PC Matic PRO

State and Local Government Security

Ransomware Stops Critical Systems

Licking County, Ohio

After a ransomware attack struck the county offices, online services and office telephones for the local government were taken down for at least a week. 911 dispatch in the county was forced to work without office phones or computers but assured residents emergency services were still available.

Newark, New Jersey

The city of Newark's computers were taken down for the second time in two years due to a ransomware attack. This time the attackers demanded $30,000 in bitcoin to decrypt the files. The CIO for the city said, "The virus compromised our network and disrupted many services that we offer, our police services are unaffected and continue operating normally..."

Murfreesboro, Tennessee

The emergency services in Murfreesboro were hit with a ransomware attack earlier this year that took their systems offline. Two servers and nineteen endpoints were affected by the WannaCry outbreak and the data on them was unretrievable.

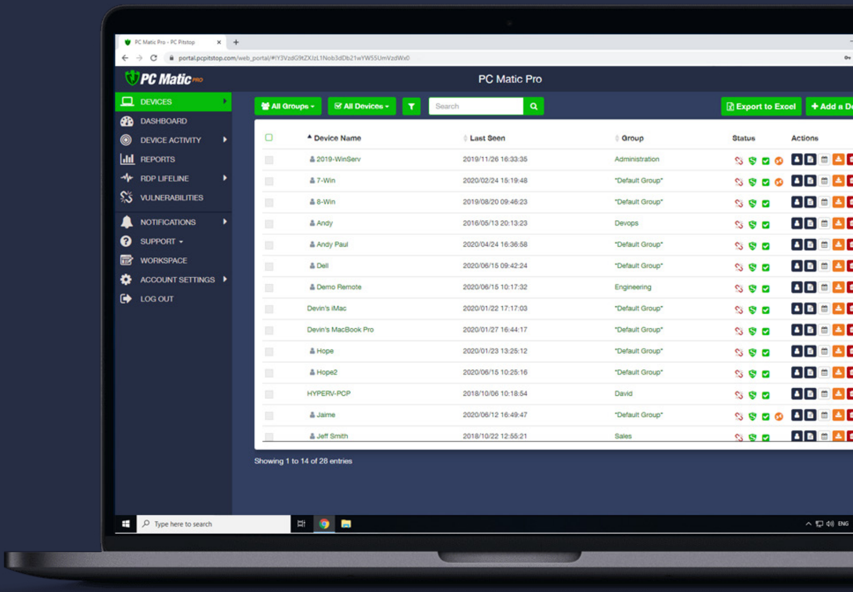
> Cyber criminals have begun to specifically target those who protect us with specific types of ransomware or campaigns. A ransomware campaign using CryptFile2 recently focused mostly on State and Local government by a factor of ten. Criminals know that many governments, especially small ones, won't be as equipped to defend against attacks.
>
> Ransomware has been noted as the top concern among local governments in a recent study and a better approach is desperately needed. PC Matic Pro takes a strong stance against ransomware with a default-deny approach based on our globally automated whitelist. We always stop unknown applications from running including even the newest ransomware.

Cyber Criminals Wage War on State & Local Governments

- According to cyber security experts, new variants of ransomware like Mars Joke have been introduced to specifically target state and local government agencies in their infection campaigns.
- Even if governments can avoid paying the ransom, downtime can often be more costly to the taxpayer. San Francisco's SFMTA was infected and payment systems went down for public transport. To avoid downtime free rides were offered as they scrambled to restore the systems. This lead to a huge cost for SFMTA and further demonstrates why prevention, not reaction, is key.
- Ransomware is expanding at a blistering pace according to statistics from the US Government. 2016 saw more than a 300% increase in attacks compared to 2015; and this year is set to continue the trend.

www.pcmatic.com
sales@pcmatic.com
info@pcmatic.com

PC Matic Pro delivers default-deny endpoint security backed by our global Application Allow List. We proactively block more threats than our competition while providing simple centralized cloud based management. Introduce better tools and security to your network with a product that is 100% made & supported in the USA.



Device Name	Last Seen	Group	Status	Actions
2019-WinServ	2019/11/26 16:33:35	Administration		
7-Win	2020/02/24 15:19:48	"Default Group"		
8-Win	2019/08/20 09:46:23	"Default Group"		
Andy	2016/05/13 20:13:23	Devops		
Andy Paul	2020/04/24 16:36:58	"Default Group"		
Dell	2020/06/15 09:42:24	"Default Group"		
Demo Remote	2020/06/15 10:17:32	Engineering		
Devin's iMac	2020/01/22 17:17:03	"Default Group"		
Devin's MacBook Pro	2020/01/27 16:44:17	"Default Group"		
Hope	2020/01/23 13:25:12	"Default Group"		
Hope2	2020/06/15 10:25:16	"Default Group"		
HYPERV-PCP	2018/10/06 10:18:54	David		
Jaime	2020/06/12 16:49:47	"Default Group"		
Jeff Smith	2018/10/22 12:55:21	Sales		

Showing 1 to 14 of 28 entries

Innovative Security & Remote Management

Zero Trust Security

Our realtime protection, SuperShield, provides default-deny protection against unknown malware and ransomware on your network. Using our global whitelist, we remove the work that normally comes with Application Allow Listing; an NIST recommended approach.

