Welcome to Guadeloupe and the 51st Meeting of WG 10.4!

WG 10.4 Workshop on Critical Infrastructure Protection

Rick Schlichting

Director, Software Systems Research
AT&T Labs - Research

Acknowledgments

Many thanks to:

- Karama Kanoun (LAAS/CNRS)
- Bill Sanders (UIUC)
- Paulo Verissimo (Univ. of Lisboa)
- speakers

Scope and importance of CIP

AT&T as an infrastructure provider

Critical Infrastructures

- Telecommunications
- Transportation
- Water systems
- Banking and Finance
- Electrical power
- Oil and gas
- Emergency services
- Continued government

The government identifies some national infrastructures as being *critical*

- Each of them is controlled by computers and networks
- Each of them has special needs for
  - Protection against malicious attacks
  - Sound engineering design principles
  - *Evaluation* of their trustworthiness

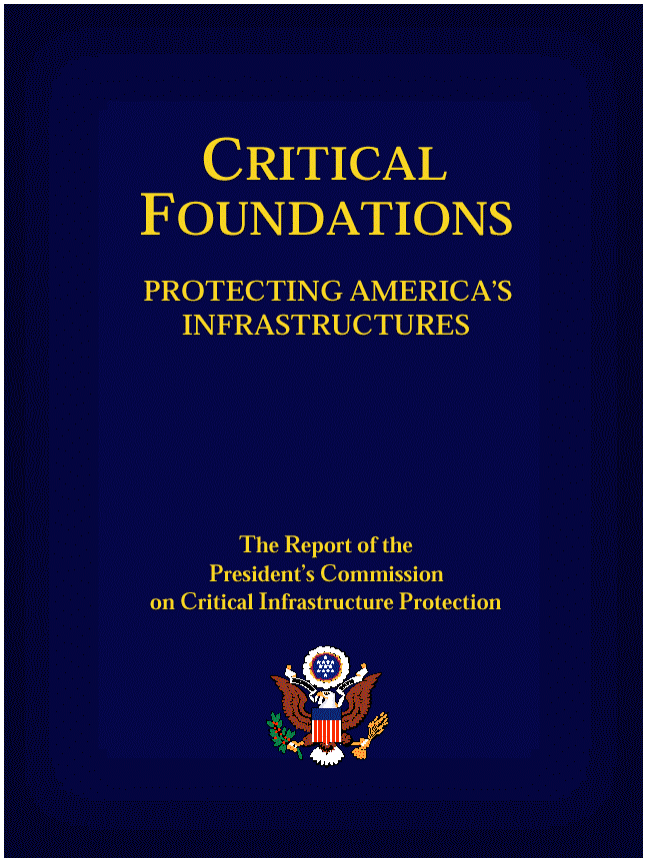
ITI

The Nation's Critical Infrastructures are at Risk

- **From "Critical Foundations: Protecting America's Infrastructures," Report of the President's Commission on Critical Infrastructure Protection, 1997:**

"...The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence.

"This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk."



