LOGINCAT

ZERO TRUST CYBERSECURITY

Tekmonks

What is LOGINCAT

As technology constantly progresses and changes, our need for cyber protection increases. No one is immune to online security threats. Attackers are employing innovative techniques and exploit new vulnerabilities every day. The demand for better protection is now a greater need than ever before. Cyber attacks affect us in personal, professional and financial ways and every new attack begs the question – What can we do to protect ourselves from that type of destruction?

- Approximately $1 trillion is expected to be spent globally on cybersecurity from 2017 to 2021.
- Only 38 percent of global organizations claim they are prepared to handle a sophisticated cyber attack.
- Total cost for cyber crime committed globally has added up to 100 billion dollars. Don't think that all that money comes from hackers targeting corporations, banks or wealthy celebrities. Individual users like you and me are also targets. As long as you're connected to the Internet, you can become a victim of cyber attacks.

There are attacks by hackers every 39 seconds.

THE FEATURES

- 360º protection
- AI based
- Zero Trust based
- Intend based hack detection
- Application Security
- Network Security
- Cloud Security
- Endpoint security
- Remote Access
- SOC

THE DIFFERENCE

- We assume the hackers are smarter than us
- LoginCat is designed for the worst case scenario - to operate in a hacked environment

THE WHY

- No need to modify existing applications
- Unparalleled Cybersecurity
- Peace of Mind
- Protects against every known cyberattack

How does LoginCat provide Security?

1

AppSecure

- Secures old single factor applications

- Protects against password hacks

- No need to modify applications

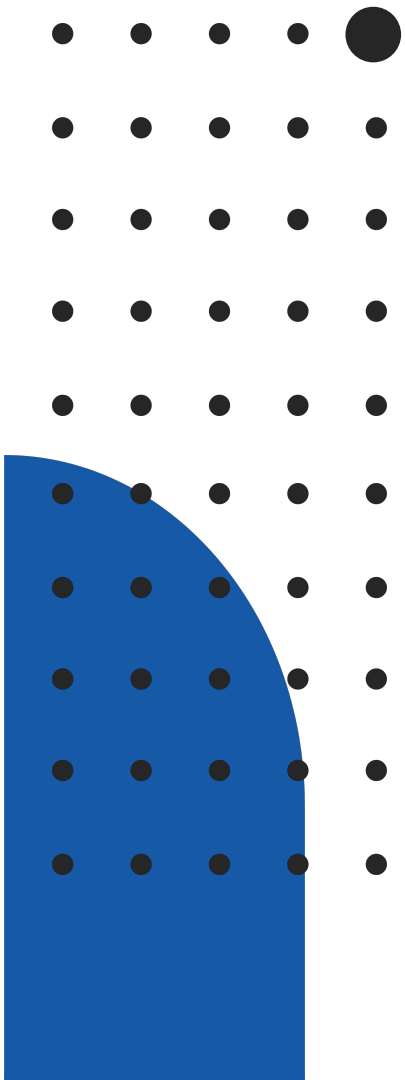
2

Smart Firewall

- Users authenticated at login so IP addresses are known

- IP addresses which have been authenticated are the only ones allowed access

- Self configuring firewall



3

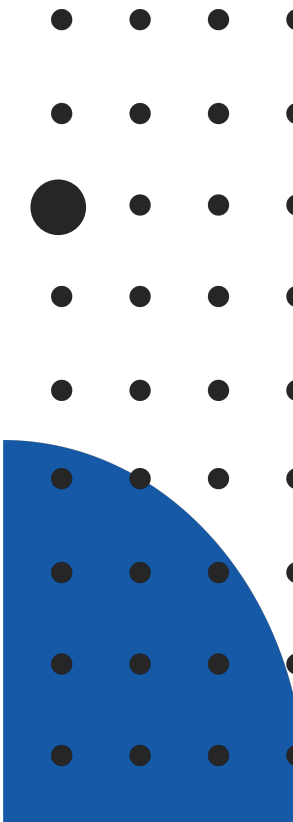
Multi Factor Authentication

- First, Eliminate passwords, replace with passphrases which are hard to crack but easy to remember

- Second, we use a second factor which can be a range of algorithms such as: OTP, Second Factor Questions or Touch ID

- Third, we use an AI algorithm to analyze the logging pattern of the user to ensure they are who they say they are.

- Fourth, we use AI to analyze the access pattern of the user post login. If we find it suspicious we can block access. Thus, we don't treat the authentication itself as the final word. Protecting corporate assets by profiling user's action even post authentication.



4

Third Factor AI Based Hack Detection

- AI based security algorithms

- Beyond IP firewalls, LoginCat will analyze incoming login attempts and ban hackers using habit and user analysis

- We know who you are, hackers don’t know who they are hacking

Produced/Printed in the UK 05/07

PATENTS: US Patent Pending

IMPORTANT PRIVACY INFORMATION: If you would like to request access to or correction of your details, or if you would prefer you or your organization not to receive further information on Tekmonks products and services please contact us at: privacy@tekmonks.com

Kemp House, 152 City Road
London. EC1V 2NX. UK.

Tekmonks