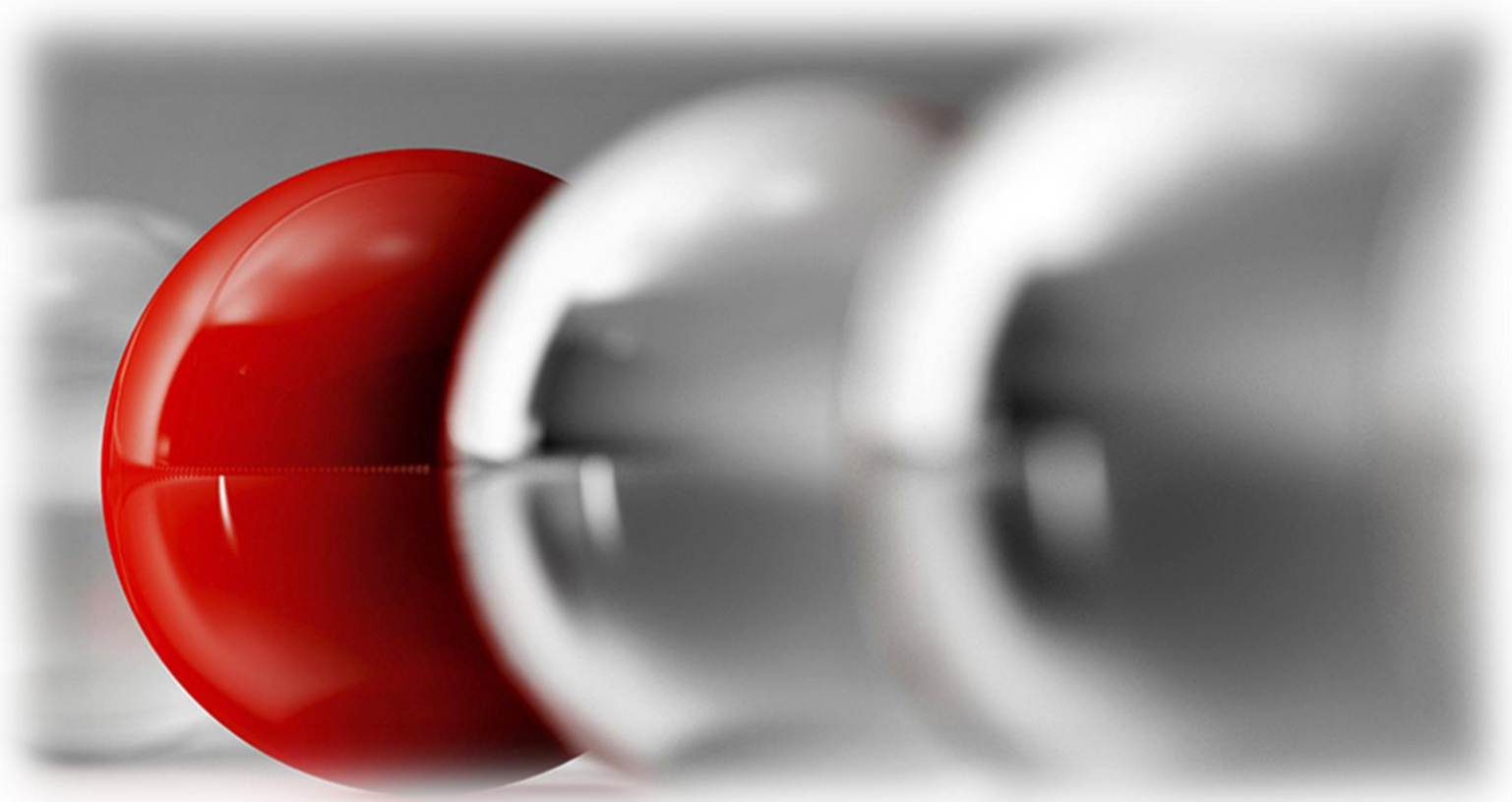


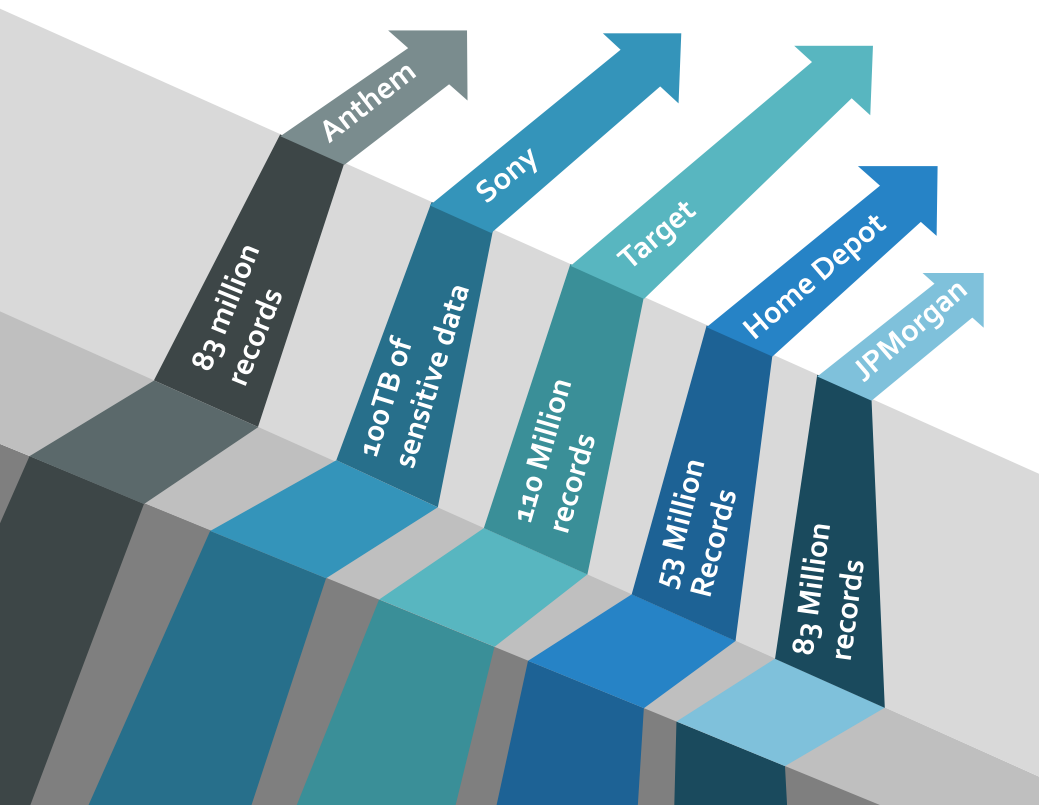
Detecting Threats Via Network Anomalies



Paul Martini
Cofounder and CEO
iboss Cybersecurity



Why is Anomaly Detection Important?



- **Largest enterprises with the biggest investment in prevention are still getting breached**
- **Signatureless defenses like sandboxes are being evaded**
- **Even solutions that can find active infections or C&C callbacks, can't stop data exfiltration**

Evasive Malware *Will* Find a Way into Your Network

- **Using non-standard ports: High streaming UDP ports**
- **Tunneling through allowed protocols: SSL, SSH, DNS**
- **Using circumvention protocols such as TOR**



Malware *Will* Get Past Your Sandbox

- **By detecting virtualization software**
- **Comparing files against known sandbox profiles**
- **Mimicking innocuous software so it can pass through undetected**
- **Sleeping until human movement is detected**
- **Hiding code in a registry key so there's no file presence**



Once You're Infected, Dwell Time Starts Ticking

- **It's the gap between when an active infection gets in your network and when it is detected**
- **The longer the dwell time, the greater the data loss**
- **Preventive measures can't reduce dwell time**



