

Small Business Office Secures Its Network and Computers Before a Client Security Audit

A firewall, segmentation and endpoint protection for a single-site office of 10 to 50 users, with audit-ready records.

Example scenario: a single-site business with 10 to 50 users, at headquarters or a branch. Not a specific client. This example uses 35 users.

The situation

A questionnaire arrives from the company's largest client, and the cyber insurance renewal asks the same things. Is a business firewall in place? Are the computers protected, including the laptops that leave the office? Can the company show how its network is built and segmented?

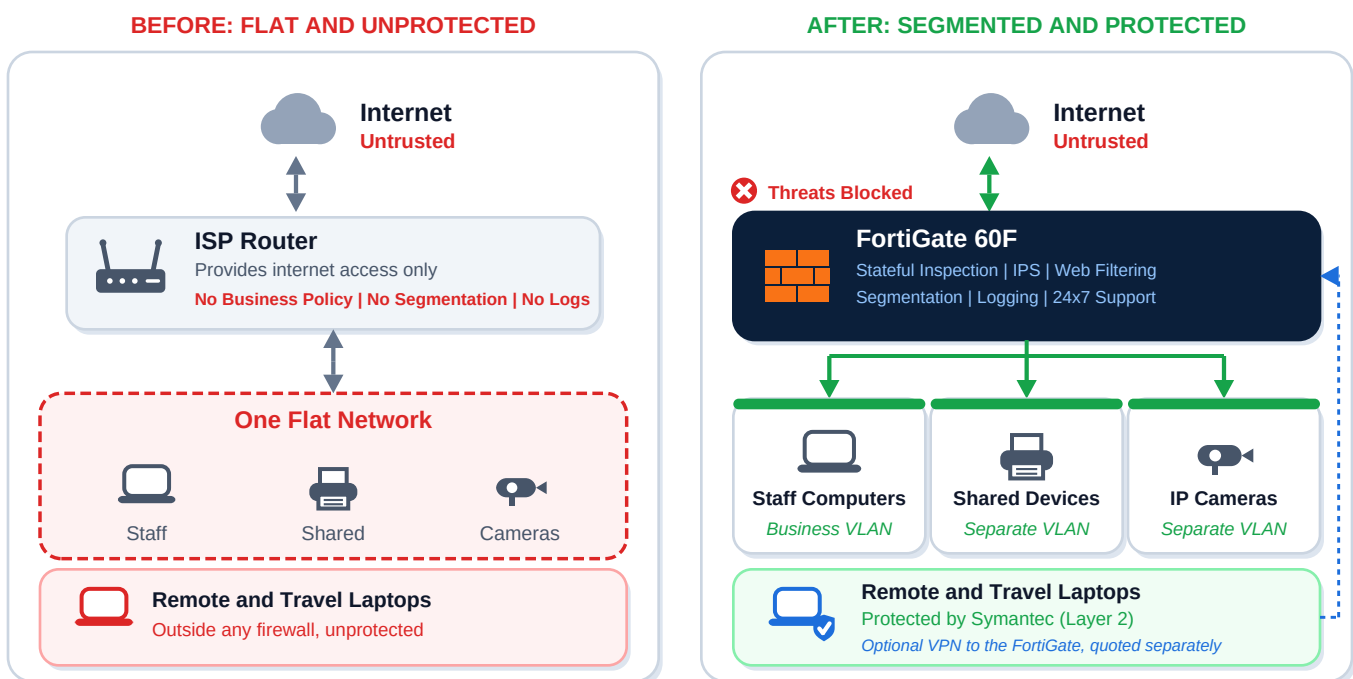
Today the answer to each is no. Thirty-five people work from one office on the router the internet provider installed, which provides access and enforces no policy. Workstations, printers, a scanner and eight IP cameras share a single flat network, so one compromised laptop can reach every other device, and there is no central log of what moved across it. A third of the staff also work from home, client sites, hotels and airports, outside any firewall, handling the same client data as the machines in the office.

Until the company can answer, both the client contract and the insurance renewal are at risk.

