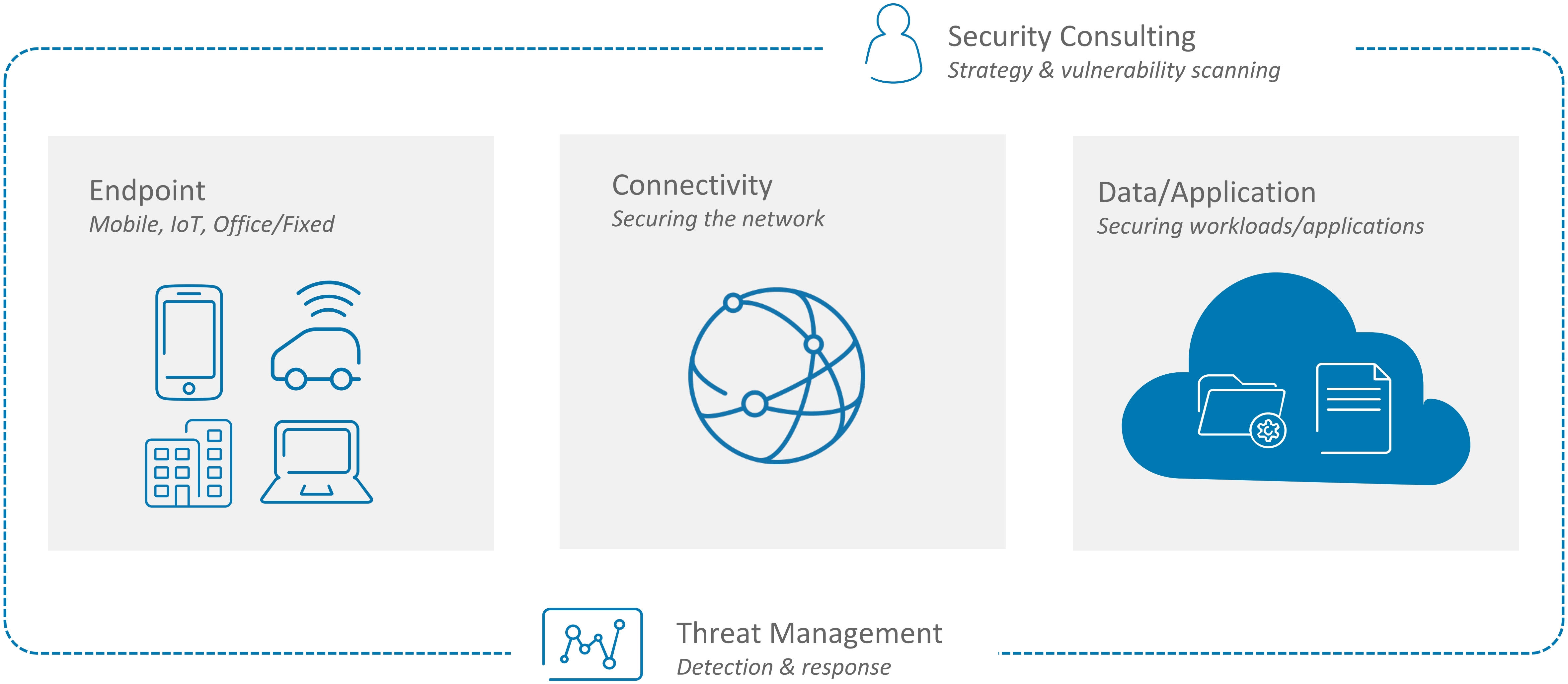
Next Gen Security from AT&T

David Sanford Security Strategist

2/2/2017

At AT&T, we manage highly secure solutions to help protect what’s important to our customers.

