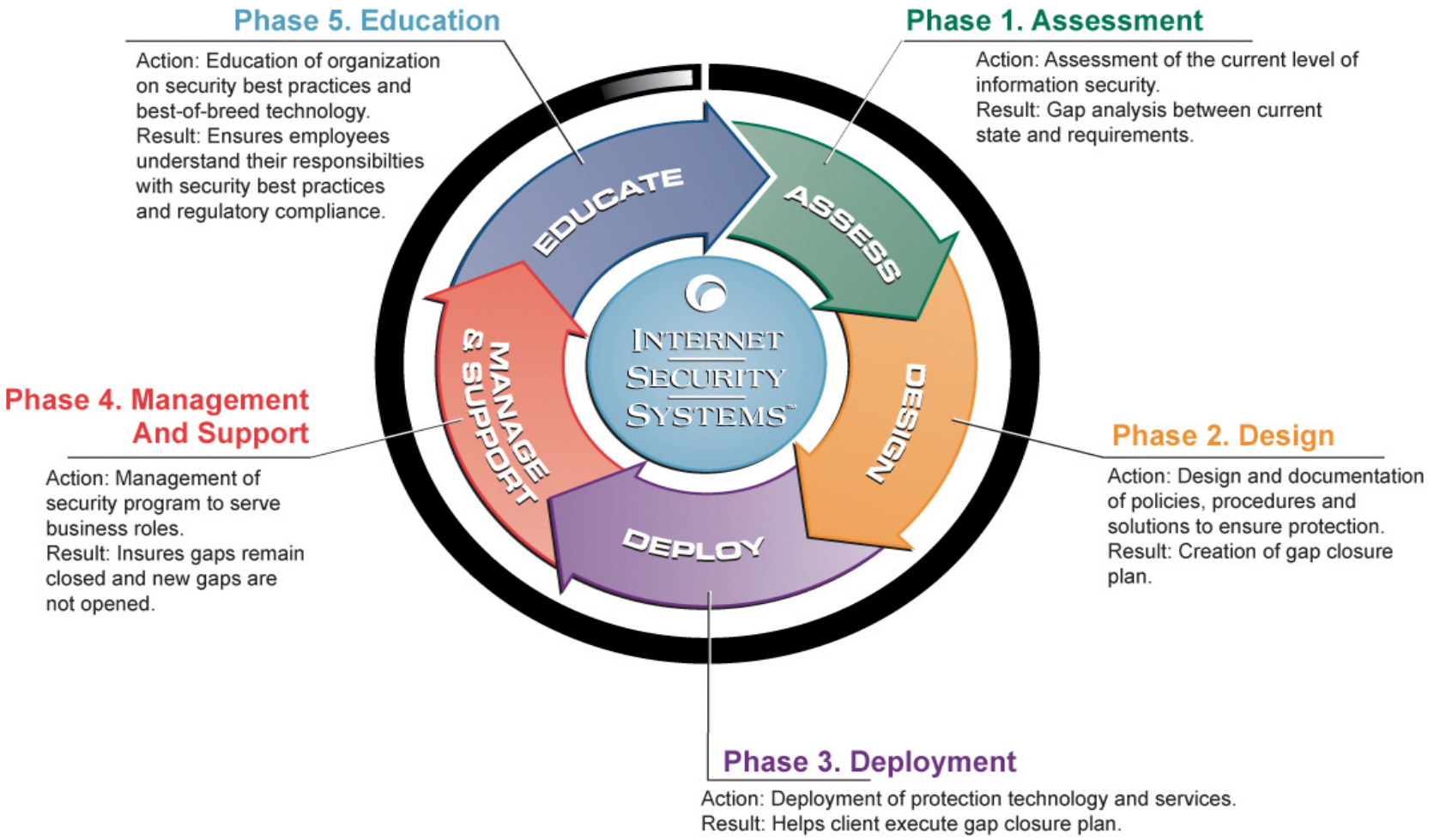
Security Basics: Putting the Pieces Together

