

**NORMAN®**

# Norman Enterprise Security NESEC

# Agenda

What is NESEC

Product overview

Pricing

Campaigns

Migration

Collaterals

# Norman Enterprise Security

# What is NESEC?

An agile solution suite that reduces complexity for both security and IT operations teams, optimizes TCO, improves visibility and delivers control back to IT.

# What is NESEC?

- Security solution aimed at «high-end» SMB (50+) and Enterprise
- Modules:
  - Norman Application Control
  - Norman Device Control
  - Norman Patch and Remediation
  - Norman Content Wizard
- Single management console
- Single endpoint agent

# What does this mean for the customer?

- **Reduces complexity and TCO** via an agile, single console, single agent, single server architecture that can manage thousands of endpoints regardless of their location.
- **Delivers best-of-breed, modularly licensed, product capabilities** that meet growing IT requirements.
- **Unifies IT operational and security workflows** to enable greater control, visibility, and more effective policy management while still allowing for customized, role-based user interfaces to be assigned.

## What does this mean for the customer? (cont'd)

- **Simplifies management** of systems, agents and policies in real time - from a single console.
- **Optimizes resources** by extending policy or remediation efforts to a single endpoint or group.
- **Centralizes reporting and logging** to increase accuracy, reduce the compliance burden, and enhance visibility.

# What does it look like?

**Norman Enterprise Security - Home - Windows Internet Explorer**  
http://nrvm-server/default.aspx

**NORMAN ENTERPRISE SECURITY**  
Home Discover Review Manage Reports Tools Help Administrator | Log Out

Refresh dashboard widgets to see the latest results. Refresh all Print.. Configure dashboard settings...

### System Alerts (3)

#### Server Information

Company : Norman AS  
Serial number : 02422247-7D113710

License replication : 100%  
System replication : 100%  
Patch / Content replication : 100%  
Package replication : 0 remaining  
Auto-download new critical packages : [Off](#)

Product Licenses:

Product Module	In Use	Pending	Available
AntiVirus	1	0	9
App Control	0	0	10
Dvc Control	0	0	10
Patch	1	0	9

#### Latest News

- [Microsoft Security Bulletin MS12-064 - Critical](#)  
10/9/2012 2:00 AM ->>>  
from [Latest News](#)
- [Microsoft Security Bulletin MS12-065 - Important](#)  
10/9/2012 2:00 AM ->>>  
from [Latest News](#)
- [Microsoft Security Bulletin MS12-070 - Important](#)  
10/9/2012 2:00 AM ->>>  
from [Latest News](#)

#### Agent Module Installation Status

Endpoints: 1

Module	Installed	Pending	Not Installed
Patch	1	0	0
Dvc Control	0	0	1
App Control	0	0	1
AntiVirus	1	0	0

#### Un-remediated Critical Vulnerabilities

Critical vulnerabilities: 83  
Endpoints: 1

Time Period	Vulnerabilities
<30 days	3
30 - 120 days	12
>120 days	68

#### Device Control Denied Actions

No data available

Latest refresh includes data logged from 10/2/2012 to 10/9/2012 (Agent Local)

Refresh rate:

#### Top 10 Infected Endpoints

No results found

#### Application Library File Assessment

No results found

**NORMAN** Server Name: NRVM-SERVER  
Date & Time 10/10/2012 3:05:05 PM

**NORMAN**



# Norman Patch and Remediation

# Why Patch and Remediation?

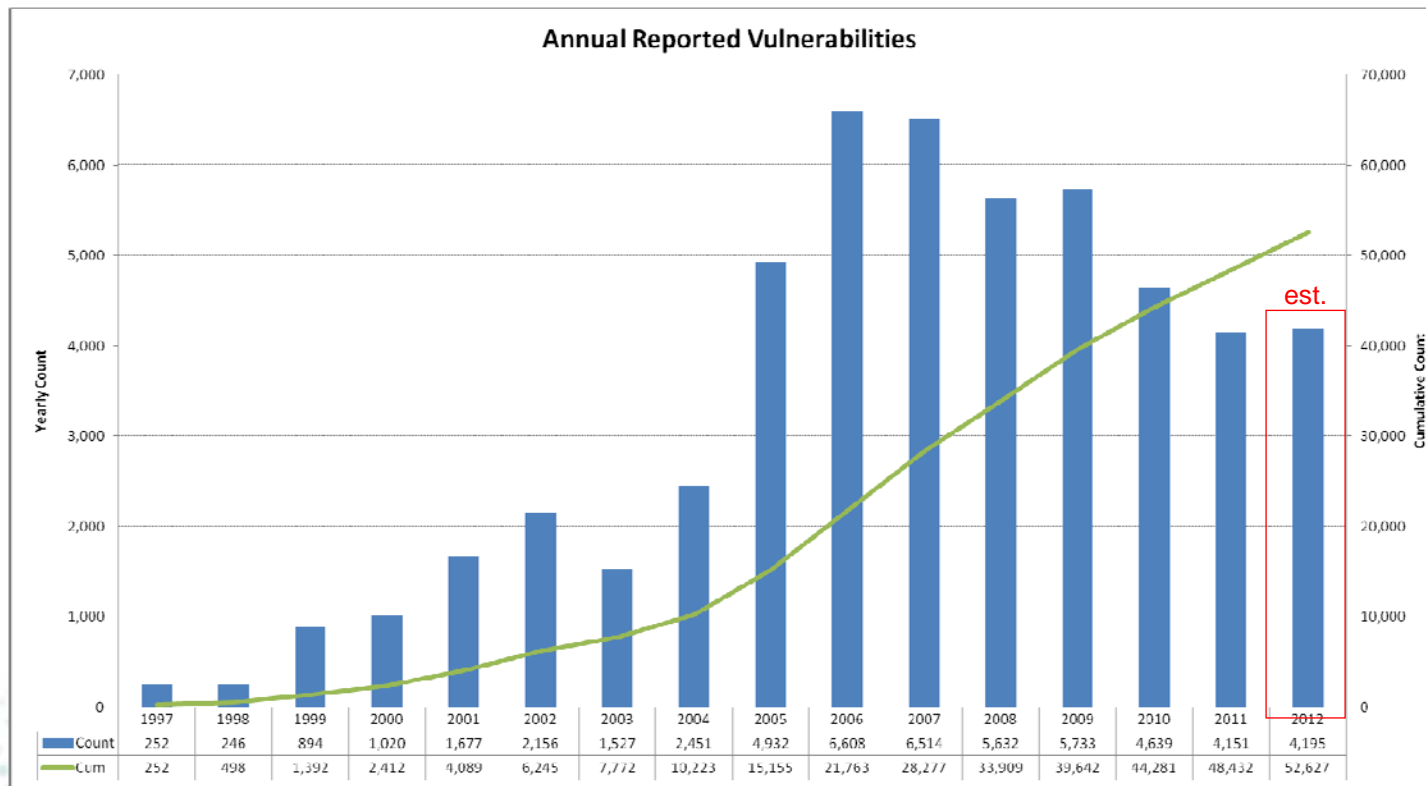
“Over 90% of cyber attacks exploit known security flaws for which a remediation is available”

