

WINDOWS SECURITY BASICS FOR THE SYSTEM ADMIN

It's not always easy, but it is always
important

FROM THE INSIDE



- ▶ Desktops? Sure ... why not?
- ▶ Laptops? Might be more work than it's worth.
- ▶ You can do more with Admins than you think!

TO ADMIN, OR NOT ADMIN?

- ▶ Not just for Desktop Wallpaper anymore (if it ever was)!
- ▶ Lots and lots and lots of policies.
- ▶ Things of which to be aware.
- ▶ Example

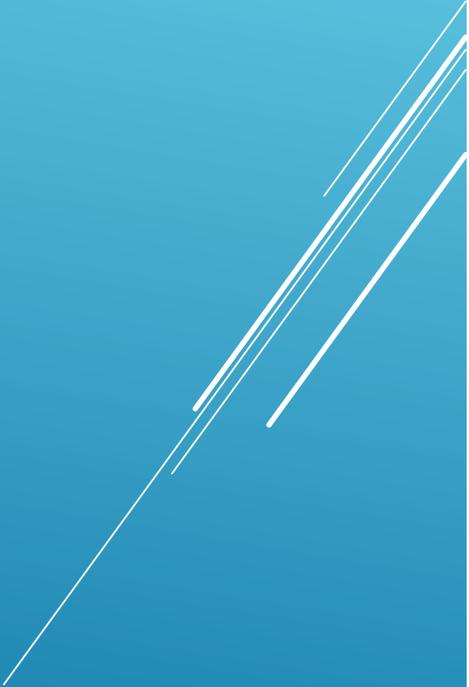
GROUP POLICY (OU POLICY?)

- ▶ Windows Firewall
- ▶ IPSEC Rules
- ▶ (Outside) Symantec Endpoint Protection
- ▶ Differences?

FIREWALLS (YES! PLURAL!)

- ▶ Requires TPM to be enabled
- ▶ Does not automatically cache recovery token

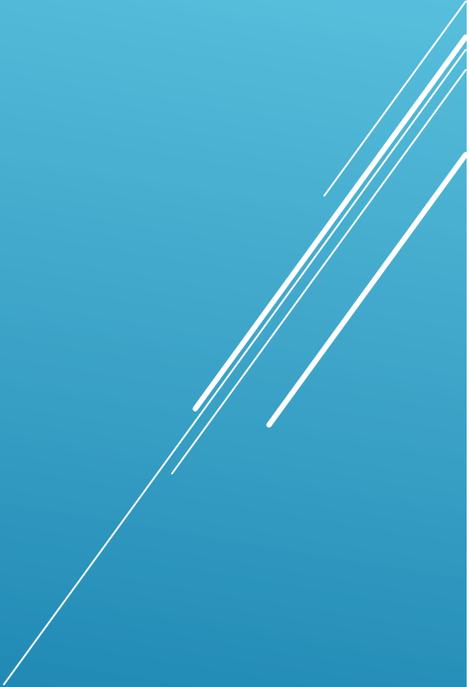
BITLOCKER – EASIER THAN YOU
THINK



- ▶ Certificates
- ▶ Login requirements

OTHER QUESTIONS

ON THE OUTSIDE LOOKING IN

The slide features a blue gradient background. On the right side, there are several white, parallel diagonal lines of varying lengths and positions, creating a sense of movement or a stylized graphic element.

- ▶ Symantec Endpoint Protection

ANTI-VIRUS / ANTI-MALWARE

- ▶ Splunk
- ▶ Windows logs are noisy!
- ▶ Windows logs are ugly!
- ▶ Working on it ...
- ▶ Example

MONITORING

- ▶ Hardware & software
- ▶ System Center Configuration Manager
- ▶ IBM Endpoint Manager
- ▶ *NO* excuse to not be using one of these tools

INVENTORY (EXCEL IS NOT
ENOUGH)

- ▶ security@duke.edu
- ▶ Security Liaisons
- ▶ Duke ITSO Web Site

QUESTIONS? (AKA “WHAT’D I
MISS?”)