Security, Visibility and Replay

Breach Containment

BAYAN ACHKAR - Senior Systems Engineer
Security Challenges

Advanced Threat Protection Requires

1. Context
2. Content (Forensics, not just logs)
3. Rapid Time To Detection
4. Rapid Time to Response
   (quickly determine kill chain / root cause / impact / mitigation strategy)
5. SSL Visibility

SSL Blind spot
Delivery Mechanism for 50% of all Malware by 2017

SIGNATURE-BASED DEFENSE-IN-DEPTH TOOLS

NGFW
IDS / IPS
Host AV
Web Gateway
SIEM
Email Gateway
DLP
Web Application Firewall

Unknown Threats
- Novel Malware
- Zero-Day Threats
- Targeted Attacks
- Modern Tactics & Techniques

Known Threats
- Known Malware
- Known Files
- Known IPs / URLs

Traditional Threats
- Novel Malware
- Zero-Day Threats
- Targeted Attacks

Modern Tactics & Techniques
- Unknown Threats

SSL Visibility
Delivery Mechanism for 50% of all Malware by 2017
GARTNER: ADAPTIVE SECURITY ARCHITECTURE FOR ATP

Five Styles of Advanced Threat Defense

- **Network Traffic Analysis** (Style 1)
- **Network Forensics** (Style 2)
- **Payload Analysis** (Style 3)
- **Endpoint Behavior Analysis** (Style 4)
- **Endpoint Forensics** (Style 5)

Source: Gartner (August 2013)
Blue Coat is the leader in enterprise IT security, providing on-premise, hybrid and cloud-based solutions to help protect web connectivity, combat advanced threats, and respond to security breaches.

From Surf Control to Riding the Security Wave
# Blue Coat Security Platform

## Advanced Web and Cloud Security
- **Advanced Threat Protection**
- **Encrypted Traffic Management**
- **Incident Response, Analytics and Forensics**
- **Protecting Web Applications**
- **Network Performance and Optimization**

### On-Premise Secure Web Gateway
- **Content Analysis**
- **SSL Visibility Appliance**
- **Security Analytics**
- **Web Application Firewall**
- **PacketShaper**

### Cloud-Delivered Secure Web Gateway
- **Malware Analysis**
- **Cloud Data Protection**
- **Reverse Proxy**
- **MACH5**

### Cloud Access Security Broker
- **Mail Threat Defense**
- **CacheFlow**

---

### Global Intelligence Network

### Common Operating Environment

### Robust Policy Infrastructure & Open Architecture

### Blue Coat Research Labs

### Global Cloud Operations
Industry recognition

BLUE COAT A LEADER IN GARTNER MAGIC QUADRANT
8 CONSECUTIVE YEARS: SECURE WEB GATEWAY CATEGORY

CHALLENGERS

LEADERS

Cisco

Zscaler

Fernco (formerly Raytheon Websense)

Intel Security (McAfee)

Niche Players

Barracuda Networks

Trend Micro

Sangfor

CloudKerberos

Symantec

Visionaries

As of June 2016
Global Intelligence Network

NETWORK EFFECT OF 15,000 CUSTOMERS

INTELLIGENCE FED BY THE LARGEST AND MOST COMPLEX IT ENVIRONMENTS IN THE WORLD

75+ MILLION USERS

OVER 1 BILLION REQUESTS TO PREVIOUSLY UNSEEN LOCATIONS PER DAY

- URL Threat Risk
- Multiple Threat Engines
- Behavioral Analysis
- Sandboxing
- Static Analysis
- Sandboxing
- Active Script Scrubbers
- Machine and Human Analysis
- 55 Languages
- 300 Realtime Web Rating Libraries
SSL/TLS Traffic is PERVERSIVE and Introduces risk

SSL is estimated at 35 - 50% of network traffic and growing 20% annually*
  • >70% in some industries (e.g. healthcare)

Advanced Persistent Threats (APTs) increasingly use SSL as a transport
  • Dyre trojan (Command & Control)

*Source: Gartner
SECURITY Industry Confirmation

SSL Inspection is a Security Best Practice
“Implement a Secure Sockets Layer (SSL) inspection capability to inspect both ingress and egress encrypted network traffic for potential malicious activity”.