Dwell Time is Your Biggest Enemy

- **Data can leave the network unnoticed via different routes**
- **How will you know:**
 - **What data has been compromised?**
 - **How much data was lost?**
 - **Where did it go?**
 - **Is it still being exfiltrated?**



Cloud File Storage

Anthem breach involved data uploaded to cloud storage



Home and Small Business Servers

TOR exploits leverage unprotected home computers and small business networks



50+ Connections

Suspicious number of connections with small payload continuously sent

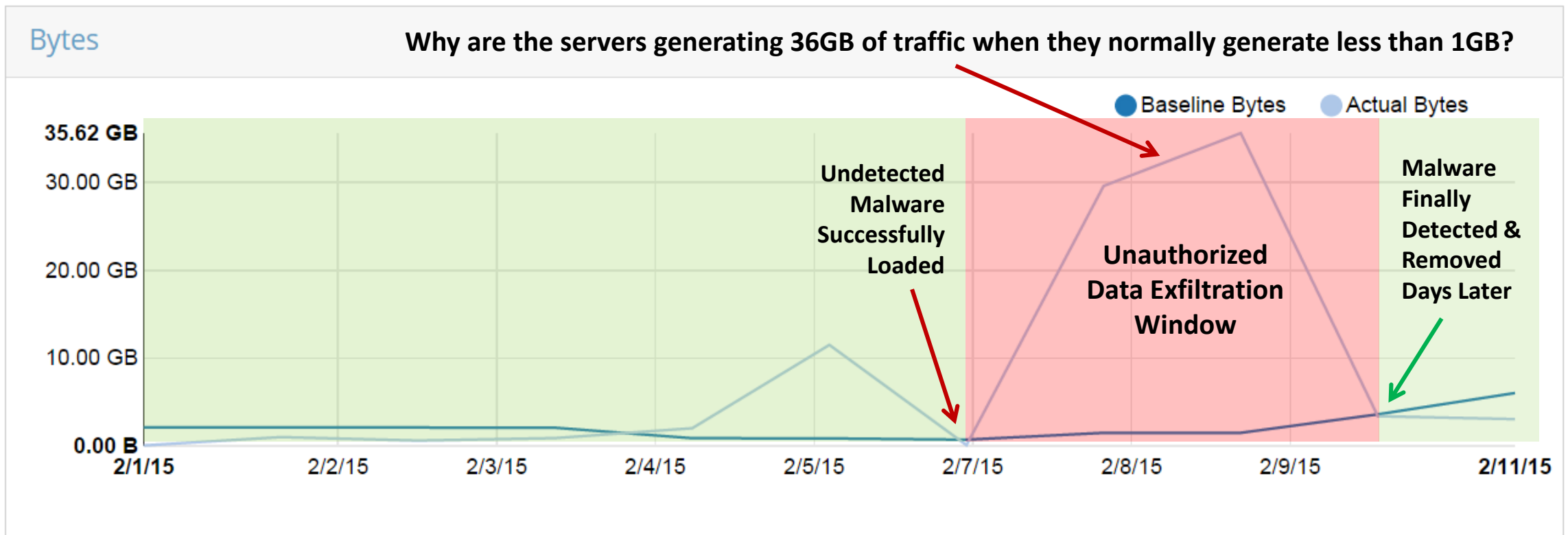


Large Transfer

Large amount of data leaves over the weekend to location in China

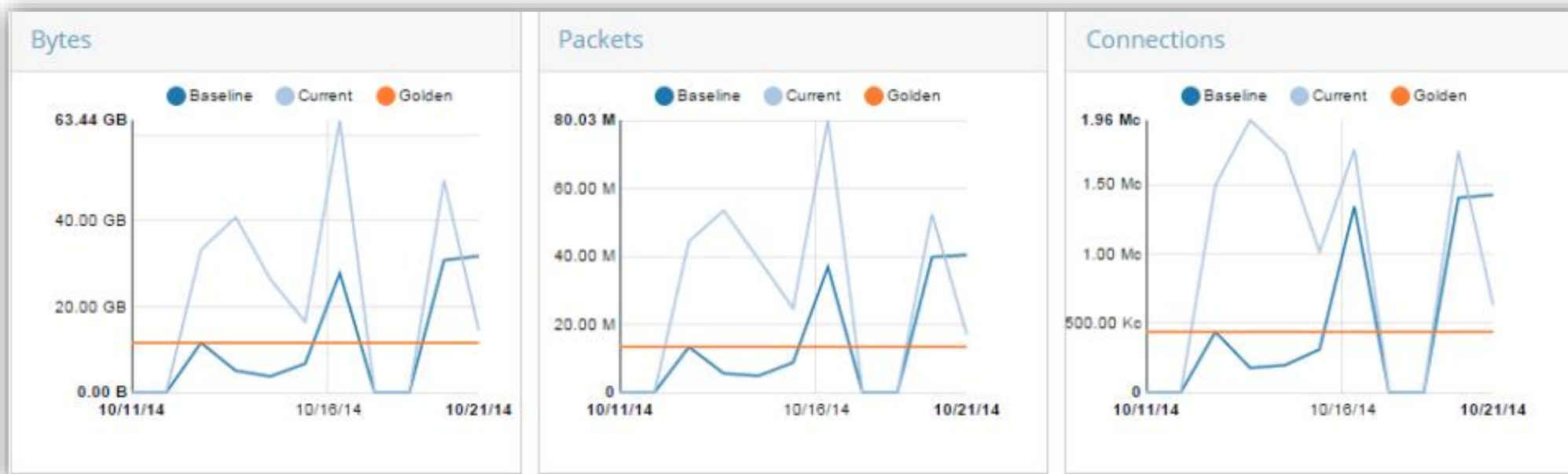
Analyze Outbound Traffic Anomalies

Reduces dwell time by detecting changes in data behavior from normal and alerts regardless of signature-based malware communication



Create Smart Network Baselines

- **Baseline sensitive servers hosting sensitive data**
- **Alert & respond on anomalous transfers to high risk countries**
- **Use baselines that adaptively learn normal data behavior**