Remote Tools

Access a suite of Remote Management Tools inside of your PC Matic Pro Cloud Console. From anywhere in the world, you can quickly VNC into a user's machine, open a Remote CMD Prompt to run scripts locally, browse and upload to file directories, remotely shutdown, and more.

RDP Security

PC Matic's RDP Lifeline provides a suite of security and management tools for RDP. Introduce whitelist based protection for RDP sessions, get realtime SMS alerting with quick actions to kill an active session, and review expansive reporting that includes IP, location, duration, device name, etc.

PC Matic Pro Endpoint Suite

PC Matic Pro delivers default-deny endpoint security backed by our proprietary global Application Allow List. We proactively block more threats than our competition while providing simple centralized cloud based management that is 100% developed & supported in the USA.

www.pcmatic.com
sales@pcmatic.com
info@pcmatic.com

Security Features

PC Matic Pro's enterprise grade security uses several advanced technologies to secure your endpoints with a philosophy that is centered around prevention, not reaction.

Global Allow List

Constantly updated and already containing millions of good files, our default-deny approach provides NIST recommended security with no more work than traditional solutions.

Script Prevention

Fileless malware defeats traditional deny list and allow list solutions. Our advanced heuristics monitor known good applications and prevent them from leveraging scripting engines like Powershell.

Anti-Tampering

Built-in protections, including an ELAM driver, at each device prevent any user from uninstalling, turning off, or removing the realtime protection so your network stays secure.

Device Authentication

To keep your cloud-based console secure, our multi factor authentication easily prevents any unauthorized access by identifying and blocking unknown devices from logging in.

RDP Features

In 2019 over 60% of ransomware was distributed through Remote Desktop Protocol ports. Now a large target for cyber criminals, PC Matic Pro secures and monitors RDP sessions with full remote control.

RDP Security

With RDP Authentication, PC Matic Pro easily blocks unknown devices from connecting through RDP inside your network. Any attempts are immediately killed and logged inside your console.

RDP Logging

Detailed logging of all RDP sessions provides the ability to quickly review activity including session duration, IP address, location, device name, and if the session was blocked or allowed.

RDP Scheduling

Remotely control RDP from your single cloud console. Fully enable or disable RDP ports, set them on a reoccurring schedule, or temporarily open them for a couple hours that day.

RDP Alerts

If a new session is attempted on any device, you can receive realtime alerts to your phone with quick actions to kill that session, whitelist that device for the future, and shutdown that machine.

EDR Features

Even with a focus on prevention and stopping malware pre-execution, PC Matic Pro includes more sophisticated EDR tools than any of our competitors.

Remote Access

PC Matic Pro includes an integrated VNC agent for quick remote access to any device on your account. With two mouse clicks you can share and control any desktop to help fix problems.

Remote CMD

Need to get something done behind the scenes? A realtime remote CMD prompt for each device lets you send commands without disrupting a user that's currently at the machine.

File Manager

Review a full directory for every device and easily upload or download files to and from your machine. Send a new installer over by simply dropping it on the users desktop for them to double-click.

Reboot & Shutdown

After applying updates, when you're looking to power down at the end of the day, or if you're locking down part of the network, send remote reboot and shutdown commands to your devices.

Reporting Features

With a wide array of security features and monitoring across your devices, it's important to have a detailed set of reporting and alerting to review and customize.

Realtime Alerts

Stay on top of blocked applications, new RDP sessions, quarantined files, and more inside your console with realtime alert notifications and quick actions to remediate any alert.

Alert Customization

Don't want to be bothered by an alert about a hard drive running low on space? Turn it off. Adjust the threshold to 95%. You can customize every alert so you don't get bogged down by alert fatigue.

Scheduled Cleaning

Beyond traditional antivirus, PC Matic Pro includes the ability to automate an array of tools that ensure every device is cleaned, updated, and running properly without your intervention.

Patch Management

Automatic updates for third party applications removes the security hole that comes with outdated software. Apply version control and automation to prevent users from clicking 'remind me later'.