ITI

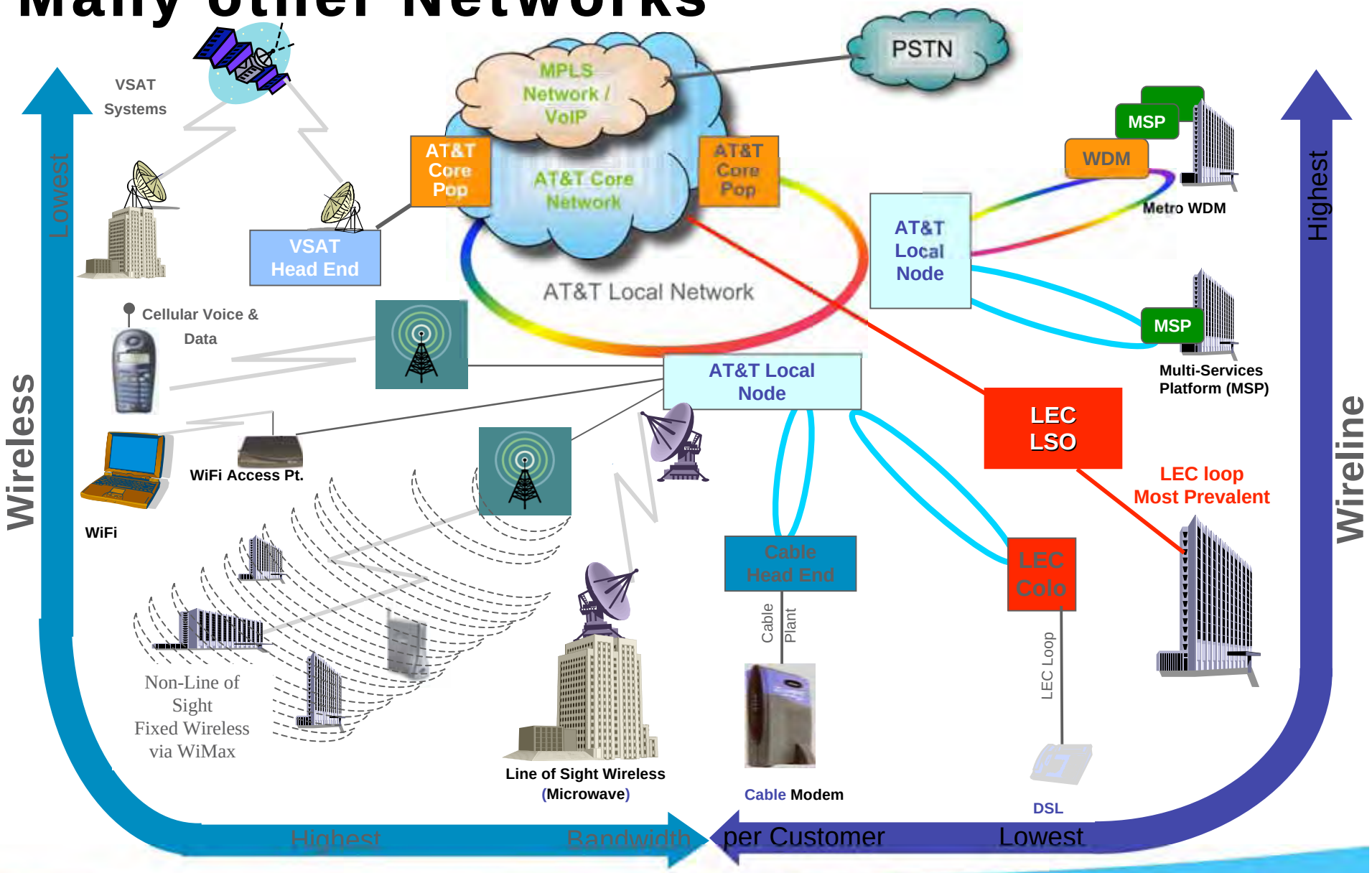
The AT&T Global Network

Over 5.4 Petabytes of Traffic Average Business Day

MPLS-based Services in 127 countries at 1500+ service nodes
112,000+ MPLS customer ports
30 data centers on 4 continents
Over 525,000 route miles

at&t

Many other Networks



CIP and AT&T

Importance

- As as a *user* of CIP techniques and technology
- As a *developer* of CIP techniques and technology
- As a *provider* of CIP techniques technology to enterprise customers

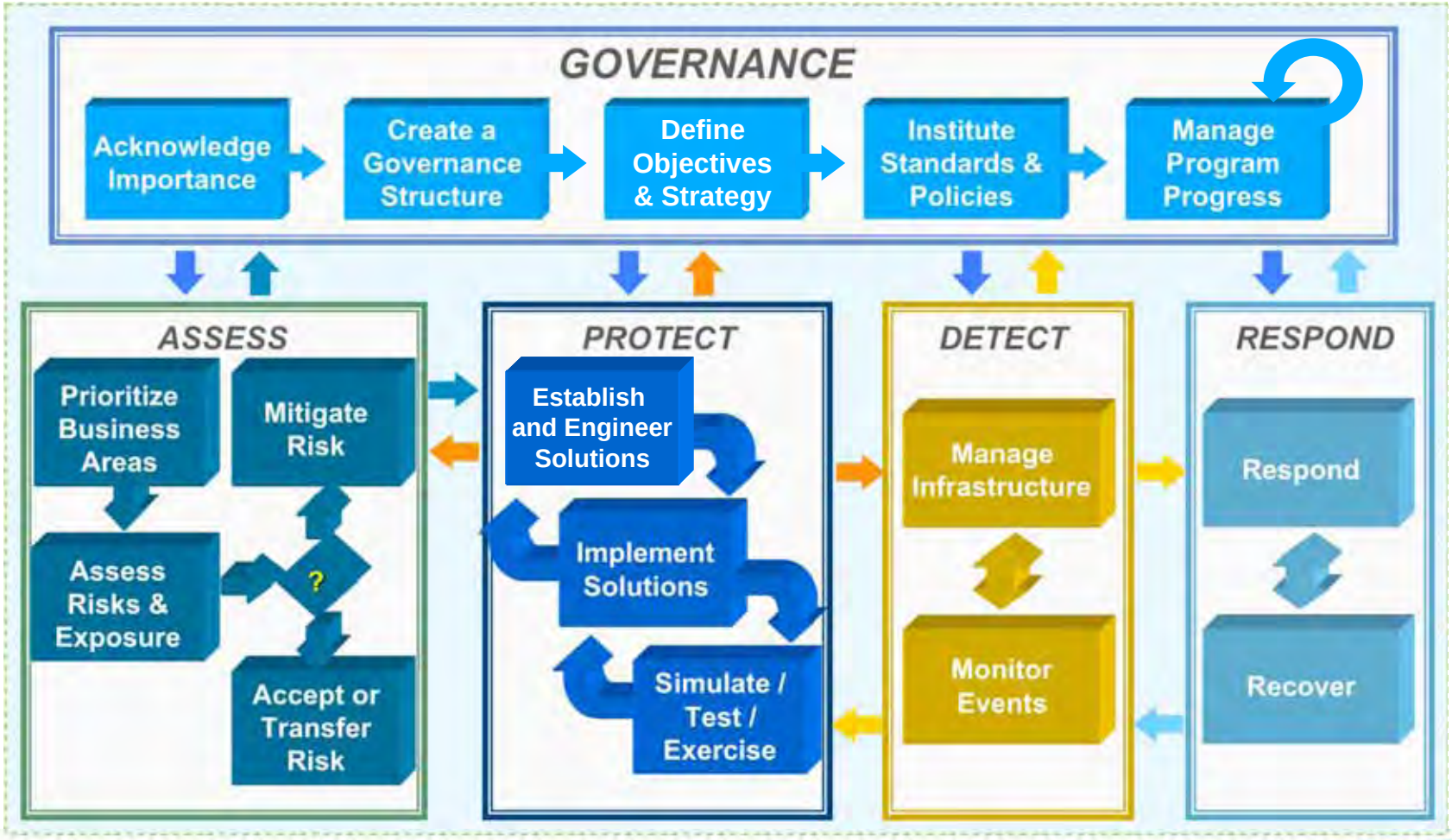
Focus

- Traditional: Physical protection of assets and provisions for recovery (e.g., Network Disaster Recovery trailers).
- Cyber attacks: Network monitoring and control; moving security *into* the network.

