Business Challenge
Targeted phishing remains the number one cyber-attack vector, contributing to over 95% of successful breaches and threatening the overall security posture of enterprises worldwide. Focused on the earliest stages of an attack, Area 1’s unique Cyberattack Preemption solution works with Symantec’s Blue Coat ProxySG to provide advanced visibility and prevention of targeted phishing attacks. As enterprise security teams deal with the sophisticated and focused nature of these attacks, the need for getting greater visibility into these attacks and the ability to take action against them at the earliest stages of an attack cycle becomes critical.

Solution: Blue Coat ProxySG and Area 1 Horizon
The combination of the Blue Coat ProxySG together with Area 1 Horizon helps enterprise security teams identify targeted phishing campaigns, attacker infrastructure and delivery mechanisms from the outside in to give advance warning and stop these attacks during the earliest stages of an attack cycle. This unprecedented visibility provides significant time advantage ranging anywhere from days to weeks ahead; as well as actionable context that enterprises can use to stop an attack before it hits them.

Area 1 Horizon is powered by globally distributed ActiveSensors™ to monitor real-time actor activity, and emergent and active threat campaigns across the web. Additionally, advanced small pattern analytics engine (SPARSE™) uncover attacker methods, techniques and infrastructure by utilizing sophisticated data learning models. The service integrates flexibly and transparently with ProxySG appliances deployed as edge proxies to preempt targeted phishing attacks that are getting past existing perimeter defenses.

As edge proxies, the ProxySG provides a real-time perimeter defense using the power of the Symantec Global Intelligence Network, along with layered defenses including multiple AV engines, sandboxing, black/whitelisting and static code analysis. In the case an event does happen, the ProxySG logs all user activity in extremely detailed logs for use by incident response and forensics tools.

How it Works
The diagram below demonstrates how Symantec and Area 1 Security work together to preempt phishing attacks.

Area 1 Horizon works with edge deployed the ProxySG appliances, dynamically pushing pre-configured rulesets for protection against targeted phishing attacks. The solution integrates through a custom connector or through a configured link to the Area 1 cloud service; and appears as a local block list on the edge proxy. Using the ProxySG appliance, customers have the ability to configure a range of custom policies on Area 1 rulesets consistent with their security requirements. Any actions taken locally...
are captured for reporting and analytics shown through the Area 1 Horizon portal. Leveraging their existing Symantec infrastructure, customers can ensure proactive defense against a range of targeted attacks and improve their overall security stance.

Benefits
The combined ProxySG and Area 1 Horizon solution:
- Pre-empt an additional range of targeted attacks such as advanced phishing, ransomware and socially engineered threats.
- Actionable intelligence with deep context into threat origins, vector, type and targets.
- Focused and pre-emptive attack indicators for the most damaging threats, extending beyond well known, volume based, or easily identified commodity attacks.
- Area 1’s transparent cloud-based deployment with no change to existing security infrastructure.
- Augment your edge security while leveraging current workflow and operational processes established through your existing Blue Coat deployments.

About Area 1 Security
Backed by top tier investors, Area 1 Security is led by security and data analytics experts coming from NSA, USCYBERCOM, Cisco/IronPort and FireEye who realized a pressing need for a proactive solution to targeted phishing attacks. Area 1 is working with some of the most sophisticated security organizations including F500 banks, insurance providers, retail organizations and health care providers to preempt and stop targeted phishing attacks at the outset and significantly improve their cyber security posture.

To learn more, please visit: https://www.area1security.com

For More Information
Learn more about Blue Coat technology partners on our website.