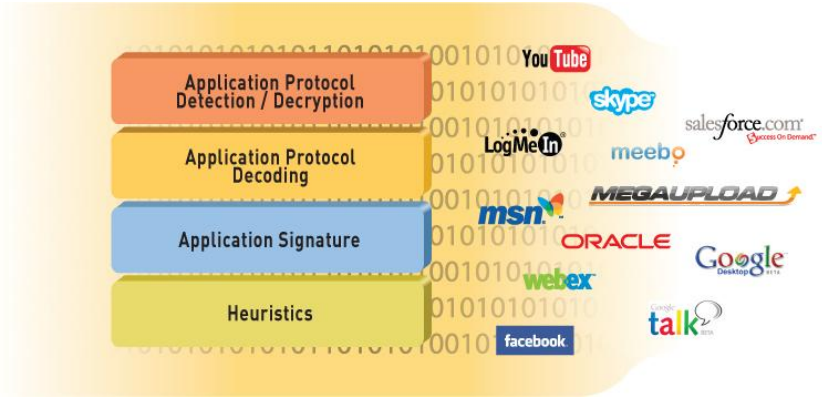
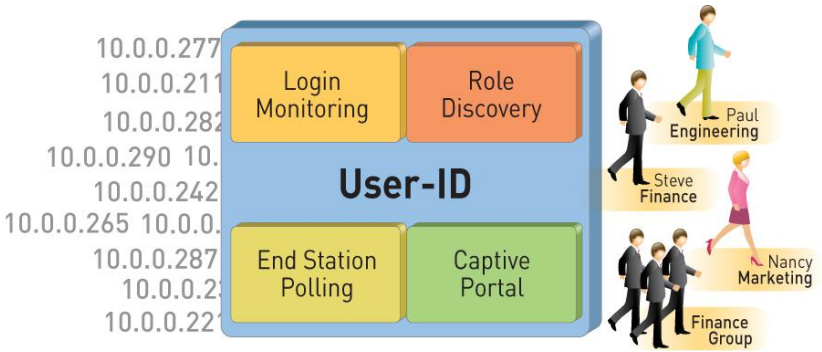
(*) Bookings run rate is defined as 4 (four) times the bookings amount of the most recently finished fiscal quarter. Bookings are defined as non-cancellable orders received during the fiscal period. Palo Alto Networks' fiscal year runs from August 1st until July 31st.