↳ Owning and operating the infrastructure is key

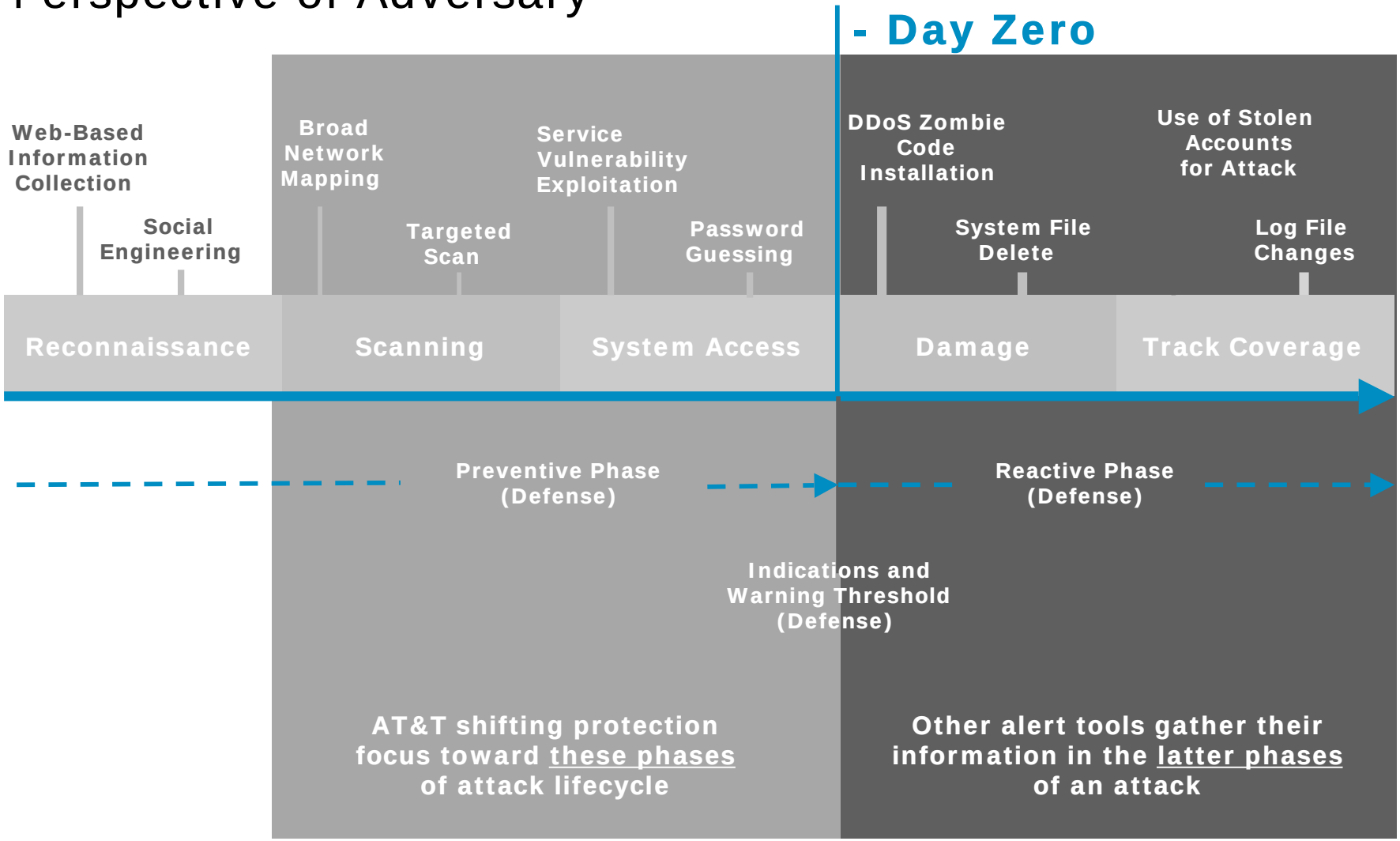
AT&T Security Best Practices

Proven Processes, Capabilities & Expertise



Cyber Attack Strategy

Perspective of Adversary



Proactive Security Alert Notification

AT&T Labs – Security Forensics Experts
AT&T Labs – Research Statisticians
AT&T GNOC – Security Technicians

AT&T FLOOD System
Analyzes 100% real-time streaming data
Auto-correlation anomalies and mitigation actions

Optical Splitters (Gateway Routers)

AT&T can detect worm and virus attacks before they are launched

AT&T Security Analysis of Network Flow Data

Activities

- Attempt to predict threats
- Attempt to detect threats in real-time
- Provide data for post-analysis of network activity

Inputs

- Metadata (flow records, registry data, routing data, network topology data…)
- Selected AT&T destined content data (packets based on a “tasked” filter)