- Gartner

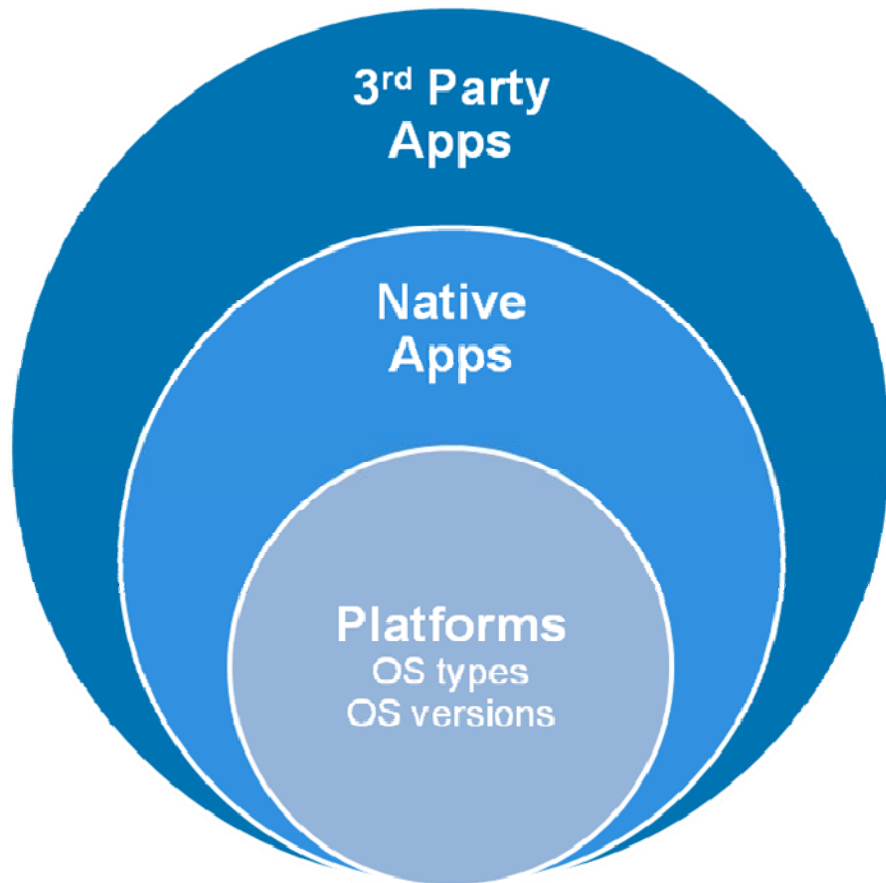
Proactively managing your vulnerabilities  
eliminates 90% of your risk ...

# Vulnerability growth remains high

- Software and OS lifecycle assumes new bugs; design flaws will be discovered as technology is adopted and deployed
- Nearly 90% of vulnerabilities can be exploited remotely
- On average, 12 new vulnerabilities are published per day
- Security threats are increasing across all platforms – not only MS Windows



