BLUE COAT

SSL/TLS Visibility
Determining Your Network Security Blind Spot Cost

Between 35% and 50% of your current network traffic is encrypted – and that percentage is growing at up to 20% per year. With the adoption of social media strategies, BYOD, cloud-based enterprise applications such as Salesforce.com, Google Docs and Office 365, some enterprises and vertical industries are seeing over 70% of their traffic as encrypted.

THE ISSUE: An overwhelming number of network-based security products including Firewalls, Next Gen Firewalls, IPS/IDS, Sandboxing, Network DLP and Web Proxies, simply *IGNORE* encrypted traffic because they cannot decrypt it, or because the performance/level of effort is too much to bear. And as security investments increase, organizations are degrading their own investments because they are blind to encrypted data moving in and out of the network.

THE RISK: The cyber criminals are utilizing this blind spot with today's advanced threats and malware by increasingly using SSL/TLS encrypted traffic to avoid detection and exfiltrate proprietary data. Gartner states that more than 50% of all threats will use SSL/TLS by 2017.

THE FINANCIAL IMPACT: In an overly simplified straight-forward analysis, from the time an organization implements a network based security solution, it will only ever be as valuable as the percentage of traffic it can see. Every organization has a Network Security Blind-Spot cost which is the percentage of SSL traffic multiplied by the overall investments previously made in network security products listed above. Simply:

NETWORK SECURITY BLIND-SPOT COST =

% of SSL Traffic * Annual Investment into Network Security Products

In looking at an example over the long term, suppose a large Enterprise with 35% of network traffic currently encrypted and increasing 20% year-over-year, has an annual ongoing investment of $2M in network controls. Here are the resulting Network Security Blind-Spot costs:

YEAR	% SSL Traffic Per Year	Estimated Investment per year into Network Security Products	Decreased Value of Investment due to NO SSL Decryption	Annual Network Security Blind-Spot Cost to the Organization
Year 1	35%	$2M	$1.3M	$700K
Year 2	42%	$2M	$1.16M	$840K
Year 3	50%	$2M	$1M	$1M
Year 4	60%	$2M	$800K	$1.2M
Year 5	72%	$2M	$560K	$1.44M

THE ANSWER: To counteract this issue, the inbound/outbound and cloud-based enterprise SSL traffic needs to be decrypted once, and then distributed to the installed security technologies for further processing and analysis. This immediately delivers the value that was originally anticipated and helps reduce the cost to zero. It also helps

preserve and extend the long-term investment in the infrastructure as the network traffic patterns evolve. In the end, simply doing this will raise an organization's Security Visibility quotient. As SSL-based traffic is decrypted once and effectively distributed to all of the invested technologies, it will increase the infrastructure investment value in-and-of-itself, while eliminating the Network Security Blind-Spot.

ADDITIONAL COSTS: While some individual point products may do some form of SSL decryption – third parties such as NSS Labs have found performance degradation of 80% on NGFW type technologies, or they have seen that SSL decryption is supported but only for a limited number of weak cipher suites. In addition to the performance challenges and lack of advanced crypto support, there is the cost of "over sizing" some of these security technologies by adding 2 to 3 times the hardware capacity.

MANAGE THE RISK: With the Network Security Blind-Spot Cost reduced and a strategy for enterprise wide encrypted traffic management implemented, the ability to evaluate, monitor and manage risk becomes significantly easier and the value of your security investments are fully achieved. Furthermore, applying advanced policies to SSL traffic to inspect and decrypt or not (i.e. don't decrypt and inspect traffic containing financial or healthcare sites) is becoming an industry standard and best practice requirement for compliance and due diligence.

KNOW YOUR NETWORK SECURITY BLIND-SPOT - WHAT DO YOU ASK?:

- Technical Questions:
    - What % of your network traffic is encrypted?
    - What is your strategy for inspecting and managing inbound and outbound SSL with your current security tools?
    - What performance issues occur when enabling SSL inspection on your current security devices?

- Risk Management Questions:
    - Is protecting and extending your ROI on your existing network security solutions important to you?
    - How much has your organization invested in Firewalls, Sandboxing, Malware analysis and detection, Proxies, Network DLP and IDS/IPS?
    - How do you identify, block and remediate threats that come in through encrypted communications?

For more information:

- Contact your local Blue Coat Authorized Security Partner or Account Manager
- Contact Blue Coat directly: https://www.bluecoat.com/contact-us and set up a 30 minute call for Best Practices on establishing a baseline for measuring and analyzing your SSL/TLS encrypted traffic.
- Contact: Kevin Reardon, VP, Worldwide Value Strategy – kevin.reardon@bluecoat.com
- Learn more: www.bluecoat.com/uncoverssl