

# Reclaiming the Perimeter: Deploying Network Admission and Endpoint Control to Secure the Mobile Enterprise



---

Arvin Babu, Perfigo

Gregory Toto, Big Fix

Hemendra Godbole, Extreme Networks

David Piscitello, Core Competence, Moderator



# What is Endpoint Control?

---

- Endpoint control assumes that
  - User may access the company network from non-work systems
  - IT may not be able to install resident admission control software (Temporary agents may be used instead)
- Early goals: Leave no trace of user activity on endpoint following logoff
  - No cached credentials
  - No leaks of network topology information
  - No record of (internal) hyperlinks visited
  - No temporary, spooled, and cached data files
  - No local copies of company-sensitive information



# Recent EPC Objectives

---

- Use identity, endpoint “state”, and location information in authorization decisions
- Protect the organization from compromise via (uncontrolled) endpoint devices by
  - Restricting access when endpoint does not warrant full trust
  - Redirecting user to a remediation site (quarantine)
- Restrict endpoint from running certain applications
  - E.g., prohibit use of FTP from non-work systems
- Block application commands based on user, endpoint state and location
  - E.g., prohibit FTP PUT from non-work systems



# Warmup Questions

---

- Is end-user security checking enough to secure against internal attacks?
- Does endpoint security only encompass user and host-machine authentication and host integrity checks?
- Why does EPC provide scanning, blocking, quarantining, and remediation in a single solution? Do I need them all, always?
- Does every company really need a network admission and endpoint control solution?



## Details!

---

- What is the notion of policy and attributes in network admission control?
- Is network admission policy for the same user vary based on location?
- Where should policies be enforced: at the endpoint or on the network? Why?



## Role of Switches in EPC

---

- If EPC is not sufficient, what role can network (edge and core) switches play?
- How does the switching infrastructure augment endpoint security solutions for blocking rapidly propagating threats (new virus/worm storms),?



# Remediation & Mitigation

---

Today, mitigation is a manual process..

- Assuming most security policies consist of monitoring, detection/analysis and policy enforcement/mitigation tasks, what are/should vendors do to collapse all of these into near-real time levels?
- How can enterprises streamline the process when users attempt to reconnect to the network (following remediation)?



# Regulatory Matters

---

- What is the role of network admission control in satisfying regulatory compliance?



## EPC Futures...

---

- What are/should vendors doing to help with security management beyond endpoint security control/management?
- How can we integrate endpoint security solutions and network access with systems management infrastructures?