# No longer just a Microsoft world

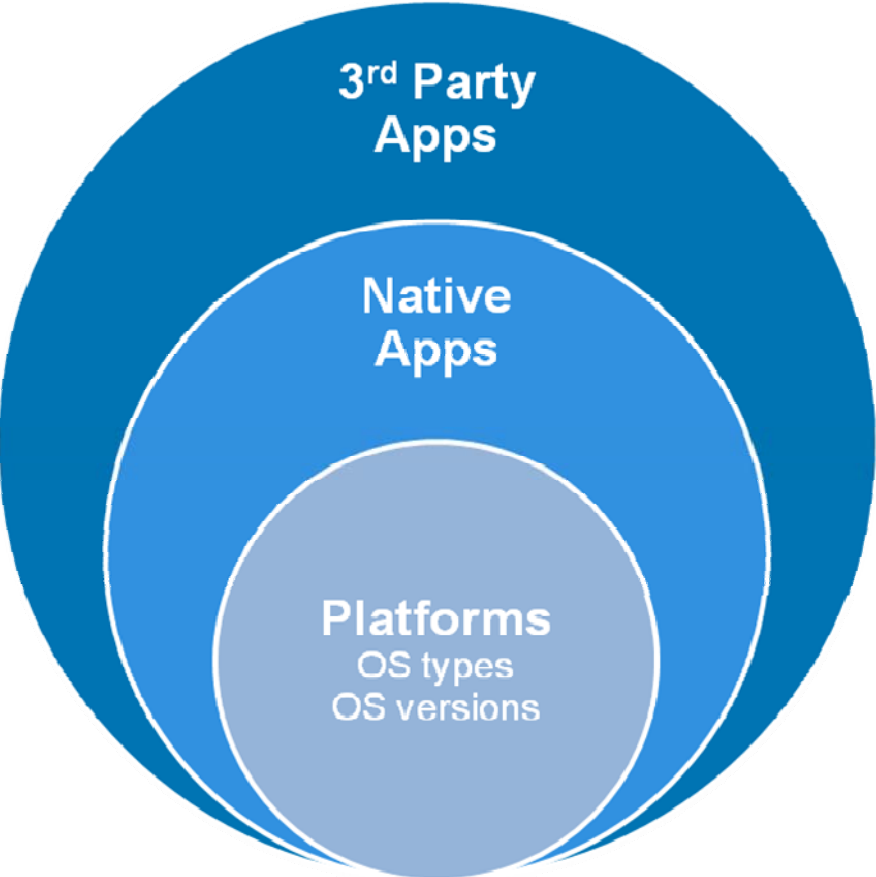


## Platform OS Vulnerabilities

Operating System	Percentage of Critical and High	Percentage of all OS Vulnerabilities
Microsoft	73%	27%
Apple	9%	29%
Linux	16%	31%
HP-UX	2%	1%
Sun Solaris	0%	4%
BSD	0%	4%
IBM AIX	0%	2%
Others	2%	4%

Apple and Linux – two of the top-3 highest percentage of all reported OS vulnerabilities.

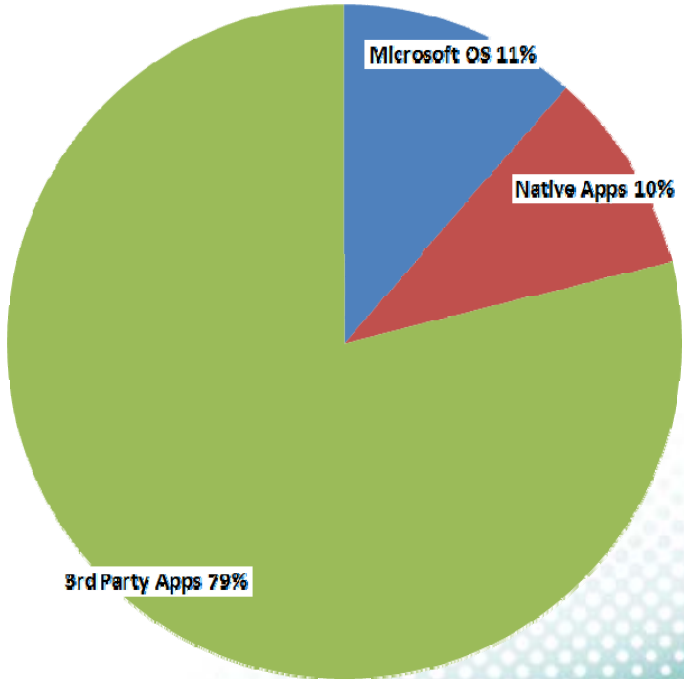
# 3rd party application vulnerabilities



3rd party apps represent a vast majority of endpoint vulnerability risk.

Patching the Typical Endpoint  
(comprising the top-90 software portfolio)

	Type	Vulnerabilities		Patching Tools
		count	pct	
Microsoft (28 programs)	OS	100	11.5%	1
	Apps	84	9.7%	
Third Party (22 programs)	Apps	685	78.9%	11
	total	869	100%	12



# Norman Patch and Remediation

Provides rapid, accurate and secure patch management for applications and operating systems

- Comprehensive Support for OS and Third Party Applications
- Streamline and Centralize Management of Heterogeneous Environments
- Visibility and Control of All Online or Offline Endpoints
- Elevate Security Posture and Proactively Reduce Risk
- Save Time and Cost Through Automation
- Improve Operational Efficiency While Reducing Energy Consumption
- Extensible and Customized Scripting