Today’s threat landscape requires a multi-layered approach



Security Consulting

Strategy & vulnerability scanning

Endpoint

Mobile, IoT, Office/Fixed

Connectivity

Securing the network

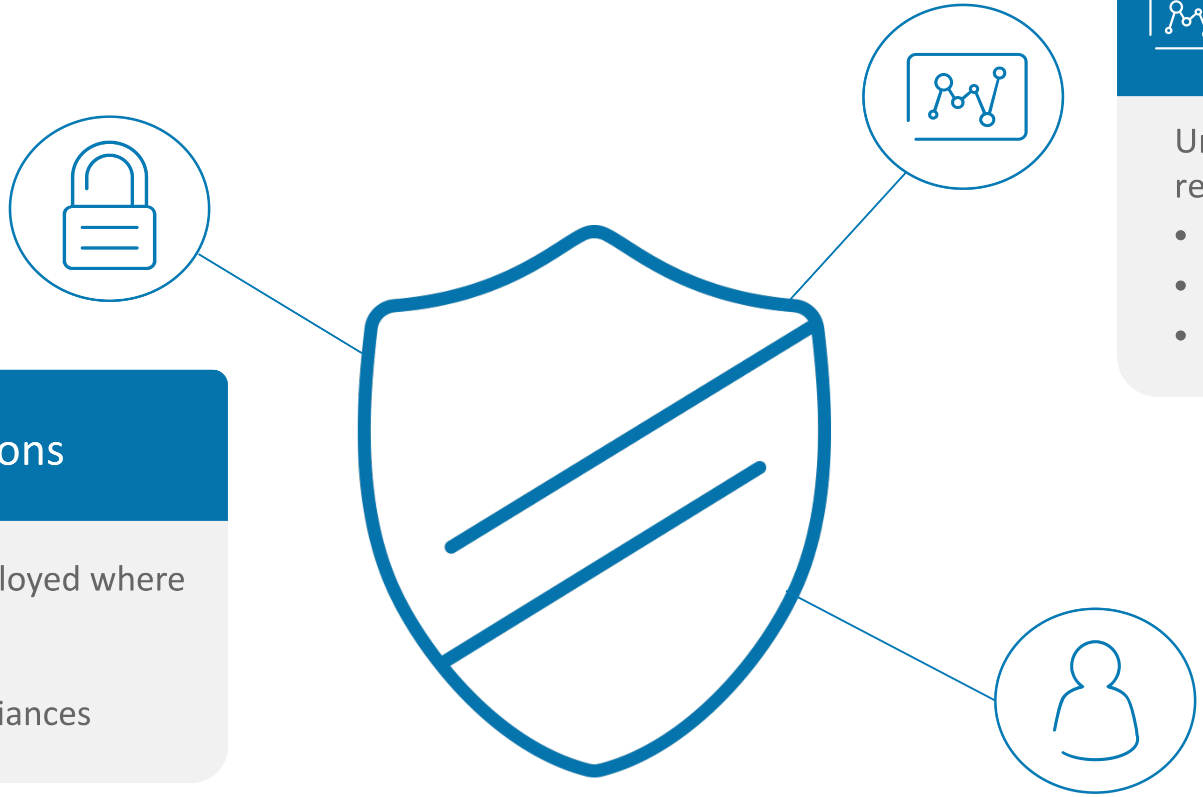
Data/Application

Securing workloads/applications

Threat Management

Detection & response

AT&T has the capabilities and expertise to help customers prevent, detect and respond to threats.



