SonicWALL Capture Advanced Protection Service

Opportunity

- Explosion of unknown, zero-day threats that signature based security solutions can't detect leaves organizations vulnerable to breaches
- Today's advanced threats are designed to evade 1st generation sandbox analysis and detection
- Threats are target not just to windows environments but also mobile and connected devices
- Hide in encrypted and unencrypted traffic
- Hide in more file types, file sizes

Customer challenges/pain points

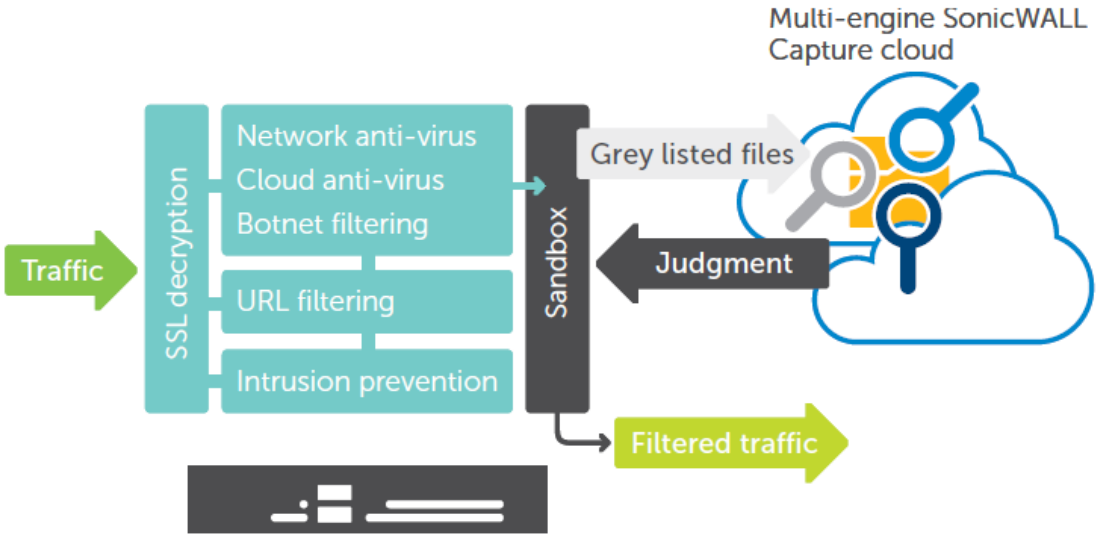
- Prevent unknown, zero-day threats from infecting networks
- Rapidly deploy signatures for newly discovered malware
- Increasing complexity and cost associated with advanced threat analysis technology

Relevant audience

• Stakeholders: IT administrators, CIOs, CISOs, CSOs, security managers, compliance managers, finance managers, business owners and employees
• Segments: SMB & Mid-to-large enterprises that aren't restricted from using cloud services for threat analysis.

SonicWall Advantage – Why SonicWall?

- **Multi-engine sandbox analysis** detects more threats, resists evasion, more than single-engine sandbox solutions
- Scans **encrypted and unencrypted** traffic and extracts suspicious code for analysis
- Detects and can **block/block until verdict** APT threats at the gateway for HTTP/S traffic
- Global infrastructure to **rapidly deploy remediation signatures** to all SonicWall Network security appliances preventing further infiltration of the identified malware/threat.
- **Cost effective and easy to deploy** solution



SonicWALL Capture Advanced Protection Service

Qualifying Questions

1. How are you preventing advanced threats from infecting your networks?
2. How are you preventing android advanced threats from entering your network?
3. If a host or client on your network is found to be infected how do you remediate and protect from follow on attacks?
4. If an advanced threat is hidden in a large file, how do you detect it?
5. If an advanced threat is hidden in encrypted traffic, how do you detect it?

Competition

PAN Wildfire

- First mover in the firewall market, cloud service and on-prem appliance.
- Strong firewall attach rate

Response

- SonicWALL Capture multi-engine advanced threat analysis detects more threats, is more difficult for threats to evade than PAN's single engine virtual sandbox.
- SonicWALL Capture block till verdict for HTTP/S prevents infection, PAN only blocks known malware, can't block till verdict suspicious files, prevent infection, requires manual remediation post infection.

Fortinet

- Forti-sandbox appliance, VM and cloud deployment. Suspicious files, objects fed from Fortigate, Fortimail etc..
- Virtual sandbox, windows OS only
- Integrated with Forti guard threat cloud for signature remediation
- Host/endpoint quarantine post infection

Response

- SonicWALL Capture multi-engine advanced threat analysis detects more threats and is more difficult for threats to evade than Fortinet's single-engine, virtual sandbox.
- SonicWALL Capture can analyze files not just for windows environments but also for android environments
- SonicWALL Capture block till verdict for HTTP/S prevents suspicious files from entering the network and infecting systems. Fortinet quarantines host/client post infection, can't block till verdict to prevent infection

FireEye

• Market leader, thought leader, expensive. Strong in Fortune 500, 2000 accounts
• NSS labs rated FireEye poorly in both their 2015 and 2014 breach detection report.
• FireEye cloud delivery platform is still in its infancy, strength is standalone appliance

Response

- SonicWALL Capture multi-engine advanced threat analysis detects more threats, is more difficult to for threats to evade than single engine analysis,
- SonicWALL Capture block till verdict for HTTP/S and global signature deployment prevents infection and follow on attacks
- SonicWALL Capture firewall integrated cloud service is easier to deploy, manage, reduces TCO

Features	Description
Multi-engine advanced threat analysis	Virtual sandbox analysis, full system emulation and hypervisor-level analysis
Broad file type analysis	PE, MS Office, PDF, archives, JAR, APK, Windows, Android
Can block until verdict for HTTP/S	To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.
Rapid deployment of signatures to prevent follow-on attacks	When a file is identified as malicious, a signature is immediately deployed for firewalls with SonicWALL Capture subscriptions to prevent follow-on attacks.
Monitoring and reports	SonicWALL Capture provides an at-a-glance dashboard and reports that detail the analysis results for files sent to the service,
Seamless firewall integration, scalable, affordable cloud service	Add on service reduces total cost of ownership