# Operating system support

Operating System	Version/Edition	Architecture
Apple Mac OS X	10.5 – 10.7	x86 (Intel)
Apple Mac OS X	10.5	PowerPC
CentOS	5 – 6	x86 and x86_64
HP-UX	11.31	Itanium
HP-UX	11.11 – 11.31	64-bit PA-RISC
IBM AIX	5.2 – 7.1	PowerPC
Microsoft Windows 7	Professional, Enterprise, and Ultimate	x86 and x86_64
Microsoft Windows Server 2008 R2	Web, Standard, and Enterprise	X86 and x86_64
Microsoft Windows Vista	All (excluding Home and Starter editions)	x86 and x86_64
Microsoft Windows Server 2008	All (excluding Core and Datacenter editions)	x86 and x86_64
Microsoft Windows XP	Professional (excluding Home, Media Center, and Tablet PC editions)	x86 and x86_64
Microsoft Windows Server 2003 Microsoft Windows Server 2003 R2	All (excluding Datacenter editions)	x86 and x86_64
Novell SUSE Linux	10 – 11	x86 and x86_64
Oracle Linux	4 – 6	x86 and x86_64
Red Hat Enterprise Linux	5.x – 6.x (Server, Desktop)	x86 and x86_64
Oracle Solaris	10	SPARC x86 and x86_64
Oracle Solaris	9	SPARC



# 3rd party application support – out of the box



## Apple

- QuickTime
- iTunes
- Safari
- iLife Suite



## Mozilla Firefox Content

- Firefox



## RealNetworks

- RealPlayer



## Oracle

- Java JRE



## WinZip

- WinZip



Adobe Reader

Adobe Shockwave Player

Adobe Flash Player

Adobe Acrobat Pro

Adobe Photoshop

Adobe InDesign

Adobe Air

- Support for the most targeted 3<sup>rd</sup> party applications (e.g., Adobe, Apple, Java, etc.)
- Track and report on vulnerabilities across all Windows and Mac machines in the same console



# What's new in NPR 7.2?

## Expanded Microsoft Windows content

- Derived from Microsoft WSUS, not the MBSA CAB file

## Introduce a new process for generating and releasing Microsoft content

- Support uninstall for Windows content when supported by Microsoft
- Support automated superseding and aging of WSUS parity content

## Faster release of Patch Tuesday content

- Built when Windows Update receives the content, not when CAB file is updated

## Optimized content delivery

- Remove the need to replicate the MS CAB file to WinXP and Win2003 endpoints
- Improved detection times on WinXP and Win2003

## Integrated Wake on LAN

- Wake up computers to perform patching.

# Norman Device Control

# Why Norman Device Control?

With Norman Device Control you can  
Minimize Insider Risk by Enforcing Security Policies  
for Removable Devices, Media and Data

# Norman Device Control

- Centrally manages security policies regarding use of removable devices (e.g., USB flash drives) and media (e.g., DVDs/CDs) using a flexible whitelist approach
- Encrypts data being copied to removable devices / media for additional protection
- Prevents malware intrusion via removable devices / media, adding a layer of protection to your network
- Provides the visibility, forensics and reporting needed to demonstrate compliance with applicable laws
- Integrates with additional IT security and operations modules

# Key Benefits

- Enables Secure Use of Productivity Tools, like USB Sticks
- Enhances Security Policy Enforcement
- Protects Data from Loss and Theft
- Ensures Data is Encrypted
- Protects against Malware via USB Devices
- Delivers Precise Control with Access Limits
- Integrates with Endpoint Operational and Security Modules for Defense-in-Depth



# Key Features

- Per-Device Permissions
- Device Whitelisting
- Flexible Policy with Granular Control
- Policy-based Encryption
- File Tracking / Shadowing
- File Type Filtering / Malware Protection
- Copy Limits
- Offline Enforcement
- In-Depth Reporting
- Centralized Management / Administrators' Roles
- Integration with Norman Enterprise Security

# What's new in NDC 7.2

- Fully integrated into NESEC
  - Customizable dashboard views

# Norman Application Control

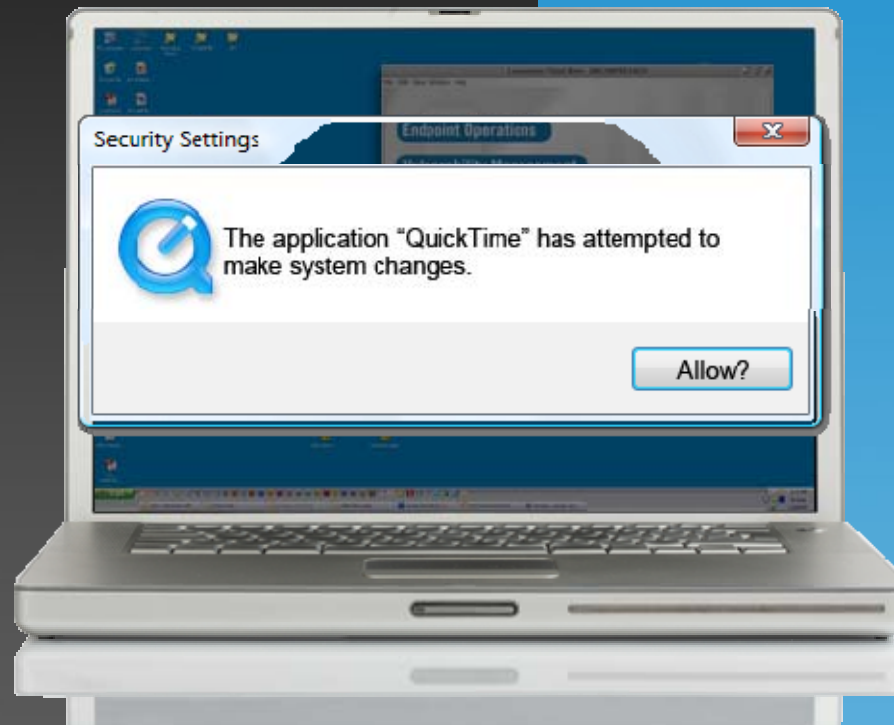


# Why Norman Application Control?

Norman Application Control provides effective malware protection and increases IT and end-user productivity by preventing any unknown, un-trusted or malicious applications from executing.