AT&T Managed Security Solutions

Security Functions

Virtual security functions deployed where needed

- Defense in-depth
- Best in-breed strategic alliances

Threat Management

Unparalleled visibility to proactively respond to threats

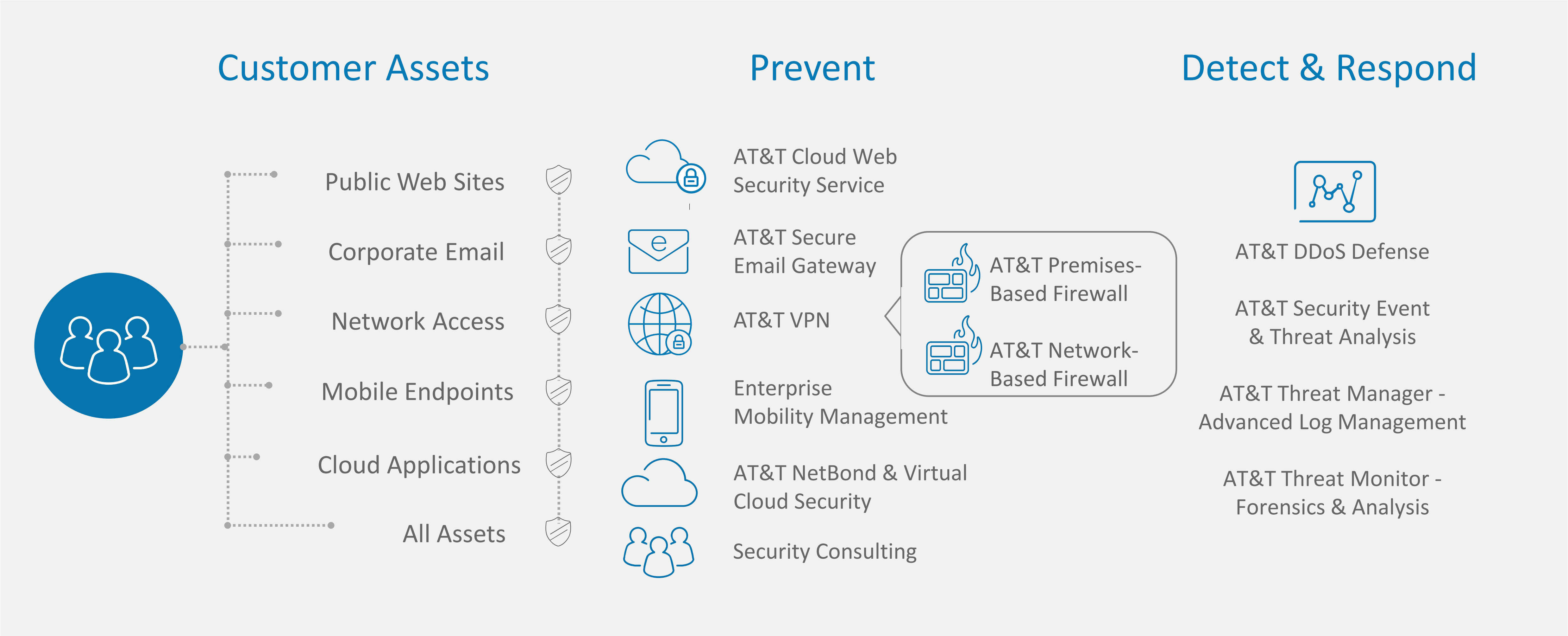
- 114+PB of traffic/day
- 3.7B records analyzed/hour
- Classified govt. data

Security Leadership & Expertise

Recognized leader by Forrester, IDC

- 8 SOCs
- People, knowledge, expertise
- Tools, processes, automation

End-to-end managed security solutions to help protect our customers' assets



Customer Assets

- Public Web Sites
- Corporate Email
- Network Access
- Mobile Endpoints
- Cloud Applications
- All Assets

