

Enterprise Network Access Controls

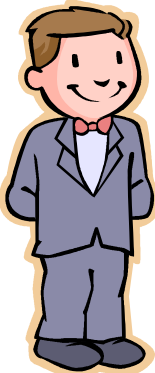
Andrew Davis

Elemental Security, Inc.

INTEROP[®]
MAKES YOU
SMART

What to Control

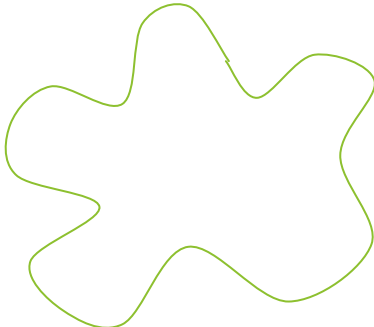
User



Application

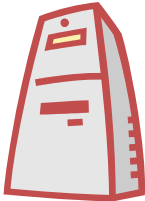


Client
Compliance



Path

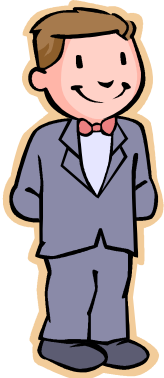
Time



Server
Compliance

Example

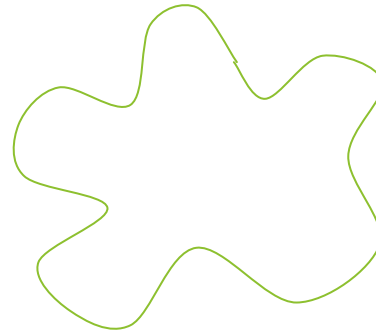
Peter



Firefox
Browser

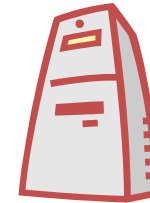


Vulnerabilities
Password
Attached Devices



Not Wireless
From Finance

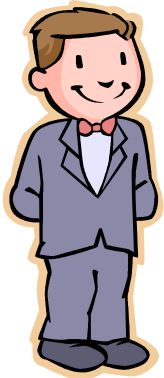
Business
Hours



Vulnerabilities
Running Processes

Scaled to the Enterprise

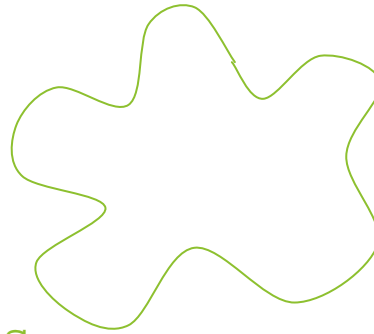
1000 Users



10 Apps
2 versions
2 platforms

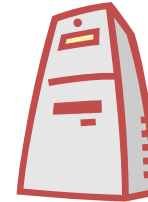


10 Vulnerabilities



Wireless?
Internal?
Encrypted?

2 Shifts



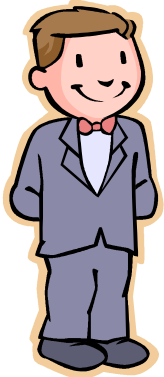
2 Vulnerabilities
10 servers

Per 1000 users:

$1000 \times 10 \times 2 \times 2 \times 10 \times 8 \times 2 \times 10 \times 2 = 128M!$

Daily Enterprise Dynamism

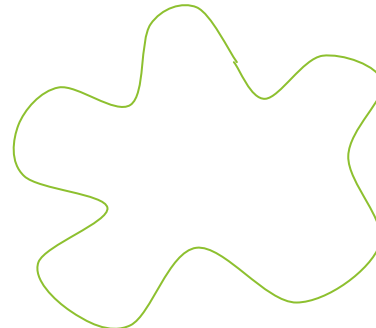
1 Login



10 Applications

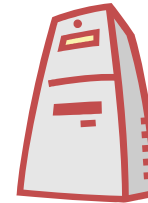
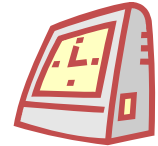