— Alert TA14-353A: Targeted Destructive Malware (Dec 2014)

https://www.us-cert.gov/ncas/alerts/TA14-353A

“The average performance loss across 7 NGFWs when SSL inspection is enabled is 81%...”

https://salesportal.bluecoat.com/#workspaces/UG9ydGFs/directories/05850000000CqKDAA0/files/06850000001US4bAAG
Privacy and compliance issues stall Decryption Projects

LEAD TO REQUIREMENTS
1) Manage what type of information is decrypted
2) Assure custody and integrity of encrypted data
Preserve privacy and compliance while enabling security

Selective Decryption enables ‘Blacklist’ and ‘Whitelist’ Policies

• Host Categorization Service
• Leverages the Blue Coat Global Intelligence Network
  • Utilizes 80+ categories, in 55 languages
  • Processes +1.2B web and file requests per day
• Easily customizable per regional and organizational needs

Policy Examples
• Block or decrypt traffic from suspicious sites and known malnets
• Bypass / Do not decrypt financial and banking-related traffic
Cost-Effectively Enhance The Existing Security Infrastructure

- Efficient, ‘Decrypt Once – Feed Many’ design for active and passive security devices
- Avoid increased hardware capacity costs
- Ensure data integrity and active device response/verification
- Deliver a more comprehensive threat defense system
ASG and the Threat Protection Lifecycle

- URL Category
- URL Risk Score
ASG and the Threat Protection Lifecycle

- URL Category
- URL Risk Score
- Hash Score
- Hash Reputation
- Malware Engines
- Static Analysis
- Behavioral Detonation
ASG and the Threat Protection Lifecycle

- URL Category
- URL Risk Score
- Hash Score
- Hash Reputation
- Malware Engines
- Static Analysis
- Behavioral Detonation
- Malware Signatures

Copyright © 2016 Blue Coat Systems Inc. All Rights Reserved.
ASG and the Threat Protection Lifecycle

- URL Category
- URL Risk Score
- Hash Score
- Malware Signatures
- Machine Learning
- Static Analysis
- Behavioral Detonation
ASG and the Threat Protection Lifecycle

- URL Reputation
- Hash Reputation
- Malware Engines
- Static Analysis
- Behavioral Detonation

63M Web Request
12M Scanned via Malware Engines
18K Sandboxed

- Hash Score
- Malware Signatures
- Machine Learning
- Behavioral Detonation

Intelligent Defense In Depth
Stage 2: analyze & Mitigate

Malware Analysis Appliance
Next-Generation Sandboxing

Dual-Detection Hybrid Analysis of Suspicious Samples
Closely Replicates Customer’s Gold Configurations
Automated Risk Scoring and Rich Analysis

Quickly analyze and prioritize advanced and zero-day threats for remediation and continuous security improvement
### Modern Malware Characteristics

**WHAT IS NEXT-GENERATION MALWARE?**

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique</td>
<td>No pre-existing signatures exist</td>
</tr>
<tr>
<td>Targeted</td>
<td>Can’t rely on others to have found it</td>
</tr>
<tr>
<td>Polymorphic different</td>
<td>Every variant is just a little bit</td>
</tr>
<tr>
<td>Short-lived</td>
<td>24-hour distribution and C&amp;C domains</td>
</tr>
<tr>
<td>Low and slow</td>
<td>Tries not to call attention to itself</td>
</tr>
<tr>
<td>VM–Evasive behavior</td>
<td>Sandbox-aware, can alter its</td>
</tr>
<tr>
<td>“Sleeper Cell” malware</td>
<td>Attempts to wait out a sandbox</td>
</tr>
<tr>
<td>Multi-stage and multi-vector</td>
<td>Email, web, and file components</td>
</tr>
<tr>
<td>Encrypted</td>
<td>Slips in, can’t see what it’s doing</td>
</tr>
</tbody>
</table>

---

**So how do you stop it?**
Stage 2: analyze & Mitigate

1. Emulation stack: known as the Sandbox.
2. Virtualization stack: known as the Intelligent VM-IntelliVM.
3. Android iVM & Cloud IOS/OSX.