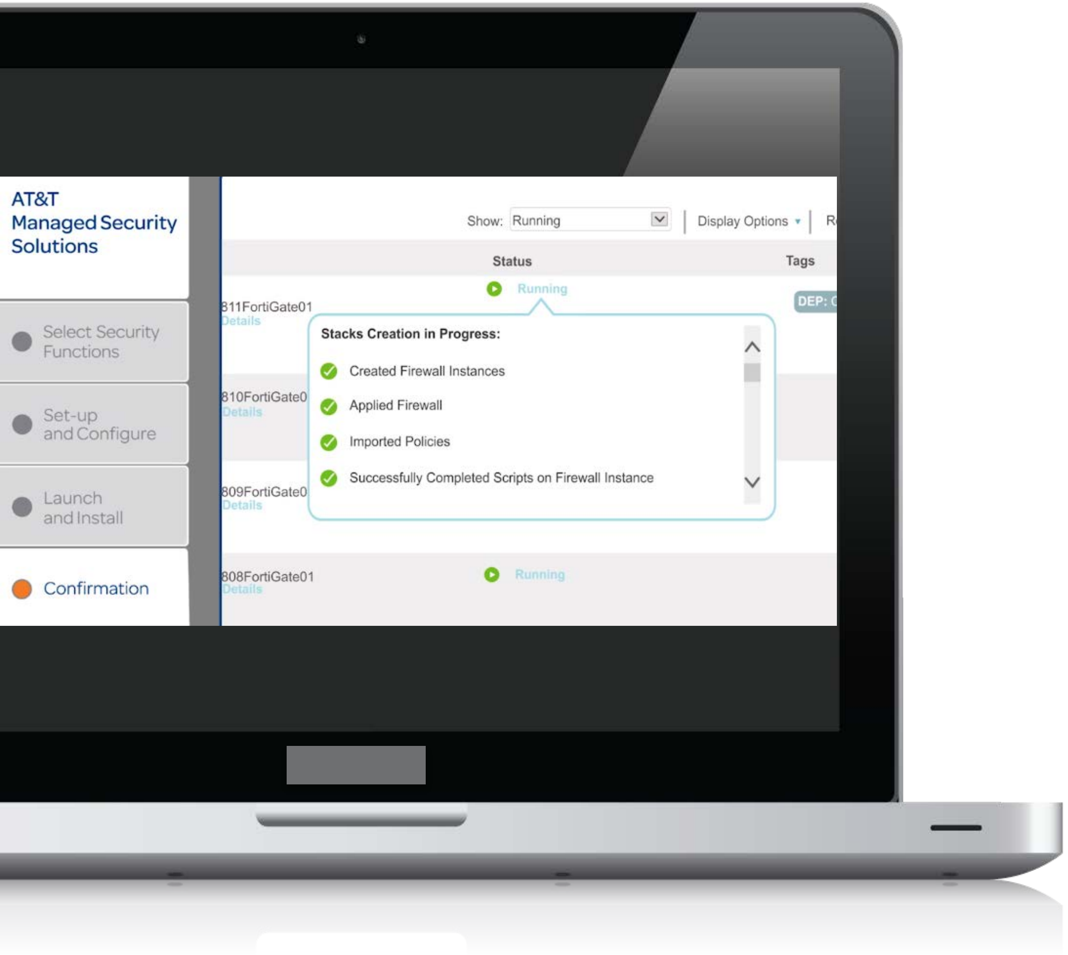
Prevent

- AT&T Cloud Web Security Service
- AT&T Secure Email Gateway
- AT&T VPN
  - AT&T Premises-Based Firewall
  - AT&T Network-Based Firewall
- Enterprise Mobility Management
- AT&T NetBond & Virtual Cloud Security
- Security Consulting

Detect & Respond

- AT&T DDoS Defense
- AT&T Security Event & Threat Analysis
- AT&T Threat Manager - Advanced Log Management
- AT&T Threat Monitor - Forensics & Analysis