50 Vulnerabilities



1 DHCP/week

2 Shifts



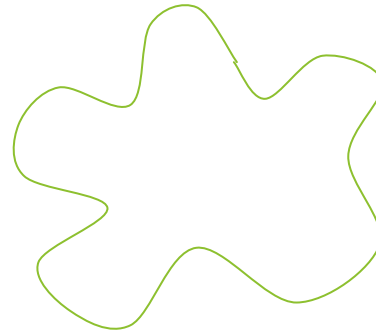
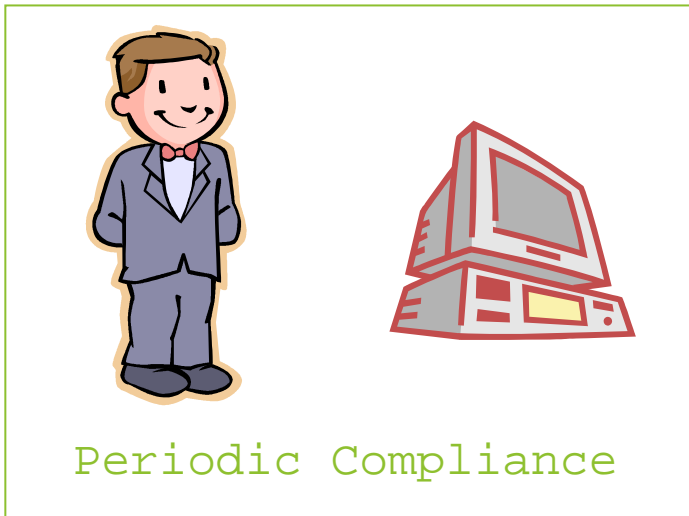
10 Vulnerabilities

ACL Changes per 1000 hosts:

$$1000 \times (1 + 10 + 50 + 2) + 200 + 10 \times 10 = 63K$$

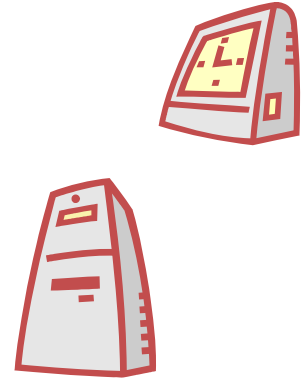
Partitioning?

1000 Hosts



Wireless?
Encrypted?