LAYER 1

Perimeter security and segmentation

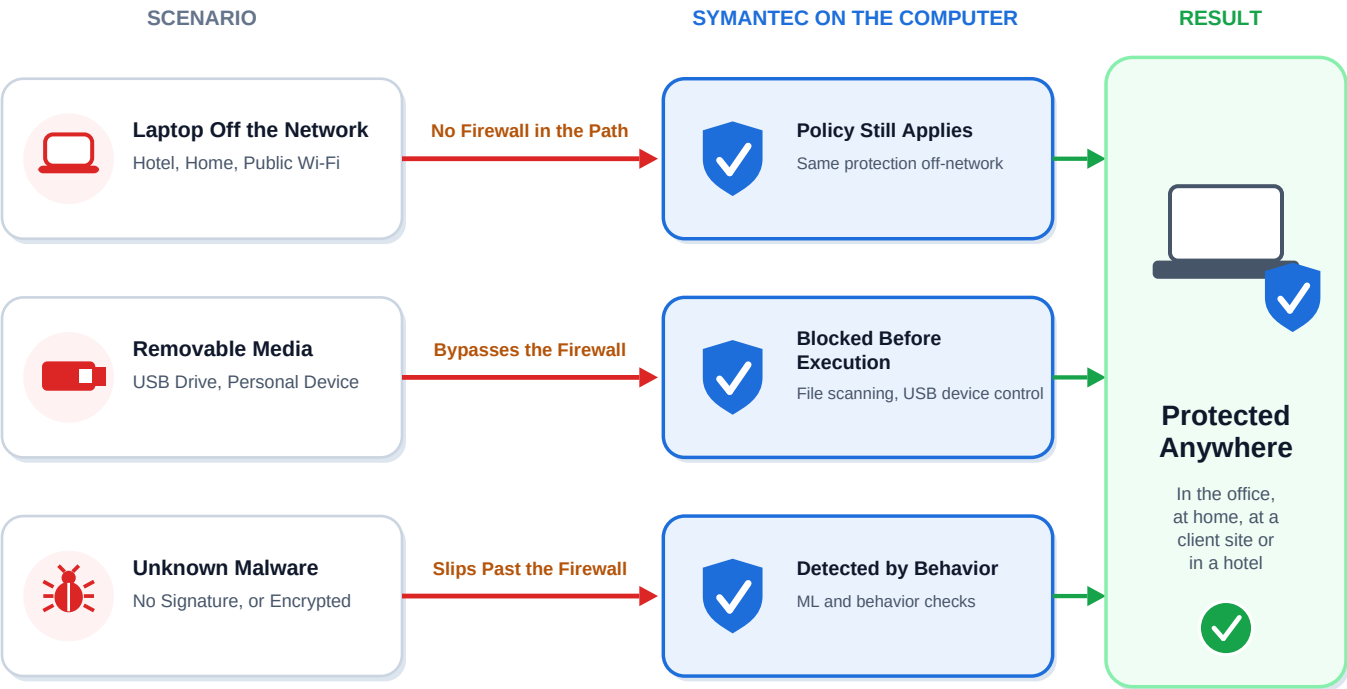
A FortiGate 60F, with three years of Enterprise Protection and 24x7 support, takes over the network edge. It inspects every session in and out, blocks known threats through intrusion prevention and web filtering, and divides the internal network into segments, so a compromised device stays contained.