Virtual security managed and deployed where needed



AT&T Managed Security Solutions

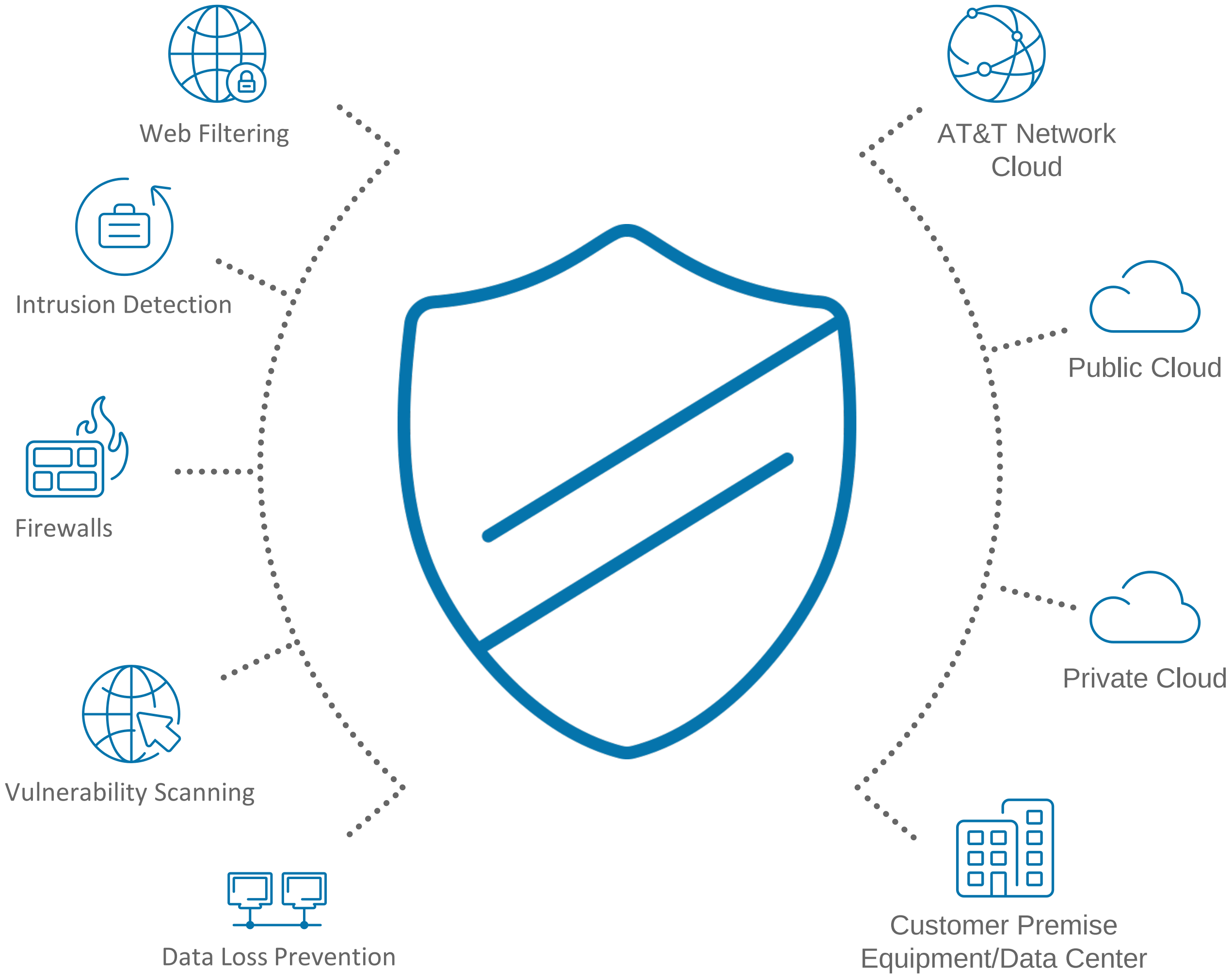
- Select Security Functions
- Set-up and Configure
- Launch and Install
- Confirmation

Show: Running | Display Options ▾ | R

	Status	Tags
811FortiGate01 Details	Running	DEP:
810FortiGate0 Details		
809FortiGate0 Details		
808FortiGate01 Details	Running	

Stacks Creation in Progress:

- ✓ Created Firewall Instances
- ✓ Applied Firewall
- ✓ Imported Policies
- ✓ Successfully Completed Scripts on Firewall Instance