# THREAT CENTRIC

» Is this bad?



# TRUST CENTRIC

- » Is this bad?
- » Is this good?
- » Where did this come from?
- » What's trying to install this?
- » Who wrote this?
- » Should my user have this?
- » Is this unwanted?

# Norman Application Control benefits

- **Increased IT Security** – Norman Application Control enables a true Defense-in-Depth security approach which eliminates untrusted or unwanted changes to endpoints
- **Reduced IT Costs** – Norman Application Control reduces operational costs of handling constant malware infections on the endpoint
- **Increased IT Productivity** – Norman Application Control reduces the time IT spends on unplanned downtime by eliminating underlying causes (e.g., malware and software conflicts), freeing them up to work on more strategic initiatives
- **Improved Control** – Norman Application Control allows organizations to regain control over endpoint changes pushed by “local admin” end users and over the “patch gap” which leaves holes open for zero-day malware

# Norman Application Control

## Manage

Automatically update whitelist policies when software updates and security patches are deployed.

## Enforce

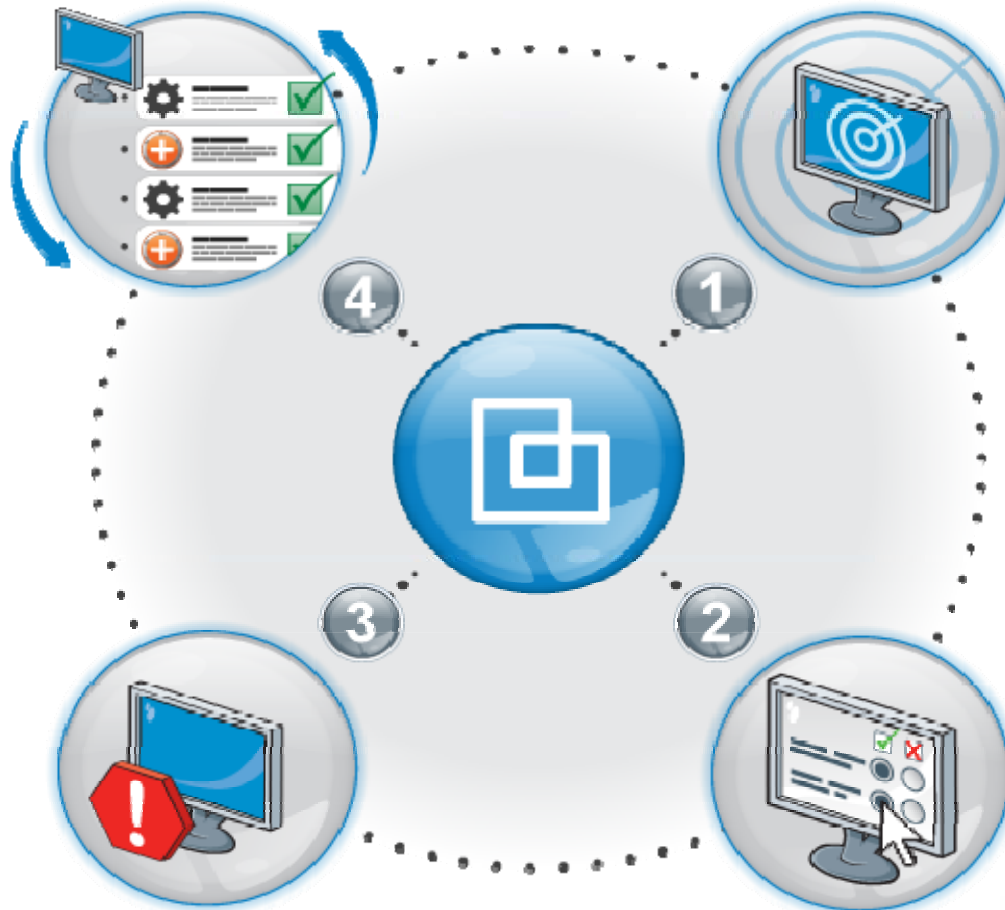
Automatically block unknown / unwanted applications and prevent zero-day attacks, and extend control over end users with Local Admin privileges.

## Discover

Snapshot individual endpoints to identify and catalog all resident executables and quickly determine potential application risk.

## Define

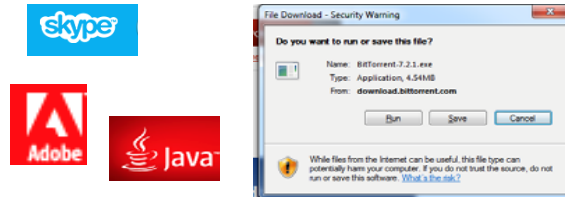
Flexible, rules-based Trust Engine ensures that the whitelist is automatically and constantly updated to permit authorized applications to run.