Unique Technologies Transform the Firewall

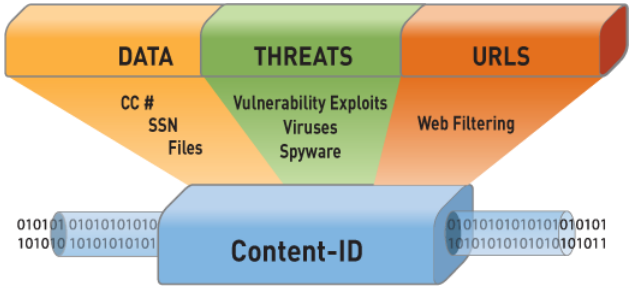
- App-ID
- *Identify the application*



- User-ID
- *Identify the user*



- Content-ID
- *Scan the content*

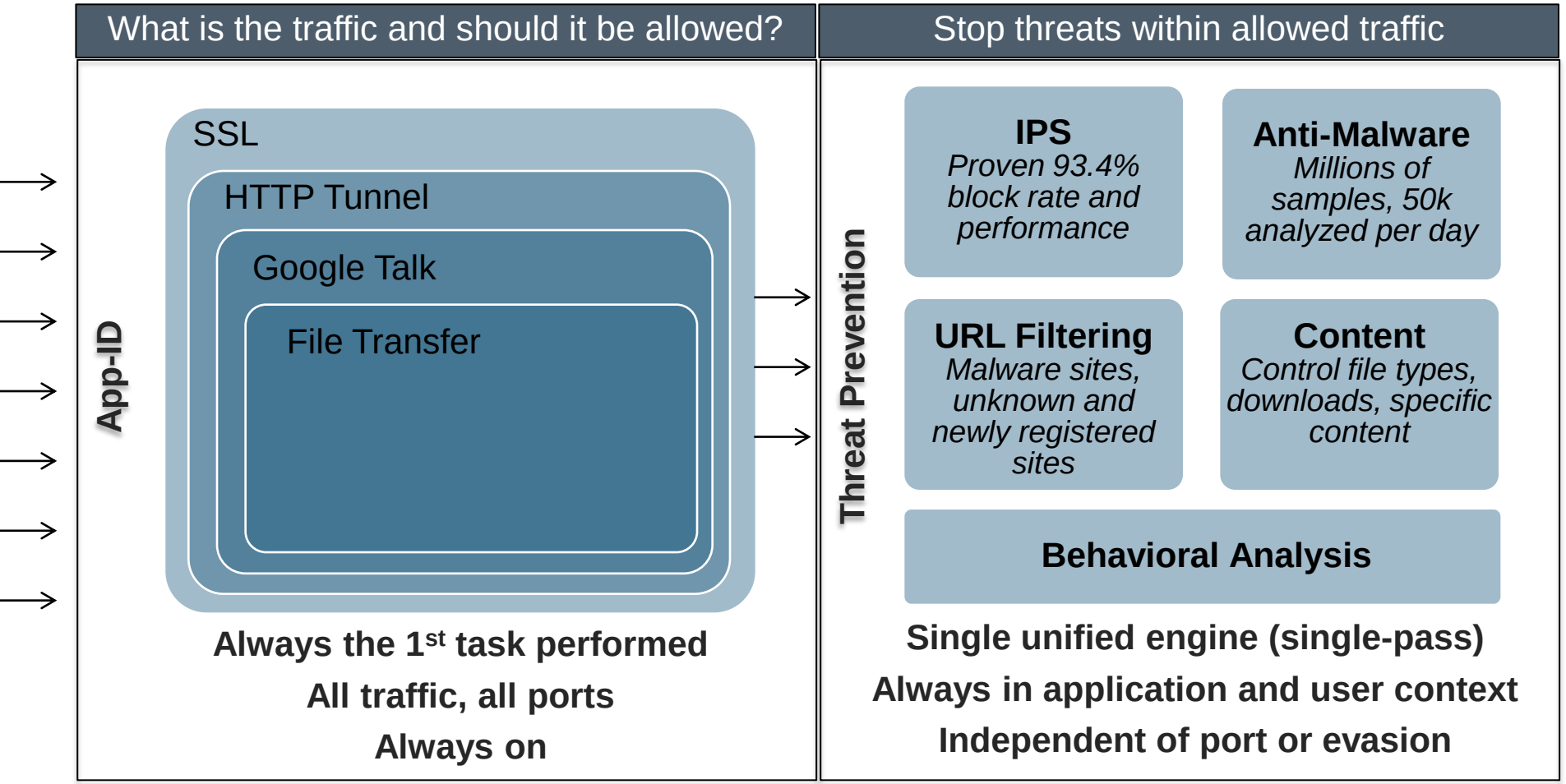


paloalto NETWORKS

The NGFW and Integrated Threat Prevention

Visibility and Control

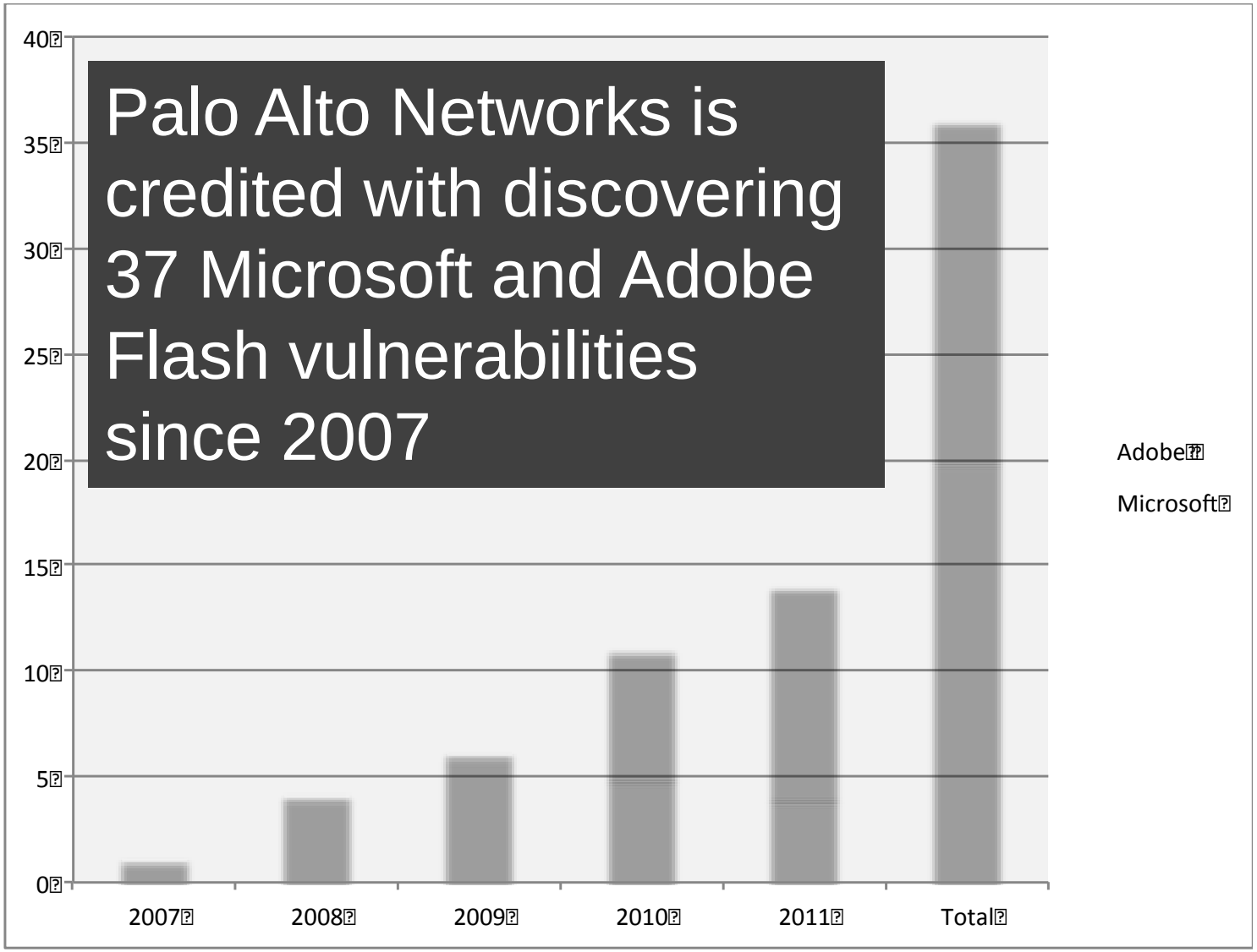
Integrated Threat Prevention



Visibility into Unknown Traffic

- **NGFW classifies all known traffic**
  - Custom App-IDs for internal or custom developed applications
- **Any remaining "unknown" traffic can be tracked and investigated**
  - Used in the field to find botnets and unknown threats
- **Behavioral Botnet Report**
  - Automatically correlates end-user behavior to find clients that are likely infected by a bot
  - Unknown TCP and UDP, Dynamic DNS, Repeated file downloads/attempts, Contact with recently registered domains, etc

Track Record of Independent Research



Visibility into Unknown Malware

- WildFire identifies unknown malware by direct observation in a cloud-based, virtual sandbox
  - Detects more than 70 malicious behaviors
  - Capture and enforcement performed locally by firewall
  - Sandbox analysis performed in the cloud removes need for new hardware and provides single point of malware visibility
- Automatically generates signatures for identified malware
  - Infecting files and command-and-control
  - Distributes signatures to all firewalls via regular threat updates
- Provides forensics and insight into malware behavior
  - Actions on the target machine
  - Applications, users and URLs involved with the malware

paloalto NETWORKS

Summary

- Palo Alto Networks coordinates multiple types of threat prevention to detect and prevent all types of risks
  - Lifecycle: From reducing exposure to blocking threats
  - Known and Unknown Threats
  - Context: Tie users, URLs and applications to any event