Small to Midsized Businesses

Simple, automated, affordable security.

What is Strongarm?

Strongarm is a **cloud-based DNS blackhole** that takes control of malicious traffic as it leaves your network. By taking control of the traffic, we can stop the attack, educate your users, and keep you safe.

What Strongarm Protects Against

- Phishing
- Malvertising
- Exploit Kits
- Ransomware
- & all other forms of malware

How Strongarm Helps SMBs

Easy to Deploy and Manage

With no agents or hardware required, you can get set up in minutes. No headaches, ongoing maintenance, or deployment challenges.

Automated

There is no security expertise required. Strongarm does all the work for you automatically, keeping you protected and aware of DNS activity.

Small Business Pricing

Strongarm offers enterprise-level security at a fraction of the price—just $3/user/month. Cost-effectively protect against malware threats.

DNS-Based Security

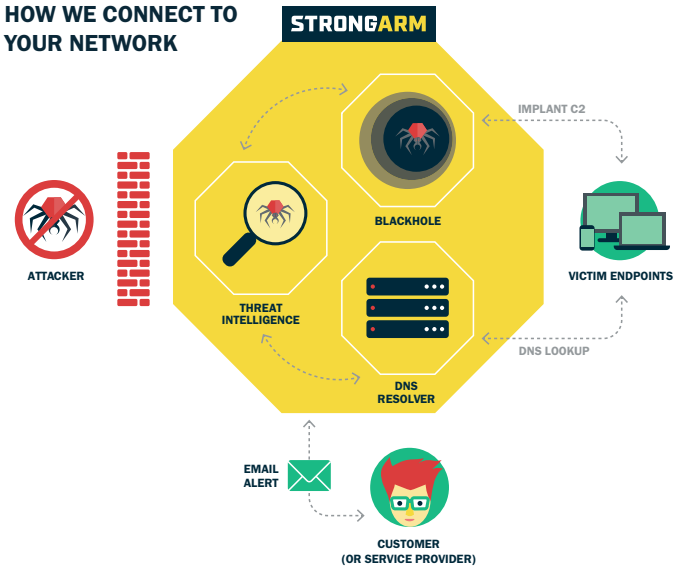
By watching DNS requests (rather than network traffic), Strongarm protects against encrypted traffic, phishing e-mails, and other tactics hackers use to get past firewalls and antivirus.

No Beeping Boxes

When our alerts arrive, you can be sure we've found something worthy of investigation. No alert fatigue or beeping boxes with Strongarm. Contextual alerts make resolution simple.

Personal attention

Strongarm's security experts offer direct, personalized insight on how to handle incidents and spot potential threats. Our team is an extension of yours, helping you stay secure.



"Strongarm provided instant value to our company, stopping a popup from installing malware and stealing data. Seeing Strongarm in action reiterated the real threats that can impact a business. Strongarm gives me peace of mind that my network is secure."

—Mike Gibson,
IT Manager, Nazareth Ford

Three Common Threat Scenarios

Happy Clickers

Scenario: No matter how much user education you provide, every organization has one or two employees who click anything that comes their way. This is how spray-and-pray phishing attacks succeed. Once a user clicks, you could be left with a time-consuming cleanup or a full-on ransomware attack.

How Strongarm Protects: Strongarm automatically stops any device from communicating with malicious sites that house ransomware. Strongarm can also usually identify which device made the request, so cleanup is simple and fast.

Highly Targeted Spearphishing

Scenario: Hopefully your team is well-trained to spot phishing attempts, but accidents happen. Whether a user is distracted or the attack is well-disguised, you are never going to hit 0% click rates. Targeted phishing attacks often go after key employees with access to the CEO or sensitive information and can lead to major fallout, such as information loss and legal troubles.

How Strongarm Protects: After a user has clicked a phishing link, Strongarm steps in and prevents the user's machine from actually connecting with the malicious site. Strongarm keeps password credentials safe, and stops the user from disclosing company secrets or PII to the attacker. As a bonus, we help re-enforce phishing education.

Clickless Threats

Scenario: Sometimes attackers infect legitimate sites with malware. Users whose systems are not patched could be open to infection, even without clicking or falling for a phish. Clickless threats include malvertising and exploit kits, which can ultimately lead to information theft or ransomware.

How Strongarm Protects: Strongarm stops these attacks by preventing your network from downloading any malicious code. This foils attacks without impacting users. We then provide analysis and confirmation of safety. Perhaps best of all, Strongarm protects even before patches are available.

READY TO GET STARTED?
Contact us: sales@legioncyber.com to start your risk-free 30 day trial.

www.strongarm.io

sales@legioncyber.com

Copyright © 2017 Strongarm

LEGION Cyberworks
PROTECT | ADAPT | SURVIVE