Always Available



10 servers,
Periodic Compliance

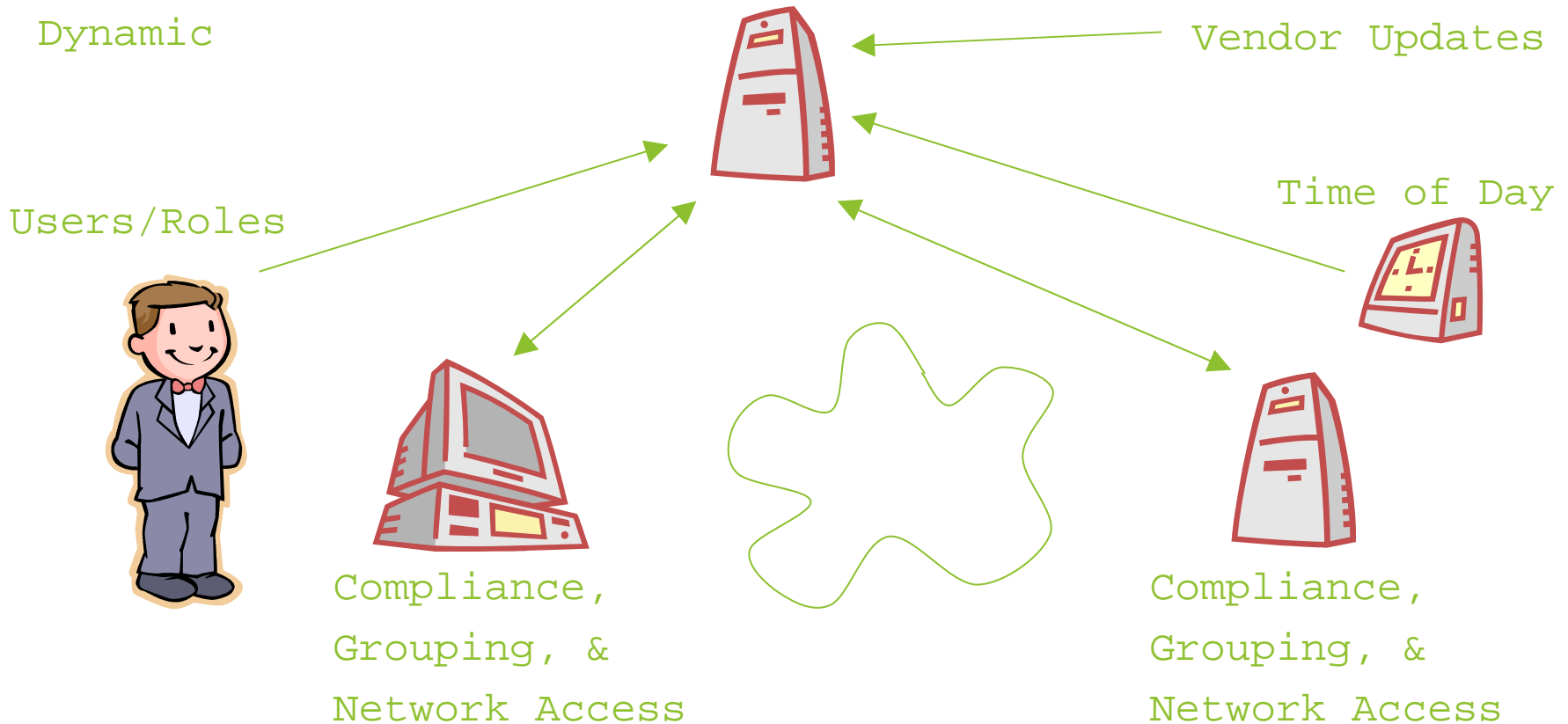
$1000 \times 8 \times 10 = 80k!$

Dynamism and granularity lost.

Extremely hard to manage these abstractions.

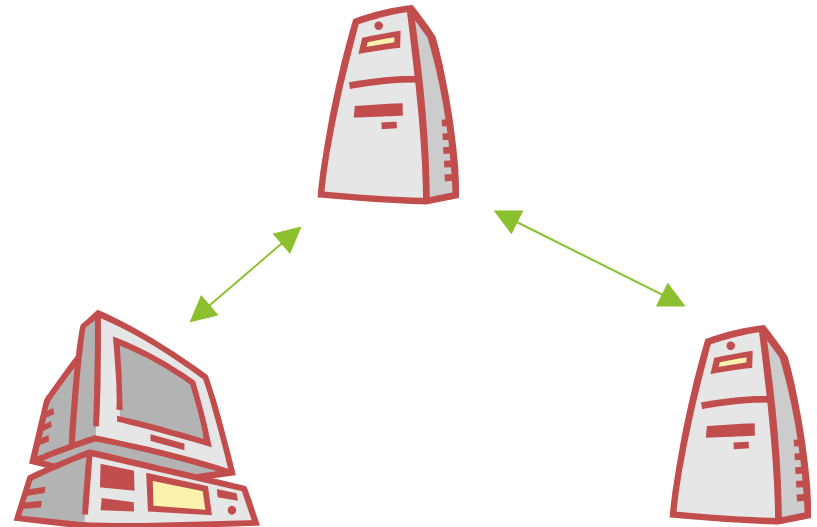
Better Management

Holistic
Comprehensive
Dynamic



Managed Host

- Visibility into Changes
 - Software Configuration
 - Hardware Configuration
 - User or Host Role
 - Network
- Scale of Change
 - Millions of sample points
 - 1 million changes a day
- Responsiveness to Change
 - Host is the only viable option



Questions?