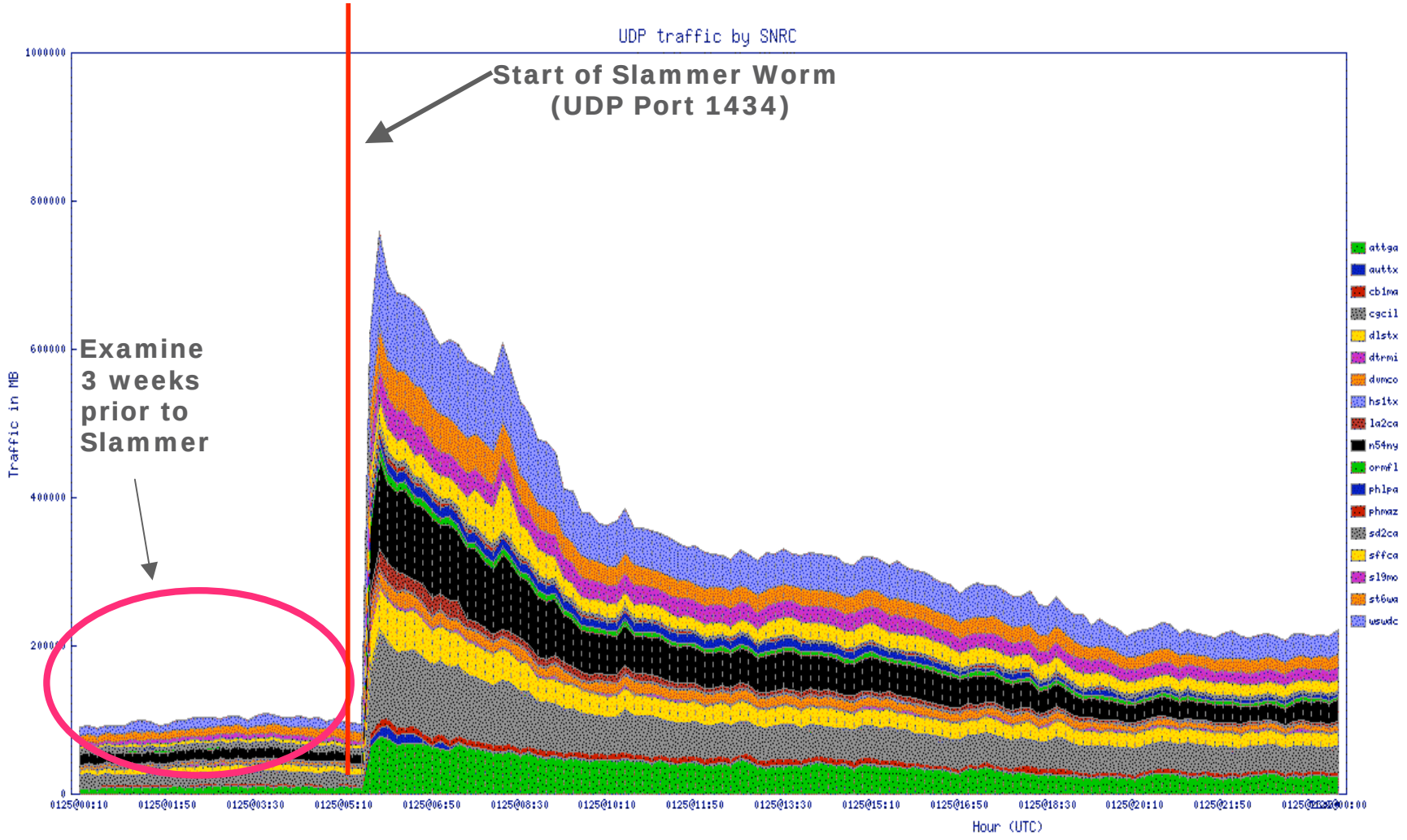
Protect customer privacy

- Incorporate specific security guidelines, control of platform functions, and strict data handling methods & procedures
- Operate in accordance with AT&T Privacy Policy.

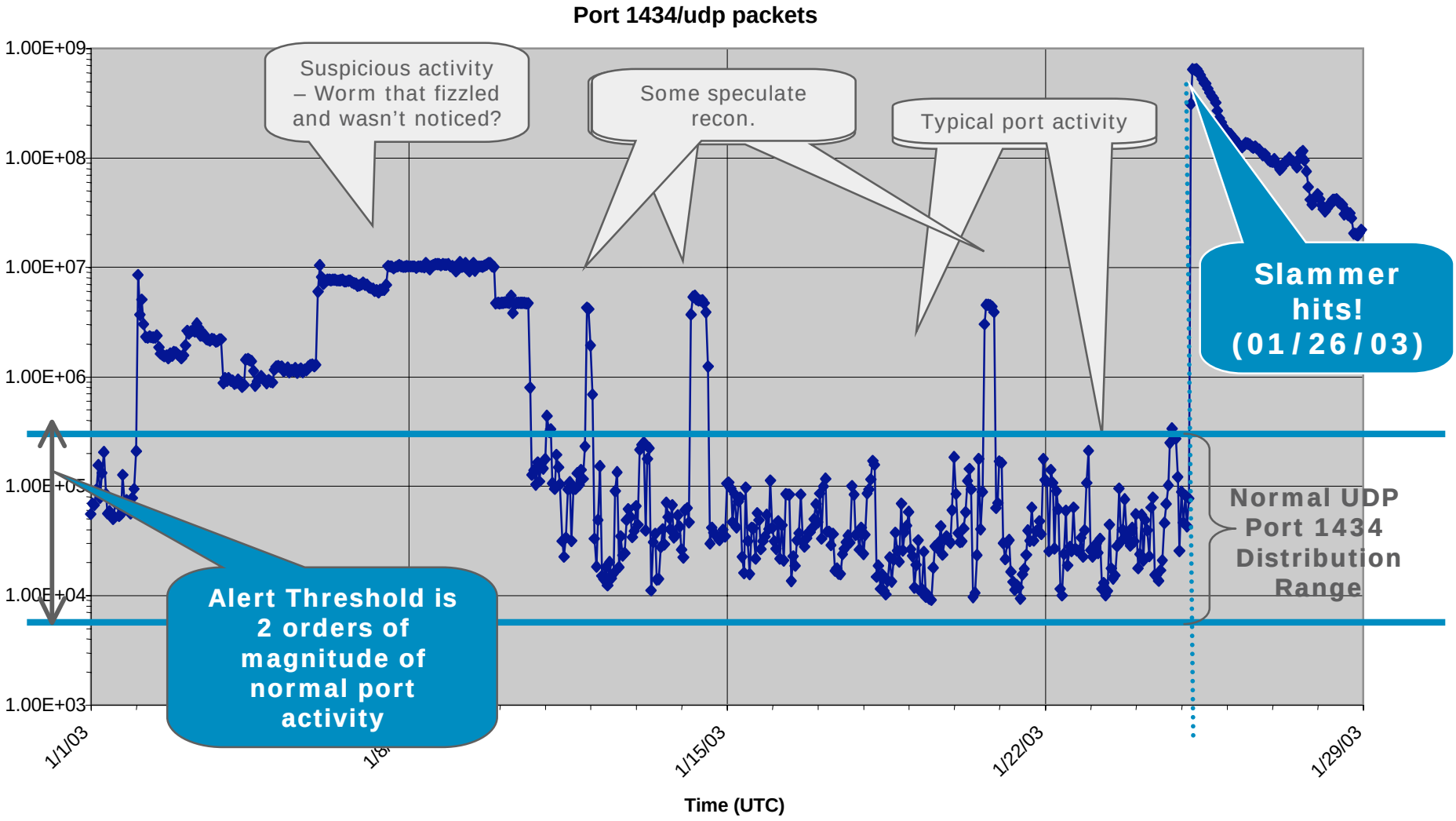
Detect, identify, quantify, and locate potential threats to AT&T’s internal systems, services, and/or clients