# Reduce Local Admin Risk with Application Control

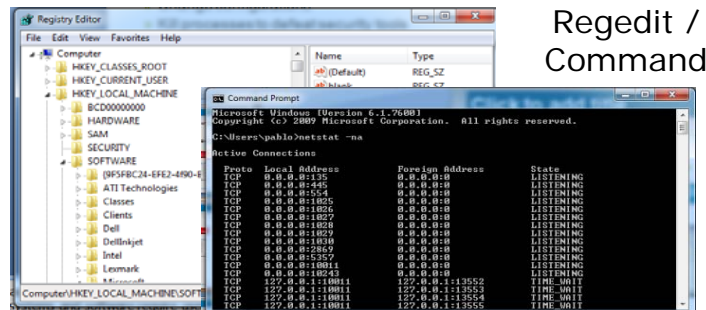
Action	Example	How NACStops
--------	---------	--------------

Install Applications



Application Control:  
*Easy Lockdown*  
*Trust Engine*

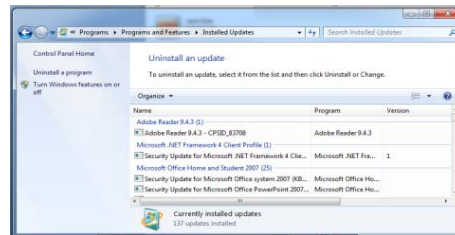
Change Configurations



Regedit /  
Command

Denied Application:  
*cmd.exe*  
*regedit.exe*

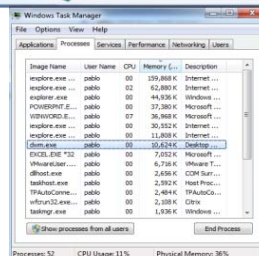
Remove Patches &  
Uninstall Software



Control Panel  
– uninstall  
program

Denied Application:  
*control.exe*

Defeat Security Tools



Task  
Manager –  
kill process

Denied Application:  
*taskmgr.exe*



# Define – Trust Engine

**What It Does** – Automate and verify trusted change on endpoints.

## How It Works

The “Trust Engine” validates endpoint changes based on trust rules and automatically updates endpoint whitelists

Trust rules can be defined based publisher, updater, path, and local authorization

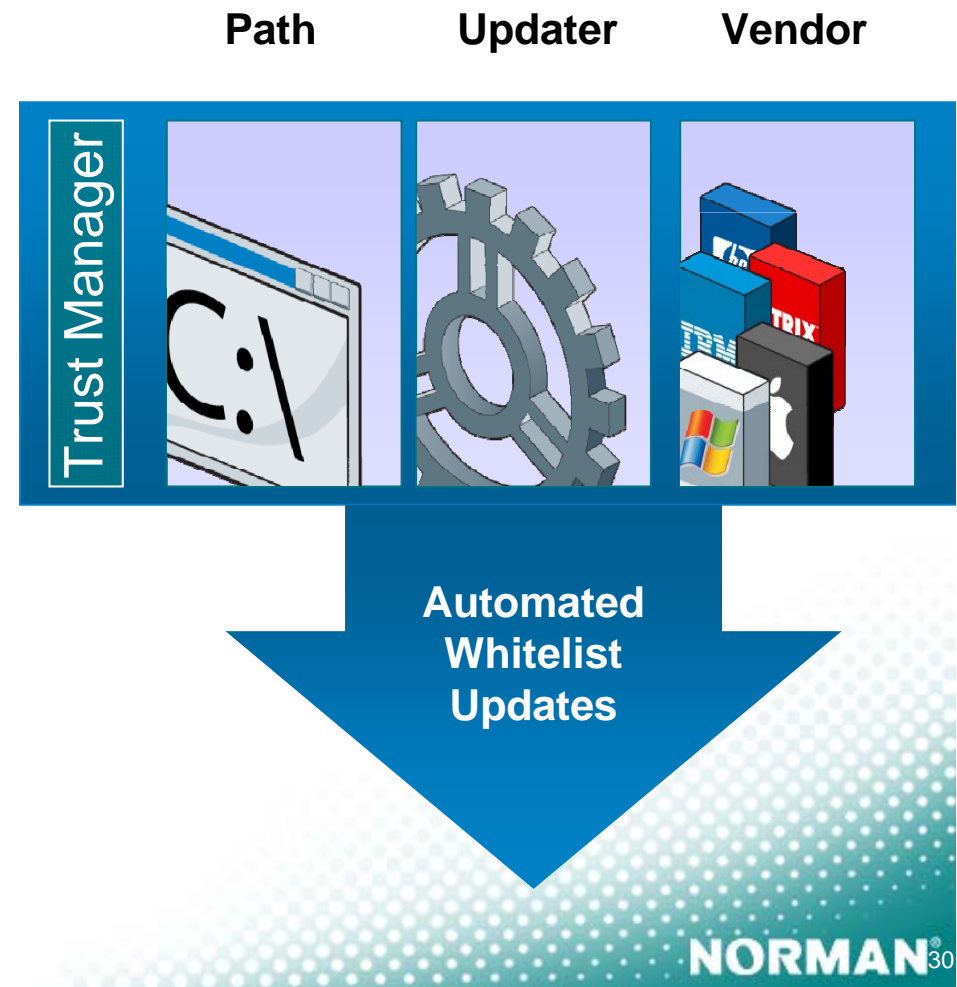
## Value

**Ensures end users are not disrupted!**

Provides adaptable security – from highly locked down to highly flexible – for dynamic endpoint environments

Lowers whitelisting TCO by automating trust decisions and whitelist maintenance

Provides frictionless end-user experience by providing flexibility necessary for daily business tasks

