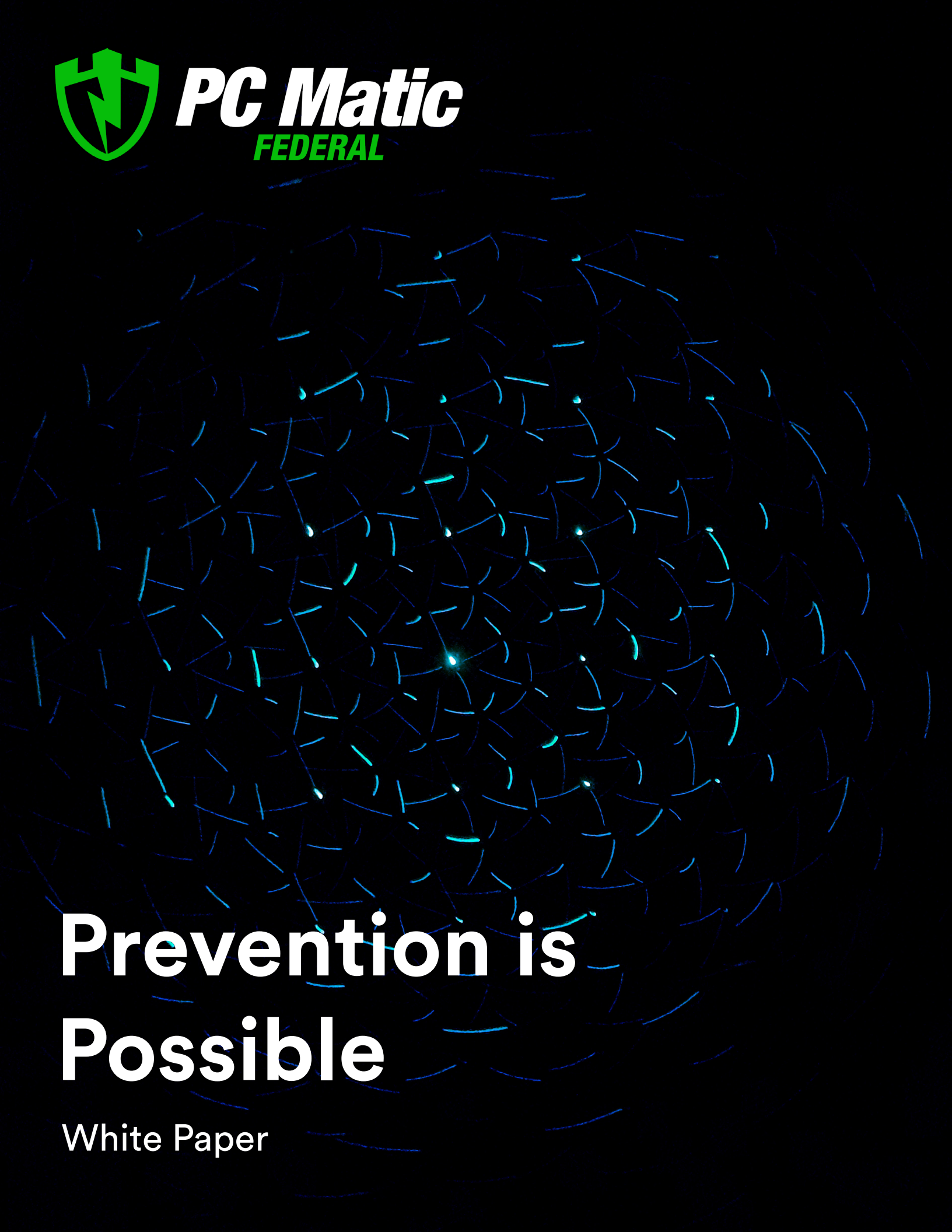
PC Matic FEDERAL



Prevention is Possible

White Paper

Evolution of Whitelisting

Whitelisting is evolving, even its name is changing. It has grown from beginnings as application control and application whitelisting to challenge the very premise dominant in the market that prevention is impossible and therefore our security approach needs to focus on detection and response.

Default Deny or Deny-All Permit-by-Exception approaches to cybersecurity are unchallenged in their ability to improve the security efficacy of any network. However, this approach remains largely unadopted despite being a top recommendation from NIST since it published SP 800-167 in 2015. This is largely due to initial difficulties populating the whitelist which requires administrators to fully enumerate all software in their environment. In large networks, this task has historically proved to be so cumbersome that it caused the market to abandon prevention, leading to the rise of EDR solutions as a way to manage risk in lieu of protecting networks.