AT&T Security Analysis of Network Flow Data

UDP Port Indication of Slammer Worm



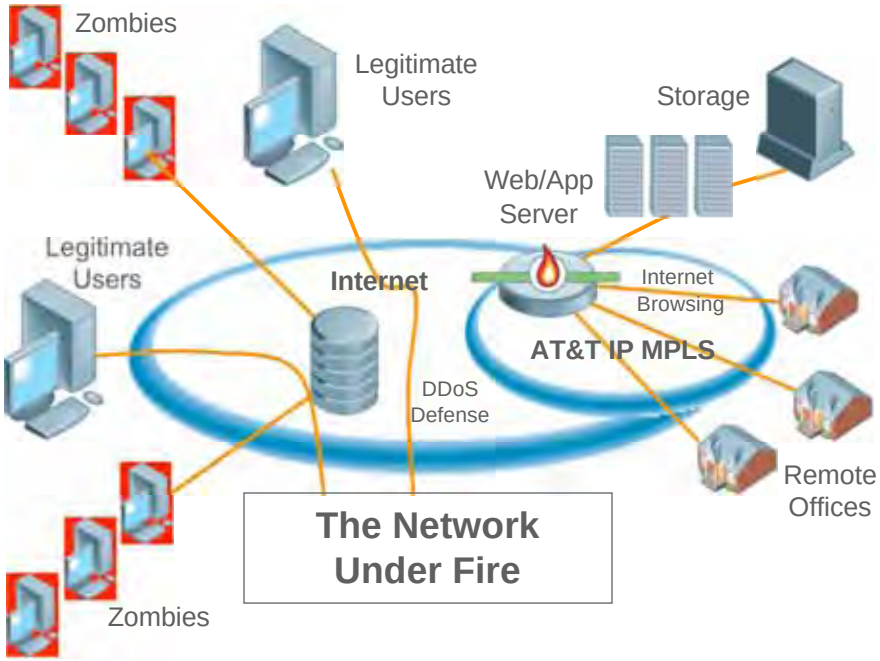
SQL Slammer Observation



Slammer attack occurred on 1/26- can provide recommended mitigations at least 2 weeks earlier!

AT&T Security Portfolio

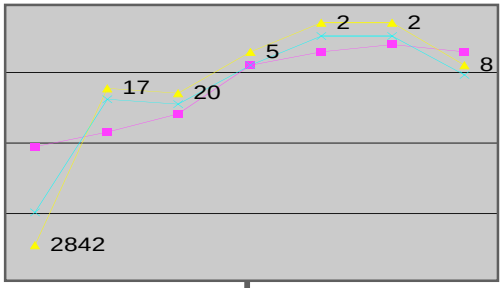
A Defense-In-Depth Approach



- **AT&T Internet Protect®**
  - **DDoS Defense**
  - **AT&T Internet Security News Network**
- **AT&T Managed Firewall**
  - **Network-Based**
  - **Premises-Based**
  - **Personal**
- **AT&T Token Authentication**
- **AT&T Intrusion Detection / Prevention**
- **AT&T Secure E-Mail Gateway**
- **AT&T Professional Services**

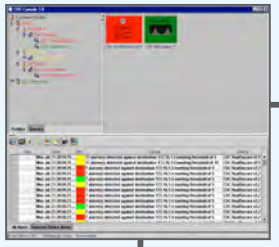
AT&T Identifies Vulnerabilities

Correlation Across Network, Servers & Applications



Security Analysis
(Profile/Anomaly Based)

Real-Time
Alerts & Alarms
with Severity &
Likely Source



AT&T Security
Professionals

Profiling Engine
"What You Expect as Normal"

