Symantec.

The Perimeter is Dead. Long Live the Perimeter.

The traditional network perimeter is vanishing in the sprawl of today's cloud generation workforce. So, too, is the security built into that perimeter. You need a better way to extend security controls and still support anytime/anywhere access—without compromising productivity.

Consider these five tips for securing your network in this always-on Cloud Generation world.

1 2 3 4 5

Tip | 1

Encryption is essential for secure communication and to protect privacy.

However, cyber criminals also use encryption to hide malware or exfiltrate data.

If network security tools cannot inspect and control encrypted content, your entire organization may be at risk.

Tip | 2

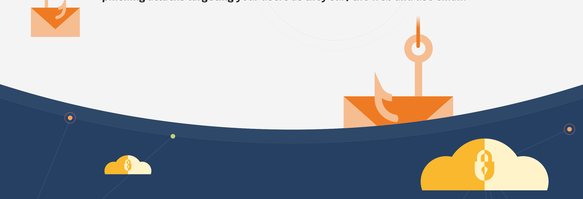
Malware analysis automatically detects malicious content and behaviors.

To stop zero-day threats, use malware analysis to automatically detect malicious content and behaviors. Use sandboxing to safely detonate zero-day threats and suspicious URLS. ***These tools should be an integral part of your modern day security defense system.***

Tip | 3

Even with the strongest threat protection, there's still a chance for threats to get through.

Web Isolation technology blocks even the most advanced threats and phishing attacks targeting your users as they surf the web and use email.



Tip | 4

Data leakage and information protection are more challenging with the growth of cloud apps and mobile usage.

Strong DLP is essential in ensuring information safety and compliance with regulatory requirements.

Tip | 5

Cloud apps—and their inherent risk—are now the norm in your stack.

Advanced CASB technology ensures that users access sanctioned apps and insulates them from risky ones.

For more information visit

www.symantec.com/cloud

Symantec.