Don't forget support! PC Matic Pro includes complimentary customer support and a dedicated onboarding team to proactively monitor your account for problems and even help you get installs done in your environment.

www.pcmatic.com
sales@pcmatic.com
info@pcmatic.com

PC Matic PRO

Better Security, Better Features, Better Price

	PC Matic Pro	Cylance	Carbon Black	Symantec	McAfee	Trend Micro
Global Allow List Protection	✓					
RDP Security Suite	✓					
True Zero Day Prevention	✓					
Fileless Malware Protection	✓	✓	✓	✓	✓	✓
Integrated Remote Management Suite	✓		✓			
Multi-Factor Device Authentication	✓					
Vulnerability Patching	✓					
Simple Cloud Management	✓	✓	✓	✓	✓	✓
Single Lightweight Client	✓					
100% Made in the USA	✓					

> "One of our biggest concerns is a trojan implanted on a computer spreading throughout the network. With so many staff and faculty using computers on our network, we are constantly being bombarded with phishing or trojan emails and users visiting infected websites. The allow list protection used by SuperShield has been a tremendous help in preventing infections and implantations." - Jerry Shipman, St. Vincent High

Support

Windows 7 - 10
Server 2008 - 2019
macOS Sierra & up
Chromebook

Licensing

1 Year Term
2 Year Term
3 Year Term
Flexible Billing

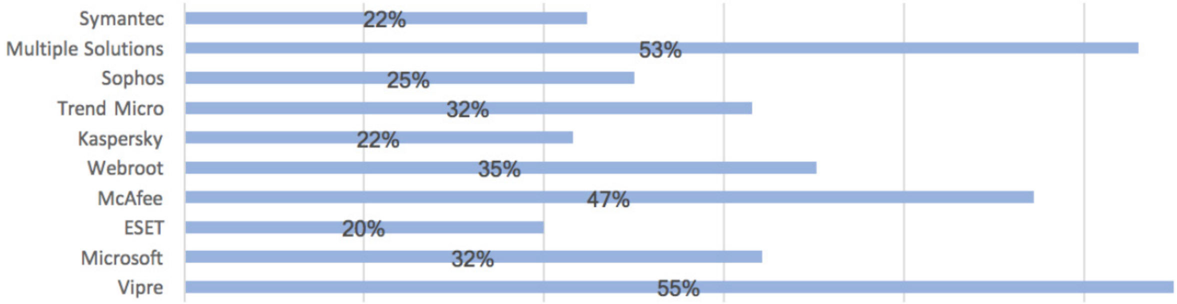
Pricing

EDU Discounts
Non-Profit Discounts
Gov't Discounts

Legacy Antivirus Has *Failed...*

The amount of ransomware variants that are being introduced into the world on a daily basis is staggering, and it's not surprising that the traditional blacklist approach can't keep up. In a recent survey by KnowBe4 you can see the percentage of organizations experiencing a ransomware attack by current AV solution.

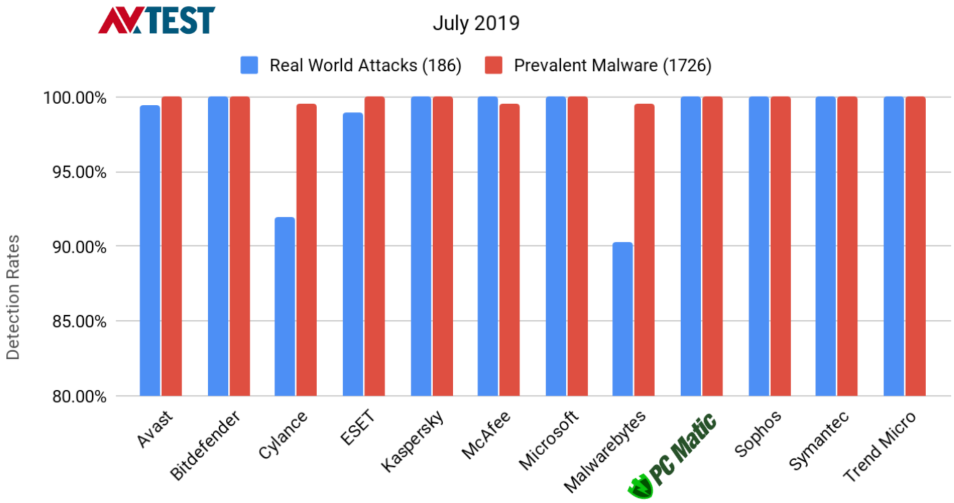
Percentage of organizations experiencing a ransomware attack (by AV solution)



*KnowBe4 Survey of 500 Organizations May 2017

A New Approach is Desperately Needed

At PC Matic Pro we are providing default-deny application whitelisting on a global level. This removes the overhead needed to implement a whitelisting solution and maintain it over time. We stop all unknown software from executing on the endpoint and only allow known, good applications that are listed on our whitelist.



Don't take our word for it; There are independent testing houses who are frequently testing our products to see how effective they actually are. If the products you're considering aren't routinely tested it is important to ask why. We offer up a recent test of our product here from AV-Test to begin your deep dive into detection rates.

Customer Success Stories:
Dawes County Sheriff

> With nearly 10,000 citizens depending on Dawes County Police to protect them, it's critical that Sheriff Dailey's systems are up and running 24/7. "As most people know, the internet is ripe with hazards. Because of the nature of how we use our computers, for very detailed and personal information, we needed to protect it as best we could. I'm tickled to death with it. I really like it. We've had zero problems with our machines, since we put it on."
>
> – Karl Dailey, Dawes County Sheriff

pcmatic.com/pro | info@pcmatic.com

PC Matic PRO