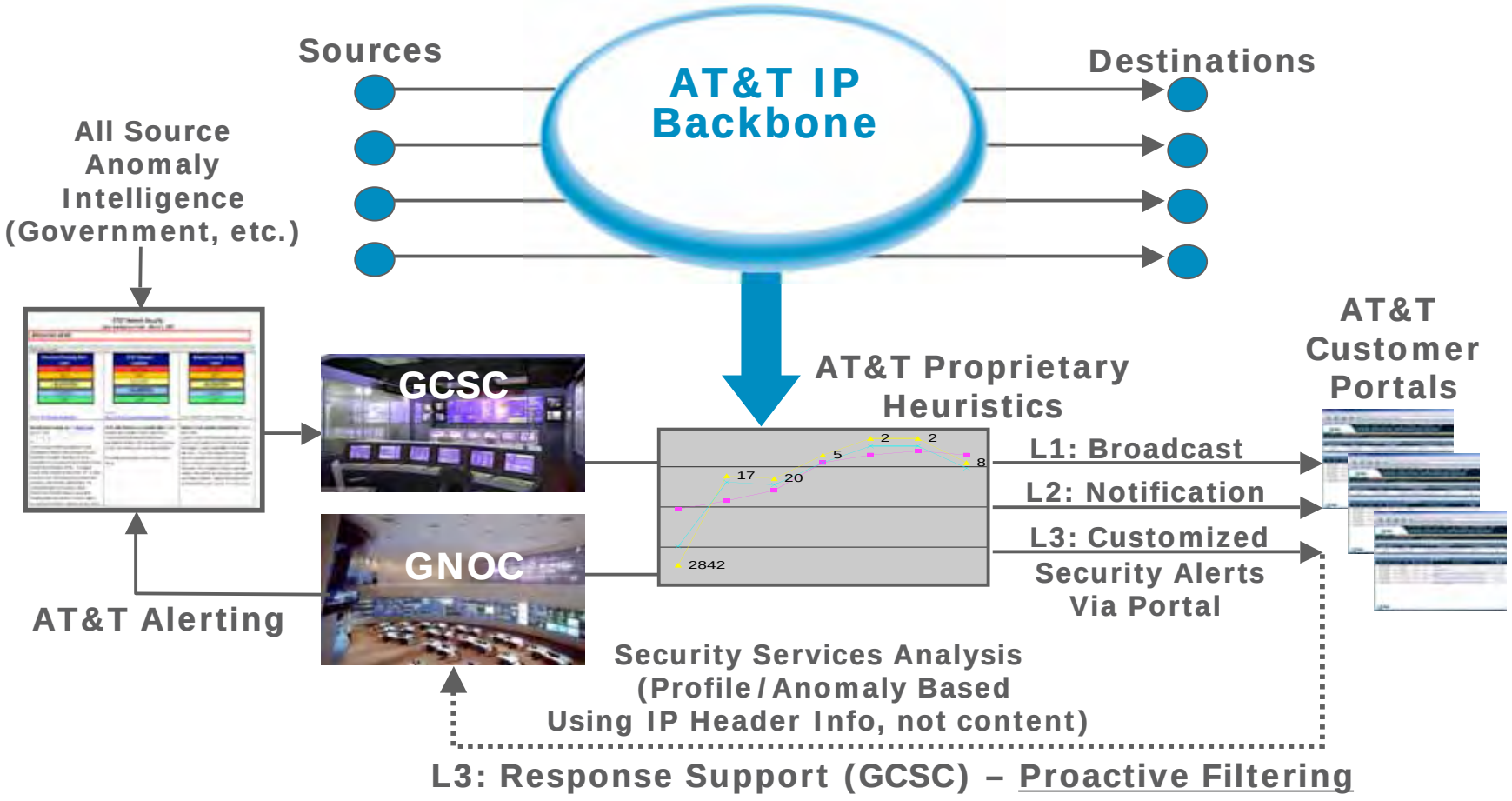
Monitoring Engine
"What you Actually See"

Correlation Engine

Normalized
Database of
Alerts

AT&T Internet Protect®

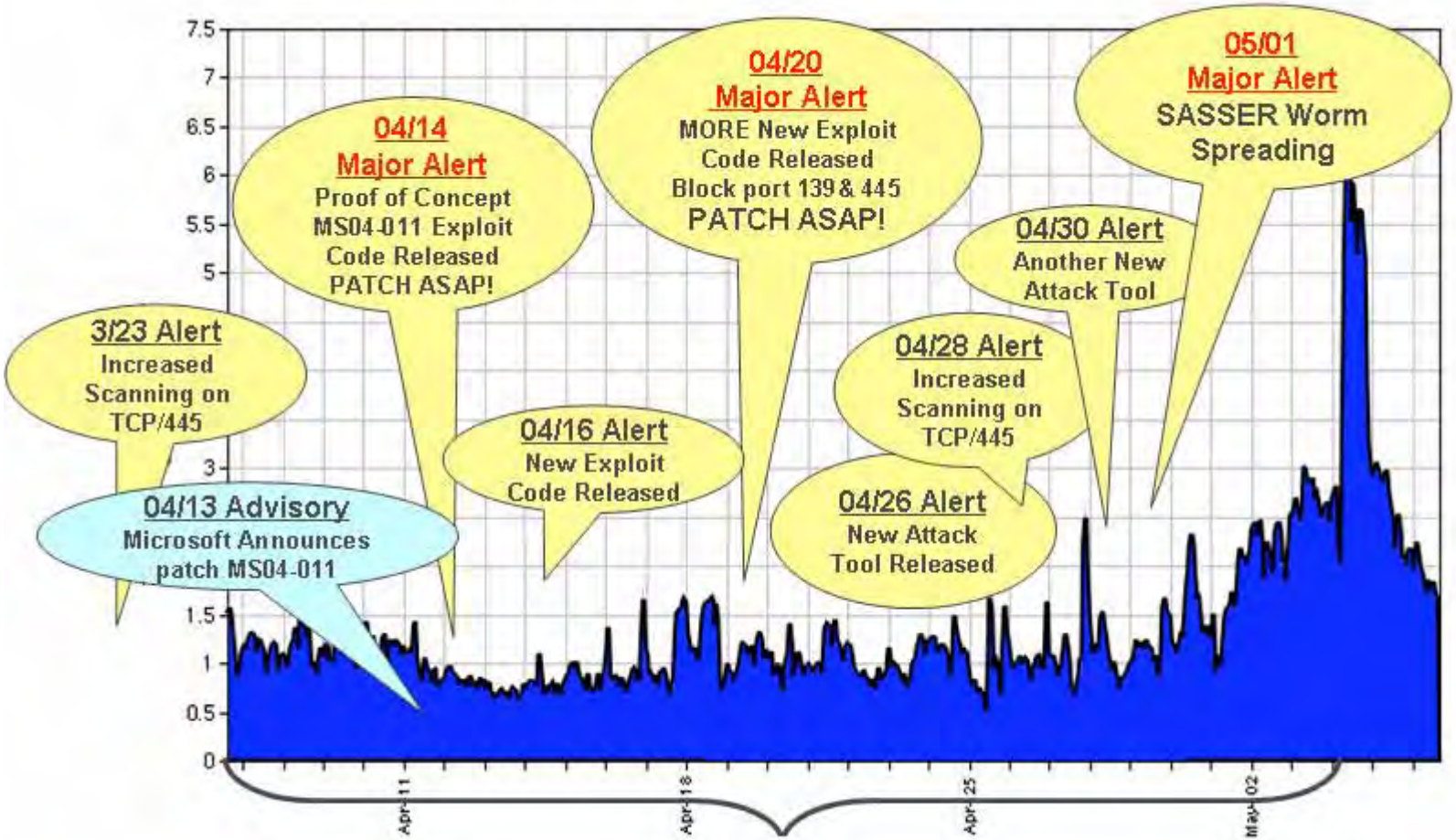
Security Alert Notification Service



GCSC – Customer Facing Team (Raleigh)
GNOC – AT&T Infrastructure Team (Bedminster)