Web Filtering

Intrusion Detection

Firewalls

Vulnerability Scanning

Data Loss Prevention

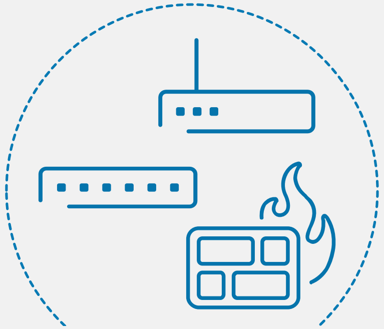
AT&T Network Cloud

Public Cloud

Private Cloud

Customer Premise Equipment/Data Center

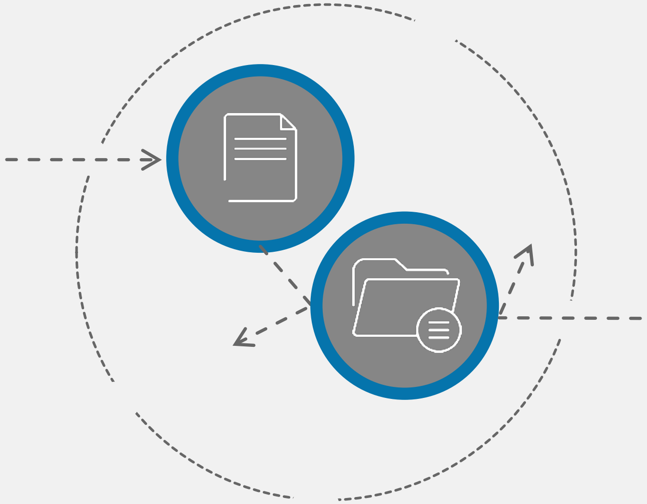
Defense in-depth



Virtualized security functions

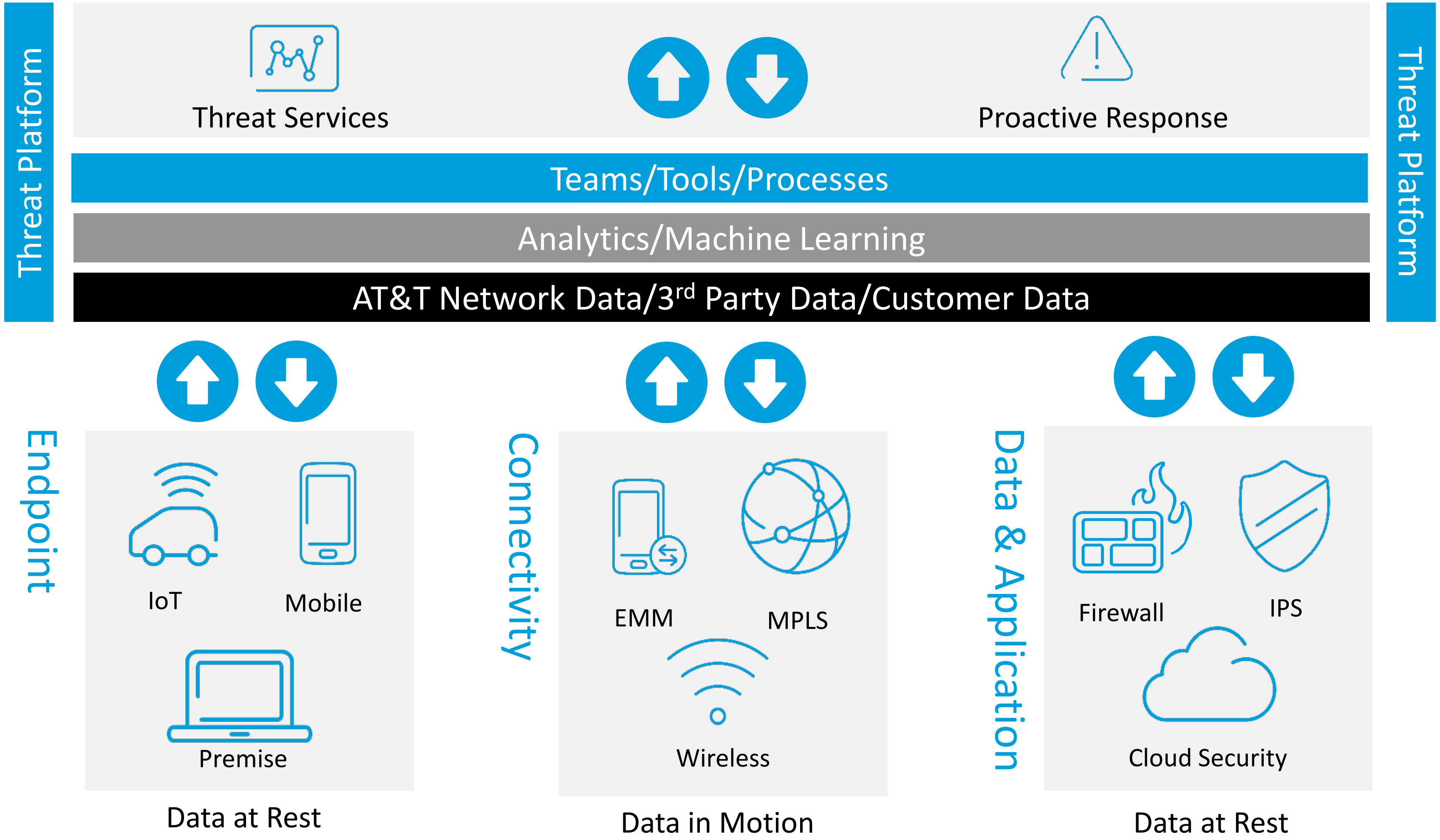
- Consistency across clouds
- Operational efficiency
- Rapid response
- Dynamic scale