LAYER 2

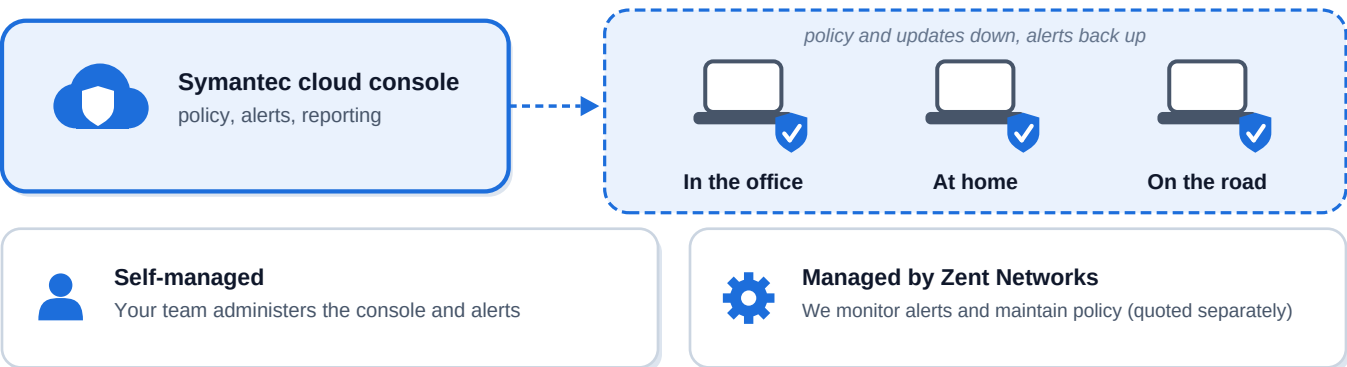
Endpoint protection that follows the device

A firewall governs only the traffic that crosses it. Symantec Endpoint Security Cloud runs on each computer instead, so the protection travels with the laptop: in a hotel, at a client site, against a USB drive from a personal device, and against malware with no known signature yet. The two layers overlap by design, so many threats have to defeat both.



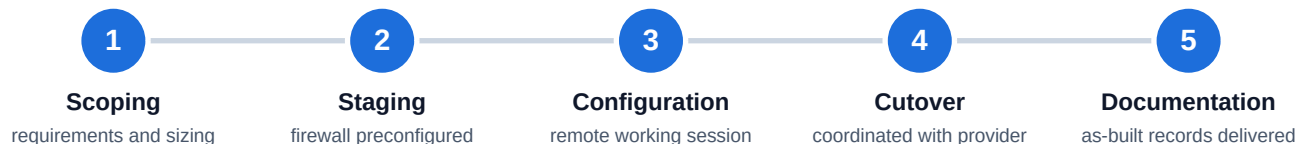
Red arrows show how each threat reaches the computer without being stopped at a firewall. Symantec on the computer stops it, so the laptop stays protected anywhere.

Centrally managed from the cloud



The endpoint protection is identical in both models; the difference is who administers the console. Self-management is included with the subscription. A managed service is quoted separately.

How a project runs



What the setup involves

Included in the base scope	Quoted separately
- Firewall installation and configuration migration - One site, up to three network segments - Up to 30 least-privilege firewall policies - NAT, DHCP and DNS configuration - Internet provider gateway coordination - Configuration backup and as-built documentation - Delivered remotely	- Endpoint rollout to each computer - Managed endpoint monitoring - Guest Wi-Fi (an additional segment) - VPN to headquarters or remote staff - Advanced security profile tuning - Change management, 24x7 monitoring - On-site installation or network discovery

The Symantec subscription is priced per user per year and is separate from the setup. Broadcom delivers the software with its installation package and instructions; help rolling it out to each computer is quoted separately. The user count is confirmed at quote.

What we need from you

- Console and ethernet cables at the site, and a laptop able to share its screen.
- A provider contact, so the gateway can be set to bridge (IP passthrough) mode.
- A list of computers to protect and a console administrator.
- Network switches that support VLANs, which we confirm at scoping.

How this answers a security questionnaire

Requirement	How this deployment addresses it
Perimeter boundary defense	Next-generation firewall at the edge with stateful inspection, intrusion prevention and web filtering, under active subscriptions and 24x7 vendor support.
Endpoint threat prevention	Symantec Endpoint Security Cloud on managed computers, with behavior-based malware prevention and USB device control, administered from a central cloud console.
Network segmentation	Staff computers, shared equipment and cameras sit on separate segments, limiting lateral movement if a device is compromised.
Documentation and logging	Configuration is backed up and documented as built. The firewall logs events; retention and review are set during setup, and monitoring is a separate service.

Answers vary by client and insurer. This example is not a compliance guarantee.

Want this for your organization? Share your headcount, internet service and number of locations, and we will recommend a size and quote the setup. Use **Ask us a question** on the article page at zentnetworks.com.