AT&T Internet Protect®

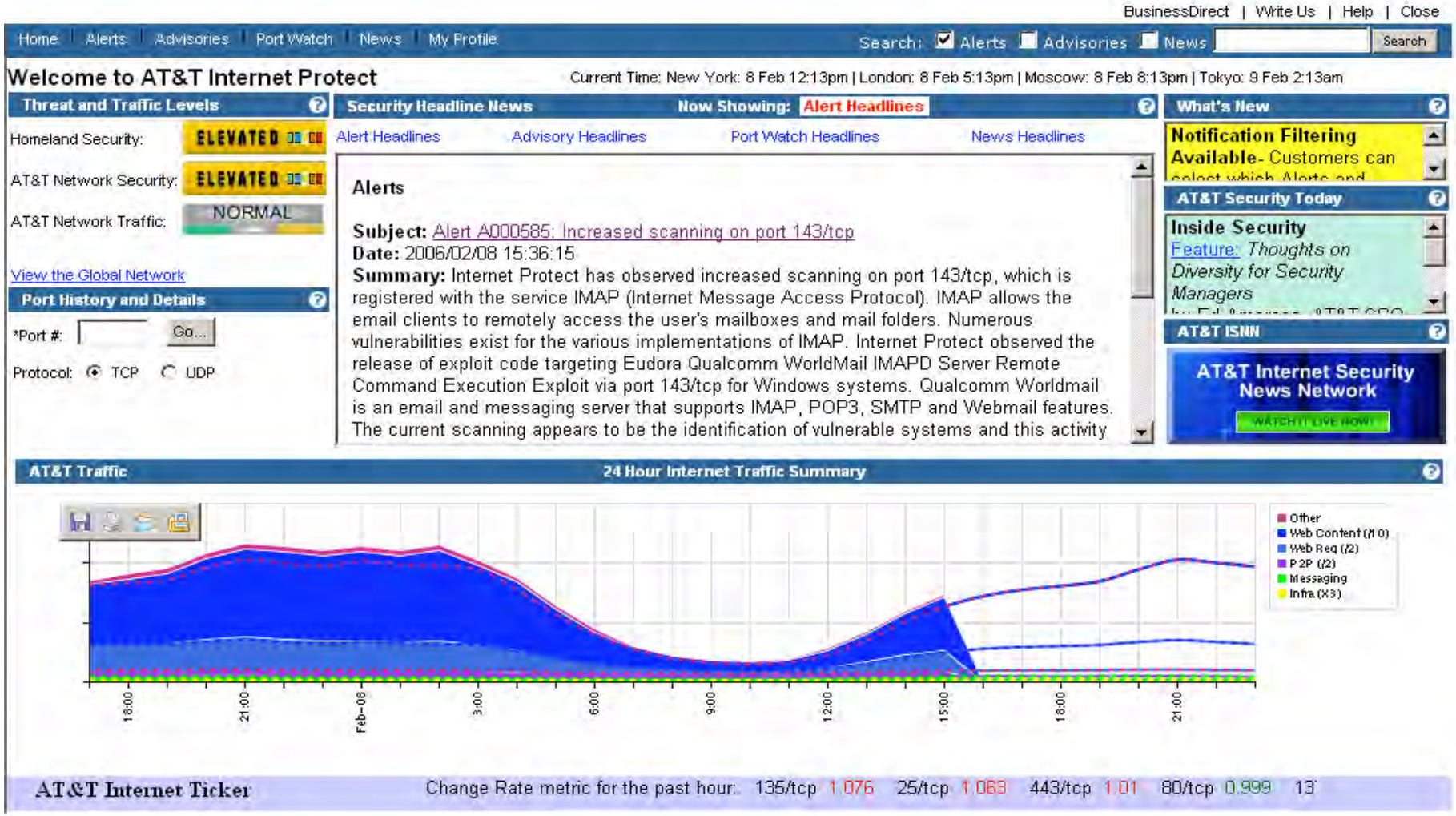
(Sasser Timeline / Alerts)



Notification of activity more than five weeks early!

