Security as a Service

C Spire works for you, helping close the door with next-generation firewall protection.

Protecting critical data should be every business's top priority. Hacks, malware, ransomware, and data breaches are no longer carried out by only highly skilled individuals in targeted attacks. Most breaches are targets of opportunity – carried out automatically by botnets scanning open internet connections.

SMBs are the backbone of the American economy as well as increasing targets for cybercriminals. One study found that 61% of SMBs experienced cyberattacks in 2017, but only 21% rated their ability to mitigate cyber risks as highly effective.

> **The growing number of sophistication and cyber threats... can be devastating to small businesses in particular.**
>
> - Howard S. Marshall,
> Deputy Assistant Director, Cyber Division, FBI

NEXT-GENERATION FIREWALLING

Firewalls monitor and control the traffic to and from your business to the world. Traditionally, businesses purchased physical hardware that they configure, manage, maintain, and monitor themselves. C Spire's solution allows the customer to skip the hardware headache and entrust our fulltime security experts, instead of attempting to become one yourself.

C Spire Next-Generation Firewall Features

APPLICATION ID

Application ID allows you to view the applications running on your network and learn how they work, their behavioral characteristics, and their relative risk.

THREAT PREVENTION

Threat prevention protects your network against threats by providing multiple layers of prevention, and confronting the threats at each phase of the attack. In addition to traditional intrusion-prevention capabilities, we provide the unique ability to detect and block threats on any ports. This feature includes:

- **Antivirus** – Used to protect against worms, viruses, trojans, and block spyware downloads.
- **Anti-spyware** – Used to block attempts from spyware on compromised hosts trying to phone-home or beacon out to external command and control servers.
- **Vulnerability protection** – Used to stop attempts to exploit system flaws or gain unauthorized access to systems.

DATA FILTERING (DLP)

Data filtering prevents sensitive information from leaving a protected network. C Spire will filter on pre-defined patterns for credit card and social security numbers and up to 3 customer defined regular expressions.

ZERO-DAY THREAT PREVENTION

- Detects evasive zero-day exploits and malware
- Orchestrates automated prevention for unknown threats in as few as five minutes from first discovery anywhere in the world, without requiring manual response.
- Builds collective immunity for unknown malware and exploits with shared real-time intelligence from approximately 20,000 worldwide subscribers.

FILE BLOCKING

File blocking halts file transfers over network protocols that should not be used for this purpose. For example: DNS, ICMP, and NTP.

USER ID

User ID enables visibility, security policies, reporting, and forensics based on users and groups not just IP addresses. This feature requires a customer installed agent on an active-directory server(s) to provide user to IP address mapping information

	Basic	Standard	Advanced
Next Generation Stateful Firewall	X	X	X
Application ID	X	X	X
Threat Prevention		X	X
Basic URL Filtering		X	X
Reporting		X	X
Site to Site VPN tunnels		X	X
Advanced URL Filtering			X
Zero-day threat prevention			X
Data Filtering (DLP)*			X
File Blocking			X
User ID**			X
Email Alerts			X
Client Based Remote Access VPN	Up to 10 users	Up to 20 users	Unlimited*

* Requires customer managed Authentification Server