Major 2020 breaches were caused by employee behavior (external/unapproved websites)
- Attacks on supply chains (i.e., trusted 3rd party partners) increased for Medium Enterprises
- Tougher cyber security and response regulations emerging globally (GDPR, HIPPA, etc.)
- Inadequate web and server protection (only 3% of global web servers employ adequate security for full range of cyberattacks).

SMBs Are Not Immune to Attacks

Every 19 SECONDS a small UK business is hacked

(Hiscox)

63%

of SMBs reported a data breach in 2019,

up from 58% and 54% in 2018 and 2017

COVID-19 remote work trend

and BYOD introduce greater risk/greater attack surface

Attacks on supply chains

(i.e., trusted 3rd party partners)

increased for Medium Enterprises

MAJOR 2020 BREACHES

were caused by employee behavior

(external/unapproved websites)

Inadequate web and server protection

(only 3% of global web servers employ adequate security for full range of cyberattacks).

Tougher cyber security

and response regulations emerging globally

(GDPR, HIPPA, etc.)

AppGuard's Mission

Enable businesses to do what

they need to do,

while preventing malware

from doing what it wants to do.

AppGuard's Mission

Enable businesses to do what they need to do,
while preventing malware
from doing what it wants to do.

AppGuard Benefits for MSSPs

Text goes here

Text goes here

Understand the Cause of Breaches

USERS

No matter
how much we train,
mistakes happen

APPLICATIONS

All applications
are flawed, despite our
best efforts

ENDPOINTS

Endpoints are the
most vulnerable piece
of your network