Example Scenario:

Malware issues a sleep call that lasts for ten days → Malware won't be seen executed.

Bluecoat Sandbox to ‘trick’ malware

The emulation technology in the Sandbox covers the entire machine - from the BIOS to a fake network - and so we see (and control) all API calls in the Sandbox.

Once the sleep call is issued by the malware, the length of time specified is irrelevant; we can tell the malware that it has slept by returning the appropriate result code.

The malware then thinks that its sleep has finished, and it starts to execute the rest of its payload.
Investigate & Remediate

Security Analytics Platform

Full Security Visibility of All Network Traffic

Forensic Details Before, During and After an Alert

Reduce Time-to-Resolution and Breach Impact

The Security Camera for Your Network
### Security Analytics Platform

**THE SECURITY CAMERA FOR YOUR NETWORK**

*Turing Complexity into Context*

- **Providing real-time analysis and full visibility of everything going in and out of your network**
- Records, classifies and indexes all packets and flows on high-speed networks
- DPI classification of over 2,000 applications and thousands of meta attributes
- On the wire, *real-time* visibility and analysis of data exfiltration & infiltration
- Security Context – including reputation, user and social personas, artifacts
- The ‘Black Box’ for incident response, forensics, root cause and impact analysis

Copyright © 2016 Blue Coat Systems Inc. All Rights Reserved.
Security Camera for your network: Full visibility of all traffic

- Complete, lossless packet capture on high-speed network (24/7 – all ports/all traffic)
- Comprehensive DPI with layers 2-7 indexing (over 2000 applications classified)
- Actionable intelligence and event reconstruction (full packet, flow, session & file reconstruction)
- Chronological display of all network events validates compliance and acceptable use policies
- Scalable deployment as either appliance/software/virtual appliance for days/weeks/months of traffic
Security Camera for your Network: Details for every alert

• Know what happened before, during and after an alert, with complete, clear supporting evidence
• Multiple sources for real-time integrity & reputation of URL, IP address, file hash or email address
• Trace back and discover Tactics, Techniques & Procedures and identify Indicators of Compromise
• Integrated workflows with leading network and endpoint security tools to add context and improve effectiveness
Security camera for your network: reduce time-to-resolution

• Retrospective forensics analysis on any attack
• Answer critical “post-breach” questions that plague CISOs – how? what? who? when? ...
• Root Cause Explorer quickly identifies the source of attack, reducing time-to-resolution
• Faster time to identification/action/reaction with Security Analytics allows up to 85% faster resolution
• Blue Coat Global Intelligence Network updated with newly-discovered threat intelligence
REAL TIME ANALYSIS
Real-time Threat Analysis

Enriching Decisions
Real-time Threat Analysis

*Enriching Decisions*
Real-time Threat Analysis

*Enriching Decisions*
Real-time Threat Analysis
Enriching Data & Decisions
Real-time Threat Analysis

*Enriching Data & Decisions*
Real-time Threat Analysis

*Enriching Decisions*

- INTERNET
- TAP/SMART TAP
- INTERNAL NETWORK
- SECURITY ANALYTICS & MALWARE ANALYSIS
- UPDATE
  - NGFW
  - IPS
  - ENDPOINT...
  - SIEM
  - EMAIL
  - EDR

---

Copyright © 2016 Blue Coat Systems Inc. All Rights Reserved.
Open Integration – Solid Partnerships

Security Analytics Platform Supports Best-of-Breed Integrations