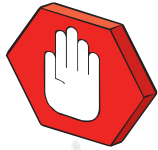


# Application Control: End User Experience - Policy Options

Norman Application Control supports multiple end-user policy types

## Policy 1

## Policy 2



# Block:

Application is not on approved list

 **NOTICE**

---

Notify end-user  
with customer defined message





Event  
Logging



# Alert:

Application is not on approved list

 **WARNING**

---

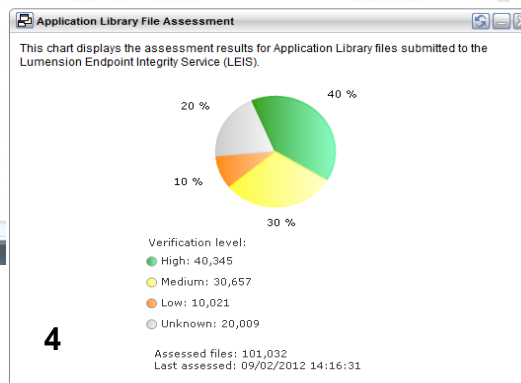
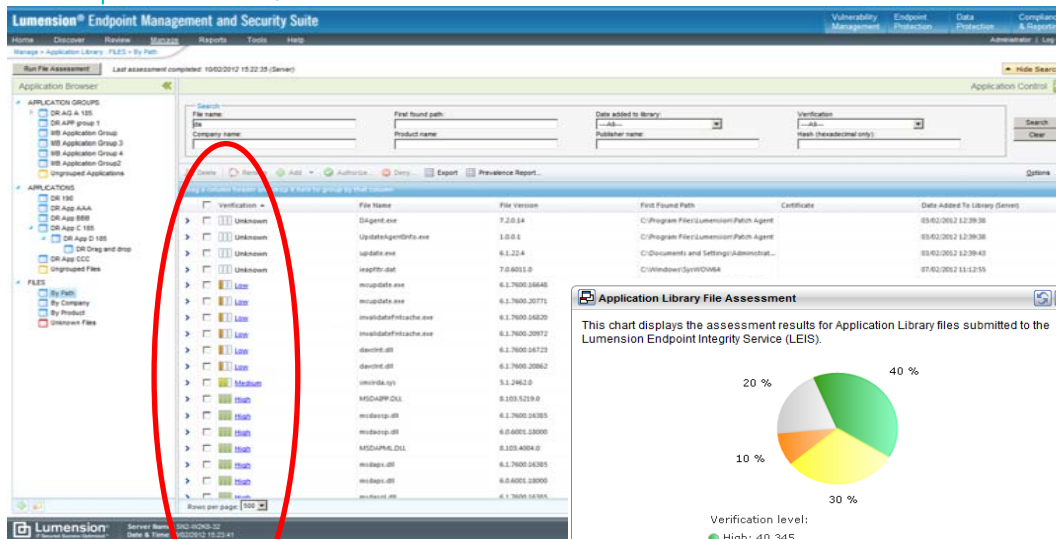
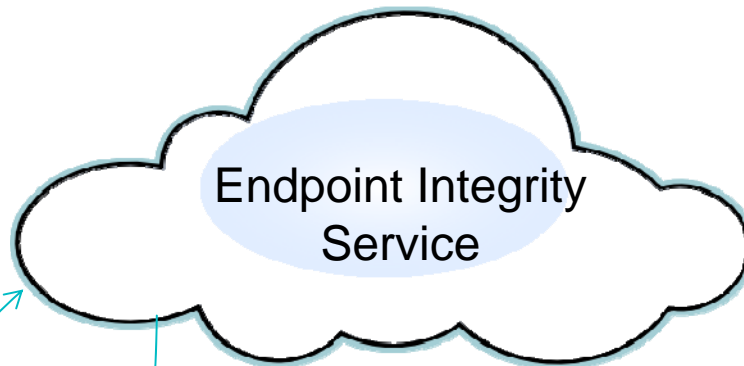
Local Authorization



Event  
Logging



# Trust Score Integration



## Trust Score Workflow

1. Hashes sent to EIS
2. EIS returns verification rating for known files
3. App Library displays rating in verification column
4. Dashboard widget updated

## Trust Score (File Verification)

- Confidence level that file is what it claims to be

## Benefits

- Reduces App Library management overhead
- Use verification rating to make authorization/grouping decisions
- Additional features to further simplify the task of App Library management
  - Select all across multiple pages
  - Drag & Drop
  - Authorize/Deny from Library



# Whats new in NAC 7.2?

- Trust Score Integration
  - EIS Integration
- Local Authorization
- Application Library enhancements
- Scheduled Application Event Log Query
- Authorized App Policy  
[aka Supplemental Easy Lockdown / Auditor Policy]
- Trusted Updater enhancements

# NESEC Pricing

# NESEC Pricing model

Server license (1-time fee)

+

Base Module1 price  
(subscription)

+

Base Module 2 price  
(subscription)

+

Base Module 3 price  
(subscription)