Enhanced security *inside* the perimeter and *to* the application

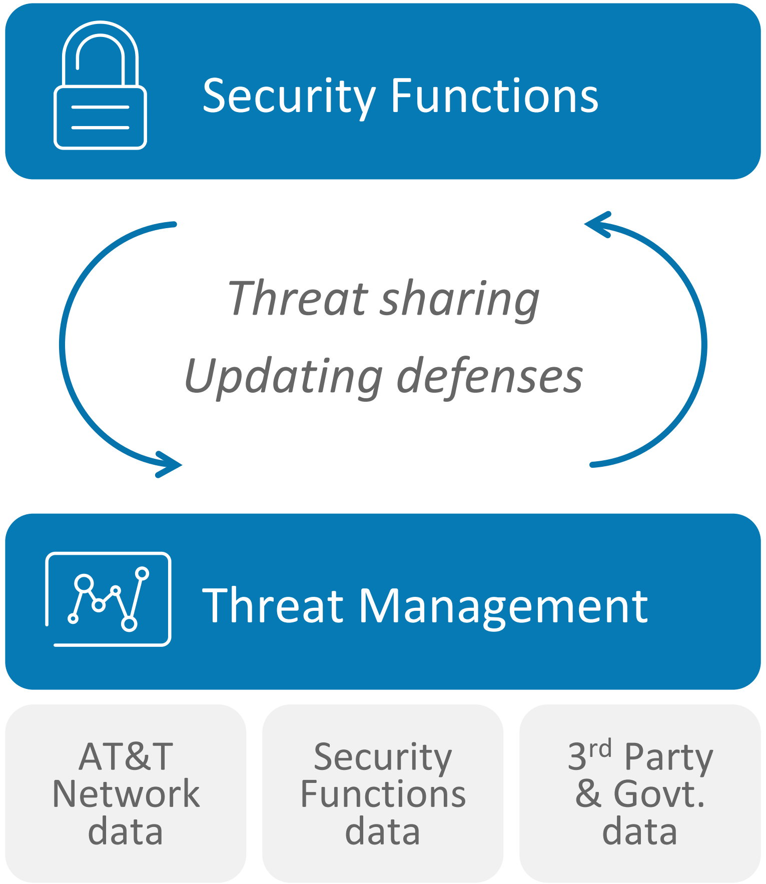


- Inside & lateral protection
- Customized perimeter per application
- On-demand policy orchestration
- Automation

AT&T next generation threat platform



Scale, reliability and enhanced visibility from AT&T Managed Security



3.7B

Records pass through our Analysis Engines every hour

Over 114

Petabytes of traffic across the network per day[1]