AT&T Internet Protect®

Client Portal via BusinessDirect

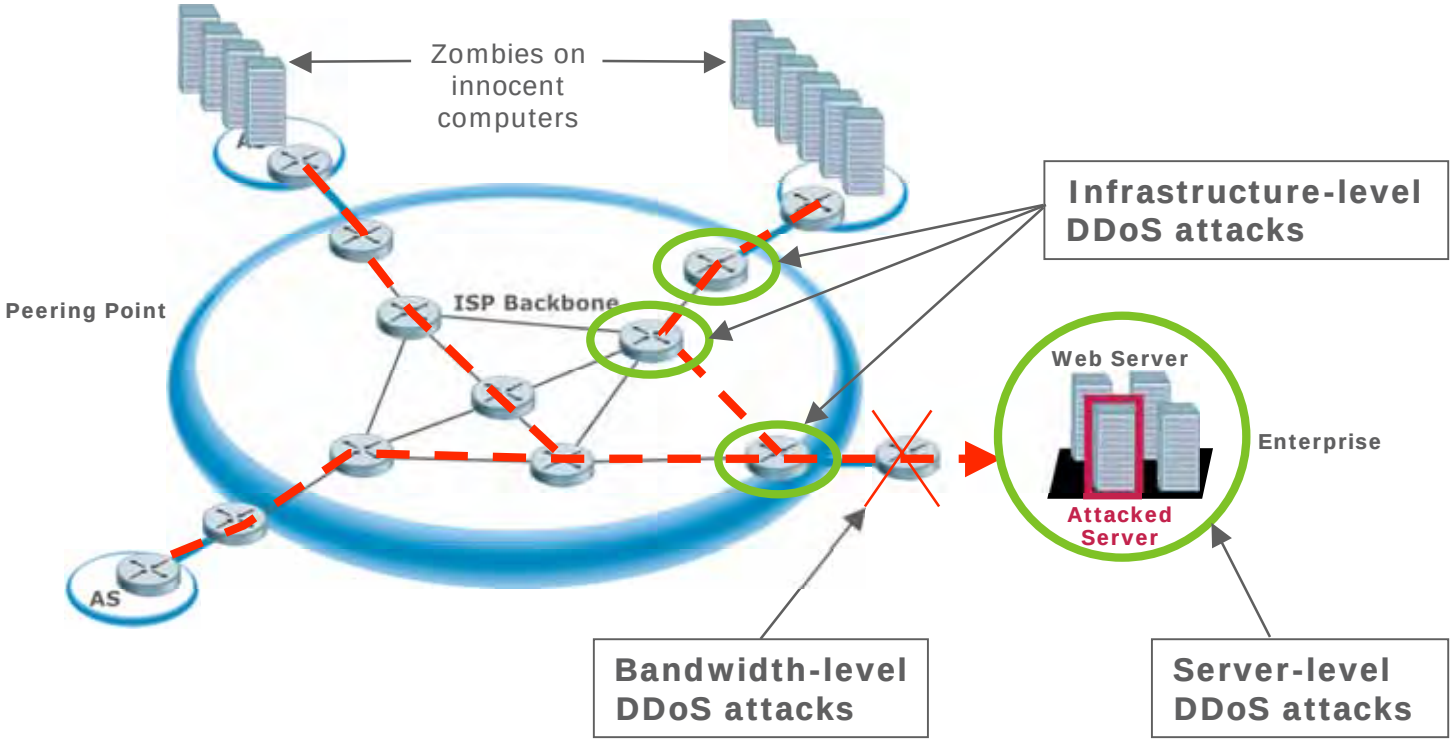


AT&T Internet Security News Network (ISNN)

- **24/7 Breaking Stories**
  Security alerts, advisories, attacks, scrolling news ticker
- **Live TV Channel**
  From AT&T to your browser or company NOC
- **Business Content**
  On-air commentary, news, specials

Distributed Denial of Service Attack

Multiple Points of Vulnerability



Features

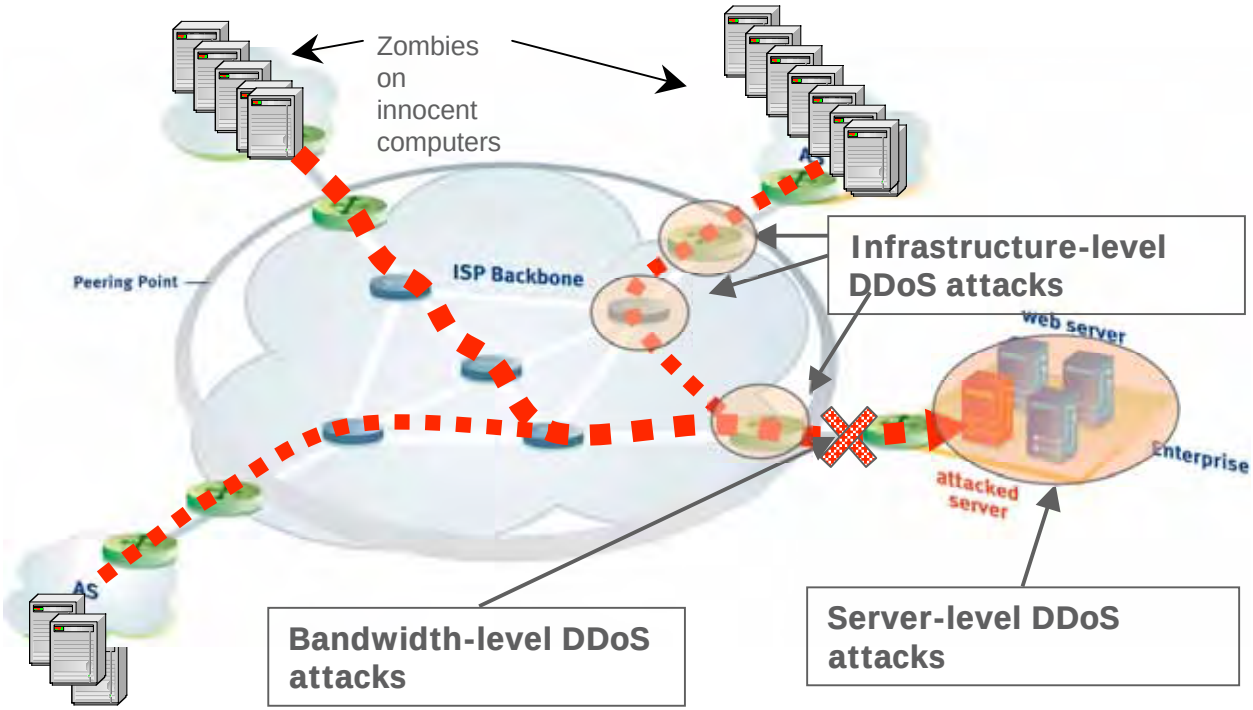
- Accurately identify attacks in seconds
- Immediately mitigate a broad range of DDoS attacks
- Dedicated or Shared

Benefits

- Defense against volumetric attacks designed specifically to disable infrastructure resources, applications and businesses
- Secures availability and ensures business continuity

Distributed Denial of Service

Multiple Points of Vulnerability



Features

- Accurately identify attacks in seconds
- Immediately mitigate a broad range of DoS and DDoS attacks
- Dedicated or Shared

Benefits

- Defense against attacks designed specifically to disable infrastructure resources, applications and businesses
- Secures availability and ensures business continuity

at&t

Your world. Delivered.

Thank You!