=

Sales price

## Discounts

2 Base Modules  
20% discount\*

3 Base Modules  
30% discount\*

There is no discount for the  
add-on module Norman  
Content Wizard

\* Discount applies to the lowest  
common number of clients

# Norman Patch and Remediation – Base Module

Norman Patch and Remediation Windows Platform						
Users	Price in Euro			Renewal price in Euro		
	1 Year	2 Years	3 Years	1 Year	2 Years	3 Years
10 - 250	15,49	29,44	41,84	15,49	29,44	41,84
251 - 500	14,09	26,76	38,03	14,09	26,76	38,03
501 - 1000	13,38	25,43	36,13	13,38	25,43	36,13
1001 - 2000	13,02	24,76	35,18	13,02	24,76	35,18
2001 - 3000	11,97	22,75	32,33	11,97	22,75	32,33
3001+	10,78	20,47	29,10	10,78	20,47	29,10
Norman Patch and Remediation Non-Windows Platform						
10 - 250	28,17	53,53	76,06	28,17	53,53	76,06
251 - 500	24,65	46,84	66,56	24,65	46,84	66,56
501 - 1000	21,13	40,15	57,05	21,13	40,15	57,05
1001 - 2000	17,61	33,45	47,54	17,61	33,45	47,54
2001 - 3000	14,09	26,76	38,03	14,09	26,76	38,03
3001+	12,68	24,09	34,23	12,68	24,09	34,23

# Norman Content Wizard – Add-on Module

## NESEC Add-On Module: Norman Content Wizard

Users	Price in Euro			Renewal price in Euro		
	1 Year	2 Years	3 Years	1 Year	2 Years	3 Years
10 - 250	5,63	10,70	15,21	5,63	10,70	15,21
251 - 500	4,93	9,37	13,31	4,93	9,37	13,31
501 - 1000	4,58	8,70	12,36	4,58	8,70	12,36
1001 - 2000	4,23	8,03	11,42	4,23	8,03	11,42
2001 - 3000	3,52	6,69	9,51	3,52	6,69	9,51
3001+	3,17	6,02	8,56	3,17	6,02	8,56

# Norman Application Control – Base Module

## NESEC Base Module: Norman Application Control

Users	Price in Euro			Renewal price in Euro		
	1 Year	2 Years	3 Years	1 Year	2 Years	3 Years
10 - 250	19,72	37,47	53,25	19,72	37,47	53,25
251 - 500	17,61	33,45	47,54	17,61	33,45	47,54
501 - 1000	16,20	30,78	43,74	16,20	30,78	43,74
1001 - 2000	14,79	28,10	39,93	14,79	28,10	39,93
2001 - 3000	13,38	25,43	36,13	13,38	25,43	36,13
3001+	12,01	22,89	32,52	12,01	22,89	32,52

# Norman Device Control – Base Module

## NESEC Base Module: Norman Device Control

Users	1 Year			2 Years			3 Years		
	1 Year	2 Years	3 Years	1 Year	2 Years	3 Years	1 Year	2 Years	3 Years
10 - 250	18,79	35,70	50,73	7,20	13,00	17,30	6,80	12,20	16,30
251 - 500	14,52	27,59	39,20	6,40	11,50	15,40	6,00	10,80	14,40
501 - 1000	12,07	22,94	32,59	6,00	10,10	13,40	5,60	10,10	13,40
1001 - 2000	9,97	18,95	26,92	5,20	9,30	12,40	5,20	9,30	12,40
2001 - 3000	9,39	17,85	25,37						
3001+	8,46	16,07	22,83						

# Migration



# Replacing old products

NESEC will replace all existing «Lumension» products

Discontinuing:

- Norman Patch and Remediation 6.4
- Norman Patch and Remediation 7.0
- Norman Device Control 4.4
- Norman Application Control 4.4

# Application and Device Control

- I will work directly with the countries who currently have active Device Control customers to determine the best way to EOL Device Control 4.4
- Lumension wishes to, as soon as possible, to stop delivery of updates to NADC 4.4
- Possible incentives to get existing NADC 4.4 customers to migrate:
  - Free upgrade (no server fee)
  - Free consulting
  - Free add-on product, for example Patch and Remediation
  - Free 1 year extension of license

# Patch and Remediation

Upgrade from 7.0 is as easy as to install over existing version

Customers on 6.4 need to upgrade to 7.0 then upgrade to 7.2.  
Alternatively re-install

# Campaign

28<sup>th</sup> November – 28<sup>th</sup> December 2012

# New sales:

## **New sales:**

Your new customers will receive a FREE license of Application Control valid for the duration of the prepaid license period, if they buy both Patch and Remediation and Device Control.

- Buy 1 year license of Patch and Remediation and Device Control, receive 1 year free license of Application Control
- Buy 3 year license of Patch and Remediation and Device Control, receive 3 year free license of Application Control

# Existing customers

Renew current license of either Patch and Remediation, Device Control or Application Control and choose the other product for free.

- The renewal offer is valid for the duration of the prepaid license period:
  - Renew one year license, receive one year license of the product for free.
  - Renew 3 year license, receive 3 year license of the other product for free.
- For example
  - Renew Patch and Remediation contract, get Device Control for free (renew 1 year license of Patch and Remediation, receive 1 year license of Device Control)
  - Renew both Patch and Remediation and Device Control contracts, get Application Control for free (renew 1 year license, get 1 year free)

# Collaterals

# What Norman HQ will deliver

- Web pages
  - NESEC
  - NPR
  - NAC
  - NDC
- Product sheets
  - NESEC
  - NPR
  - NAC
  - NDC
- Cheat sheets (Norman branded?)
  - NPR
  - NAC
  - NDC



# Other collaterals

Lumension offers a variety of different collaterals.

- Norman HQ will not take on rebranding all of these documents, but will make these available in native Lumension format.
- Each Norman office is welcome to re-purpose these documents as they see fit.
  - Please share any Norman branded versions of documents to avoid double work

Questions?