3800+

MPLS nodes in one of the largest IP networks in the world

8

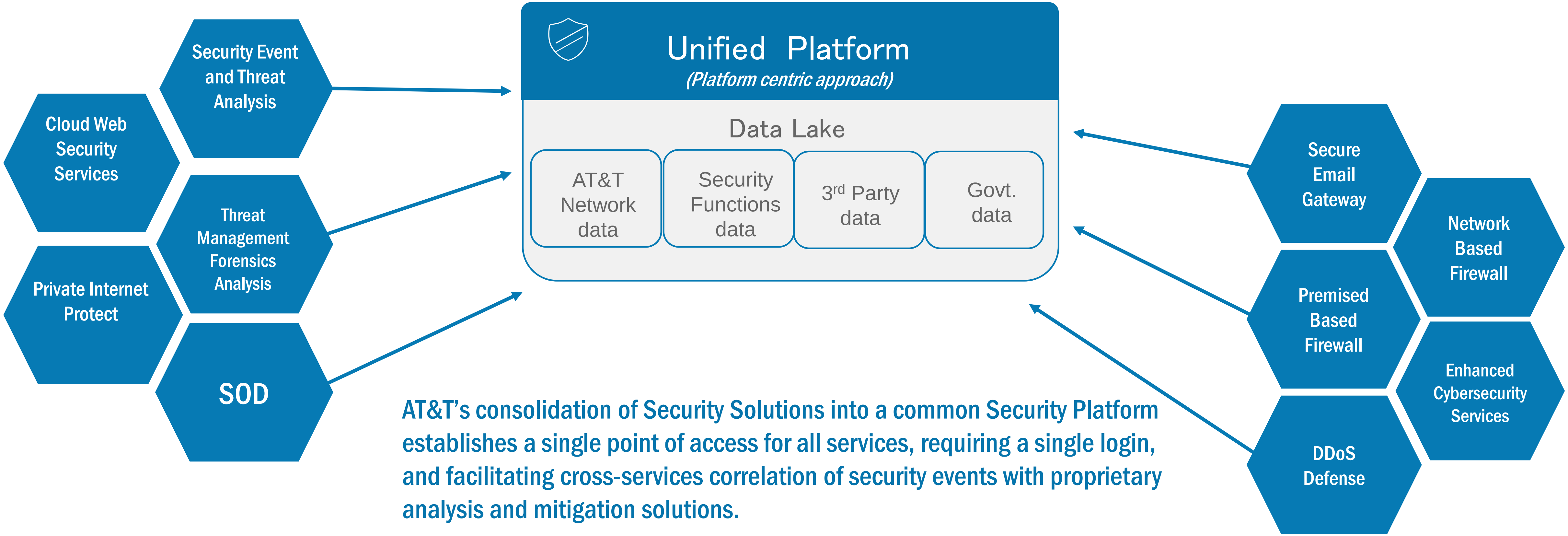
Global Security Operations Centers

24/7/365

Operations support

[1] As of December 2015

AT&T simplifies access to their comprehensive portfolio of Security Solutions, making it easier for users to prevent, detect, and respond to the ever-changing IT security landscape.



AT&T's consolidation of Security Solutions into a common Security Platform establishes a single point of access for all services, requiring a single login, and facilitating cross-services correlation of security events with proprietary analysis and mitigation solutions.

Security Innovation with the AT&T Foundry®

Software Defined Perimeter

Exfiltration Prevention

Identity & Access Management / Biometrics

Deep Learning

Security Innovation

Mission: connect with cutting-edge startups, academics and inventors to deliver valuable security services that enhance or refine platforms and customer experience

Enterprise Endpoint Security

Secures, controls, and manages traditional (PCs, laptops, servers) and IoT endpoints and

Proactively blocks completely new and unknown threats across all of your endpoints.

Across both physical and virtual environments

File-based Cloud Encryption Gateway

Gateway encrypts files as they travel from enterprise to cloud, leaving the files protected even when at rest.

The solution’s 1 key per file approach reduces the “blast radius” of a breach

True end-to-end protection of an enterprise’s cloud-stored data, never leaving AT&T’s private cloud even when in transit

Mobile and Application Security and Remediation

Proactive defense against known and unknown threats for mobile devices and applications

Combination of defenses at the mobile OS and networks

Real-time user behavior analysis and predictive analytics.

IIoT Security Gateway

Cyber-aware gateway/ firewall blocks machine-specific malicious attacks to IoT endpoints

Provides automatic defense for networked industrial equipment.

Differentiates between valid and potentially rogue commands

AT&T

Customer – Large State Judiciary System

Issue – Suspicious outbound FTP connection allowed through the firewall to a “not normal” destination.

How We Detected – ThreatWatch 2.0® Network behavioral analytics platform detected anomaly

How We Notified – A notification was sent describing potential malicious activity (possible data exfiltration) using our proprietary “SORAD™” alert notification

Customer Response – Customer conducted investigation that determined the FTP connection was malicious, which resulted in a change to the firewall rules blocking the traffic

Follow up – We added attacker’s profile to our consolidated threat reputation monitoring to improve future alert confidence and be on the lookout for similar threats

Customer – Transportation

Security Event – Customer requests for forensic and other traffic pattern matching data to confirm patient zero of a malware attack.

What we did– During the incident handling process driven by the customer, we determined that the access resulted from an infected device. and then analyze that device's network behavior historically to build a network fingerprint based on the frequency, protocols and destination of attempted network connections by the malware.

Customer Response– Used fingerprint to determine extent of infection, including patient zero and initial source of infection which was malware in an email.

Follow up – Malware was submitted to anti-malware vendors. We distributed the fingerprint across our systems including known C&C systems to the consolidated threat database to detect future similar attacks. .

MOBILIZING
YOUR
WORLD^{SM}