"...this task has historically proved to be so cumbersome that it caused the market to abandon prevention, leading to the rise of EDR solutions as a way to manage risk in lieu of protecting networks."

PC Matic's Solution

PC Matic has solved this problem for its customers with a patented Global Allowlist. For over a decade PC Matic has been providing cybersecurity in the consumer market utilizing a default deny approach. When any endpoint experiences an unknown event, that execution is blocked until it can be reviewed by PC Matic's Malware Research Team and categorized as a known good or bad and that is updated to the Global list utilized by all customers.

This means that out of the box, PC Matic comes with a pre-populated allow list consisting of millions of lines of known good drastically reducing the effort to adopt a default-deny security posture. Layered on top of the global list are local lists allowing administrators to manage their endpoints in whatever architectural groupings make the most sense for their specific network.

"This means that out of the box, PC Matic comes with a pre-populated allow list consisting of millions of lines of known good drastically reducing the effort to adopt a default-deny security posture."

As a Default Deny tool, PC Matic does much more than just application whitelisting. Also

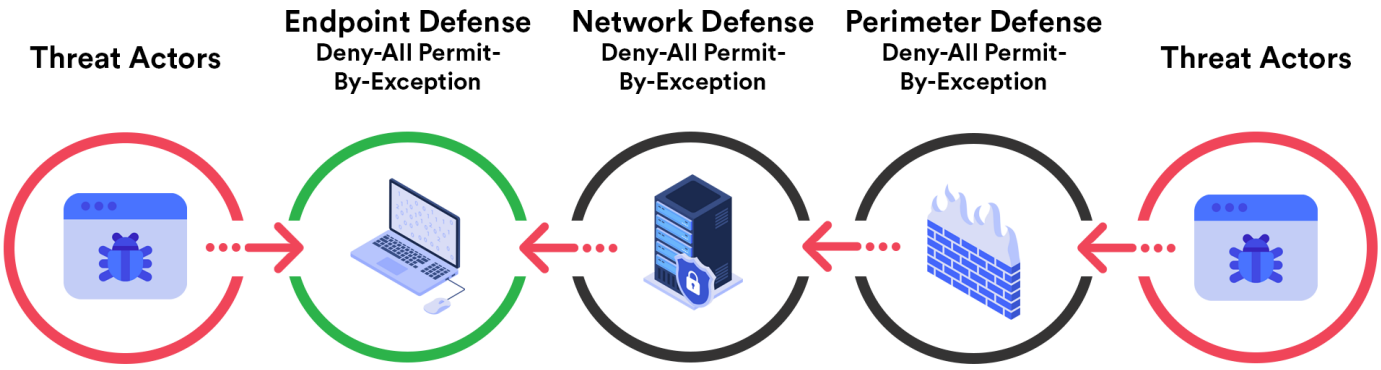
included are processes to monitor and block fileless malware and known good applications being used maliciously. This is on top of the standard approaches to application whitelisting that include allowlists for code signatures, directories, and hashes.

"...if a network administrator isn't able to accurately populate the whitelist and enable the Deny-All, Permit-by-Exception policy, are they really meeting the control?"

Regulatory Shifts

With the recent changes in the regulatory environment such as CDM and CMMC requiring whitelisting to meet the NIST 800-53 control **CM 7 (5) (b) Employ a deny-all, permit-by-exception policy** ... there has been a sudden attempt by many EDR firms to include a whitelisting feature. However, if a network administrator isn't able to accurately populate the whitelist and enable the Deny-All, Permit-by-Exception policy, are they really meeting the control and providing the preventative security layer enterprise and agency networks so desperately need?

Default-Deny Defense at Depth Paradigm



It is trite but true, there is no silver bullet in cybersecurity. However, layering a deny-all permit-by-exception approach provides agencies and companies the ability to again focus on prevention, and PC Matic provides the ability to do this without impacting availability. Prevention is possible and we would value the opportunity to demonstrate how with a technical demo of our product with your team.

PC Matic's products provide our customers with essential security that enhances the zero-trust model and fills potential gaps left by other traditional endpoint security software. With a foundation in application whitelisting, PC Matic uses a default-deny approach that prevents all known bad and unknown application from executing. Our patented globally automated whitelist provides a backbone of millions of known good applications to remove the headaches that come with traditional application whitelisting solutions by drastically reducing false positives during and after implementation. This NIST recommended approach combined with a globally automated whitelisted lowers the burden on IT and lowers the barrier to entry for most companies to meet CMMC requirements and build upon a zero-trust mindset by including proactive default-deny protection in their endpoint security stack.