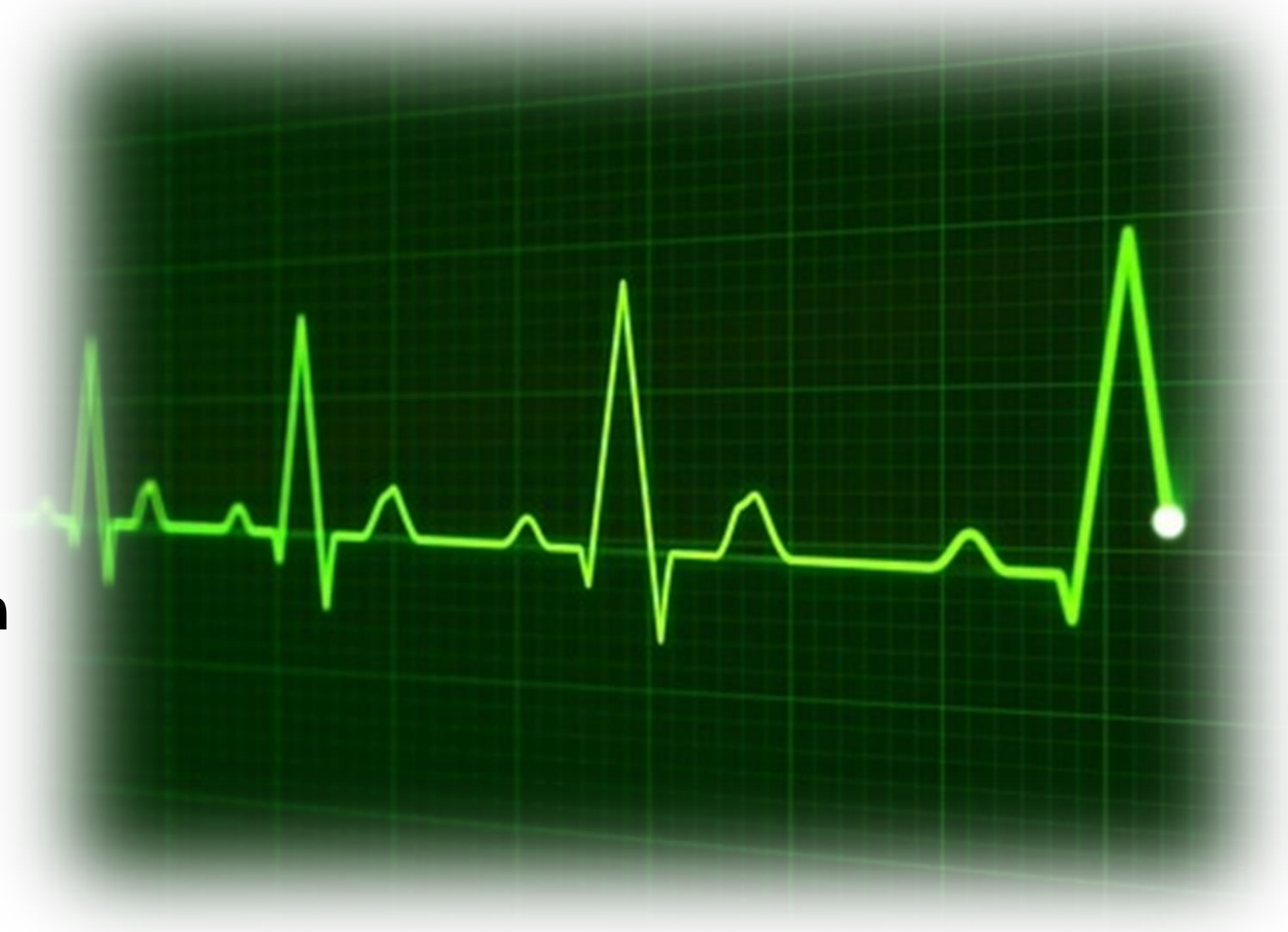
Monitor Network Servers & Devices

- **Choose the objects you want to measure**
 - Individual devices: Desktops, Servers, Tablets
 - Network subnets such as BYOD wireless networks, database servers
- **Decide how and when to measure, what are the best parameters?**



Monitor Critical Systems

- **Track abnormal behavior with continuous monitoring of**
 - **Bytes in/out**
 - **Number of connections**
 - **Number of packets**
 - **Protocol**
 - **Communication destination**



Automatically Contain Data Exfiltration

- **Automatically stop suspicious transfers regardless of malware detection**
- **Allows normal traffic to pass, while containing compromised traffic**
- **Apply triggers per server, device, location, users/group, size, connection, destination**



Remediate in Real Time

- **Its critical to receive actionable intelligence: the complete context of threats allows you to remediate quickly**
- **With answers to:**
 - Who and what devices were involved?
 - When and where did it originate?
 - What were its callback destinations?
 - Is it truly over?
 - Historical evidence: Can it happen again?



So How Do We

CLOSE

This Gap?



By increasing investments in post infection pre-detection monitoring (dwell time)

- Monitor traffic, report on infections and automatically contain data exfiltration (not relying on Netflow)
- Apply network baselining to detect anomalous traffic bi-directionally

Inventory the security solutions on your network:

SOLUTIONS YOU MAY HAVE:

- SWG
- Firewall
- IPS
- File Sandboxes



And look for technologies which detect & contain data anomalies





CAPABILITIES TO CONSIDER:

- Network baselining to continuously monitor for anomalies and alert your team in real time to reduce infection dwell time
- Contain these anomalies to allow you to respond and reduce data loss


Thank you!


For more information contact us below


 www.iboss.com

 info@iboss.com

 facebook.com/ibossconnect

 [@ibossconnect](https://twitter.com/ibossconnect)

 linkedin.com/company/iboss-network-security

 1 (877) 742-6832