Jimmy Brooks – Senior Product Manager, Verio
Rick Miller – VP Managed Security, ISS

ADDME – Lifecycle Approach



A few words about the Security Policy

Specific and Clear

- What needs to be done
- Why the policy exists
- Who or what function is responsible

Be Realistic – avoid the unenforceable policy

- Don’t make encryption mandatory and then fail to provide an easy means for employees to do it
- Passwords or Tokens that get stuck to monitors
- Is it realistic to think that people will not visit Yahoo Sports?

Assessment

Value Proposition

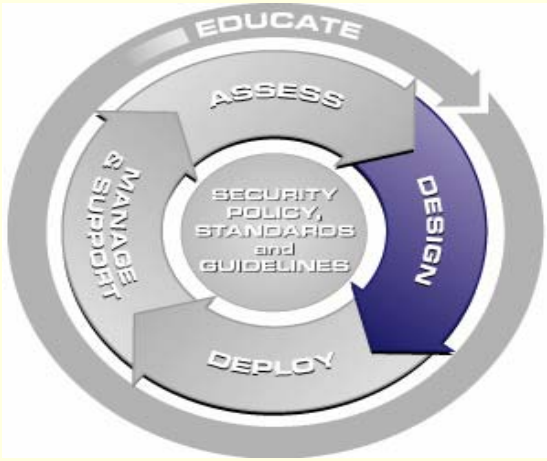
- Clear understanding of current security posture
- Detects vulnerabilities and threats
- Understanding of business risk
- Provides a clear action plan
- Empowers informed decision making
- Raises security awareness and issues
- Allows an organization to mitigate risks before they are exploited
- Validates the effectiveness of security safeguards and controls

Assessment

Suite of Assessment Tasks

- **Information Security Assessment**
- **Penetration Tests**
- **Application Security Assessment**
- **Wireless Network Security Assessment**
- **Security Testing and Certification Program**
- **Policy Gap Assessment**
- **Business Risk Assessment**
- **Vertical Market Gap Assessments**
  - HIPAA
  - Gramm-Leach-Bliley
  - Sarbanes-Oxley
  - California Senate Bill No. 1386
  - SCADA

Design



Value Proposition

- Clear strategy for securing networks
- Path to quickly implementing key security technologies, controls and management
- Builds organizational consensus on how to proceed.
- Reduces total cost of ownership

Design

Design Tasks

- **Protection Policy Development**
  - Technology Management Policies
  - Operational Guidelines
  - Configuration Procedures
- **Standards Development**
- **Procedures Development**
- **Security Strategy Workshop**
- **Implementation Planning**
- **Network Architecture Design**

- **Keep the Goal in mind …..It is not about specific technologies**

Design - Technology

- Firewalls
- VPN
- IDS/IPS
- Anti Virus
- Anti Spam
- Content Filtering

Design - Firewalls

- Where
  - Perimeter Access Control
  - Internal for functional separation and policy enforcement
- Strengths
  - Mandatory first line of defense
  - Can also be used to provide other functions (VPN, Remote access, etc.)
- Weaknesses
  - Not a good judge to the quality of the traffic being allowed through allowing Virus', Worms, buffer overflow, etc.
- Future
  - Pure access control firewalls will be part of network infrastructure and "smart" firewalls will continue to evolve as primary security technology.\

Design -VPN

- Why? – C.I.A.
- Where
  - Remote Access
  - Site to Site IP traffic
  - Internal for sensitive data
- Strengths
  - Inexpensive and Quick compared to dedicated lines
  - Secure and crypto level should be taken into consideration
- Weaknesses
  - VPN access also increases exposure to other risks
  - Increases burden on the network
  - Troubleshooting problems can be complex

Design - IDS/IPS

- Where and Why
  - Behind firewall for network exploit detection / virtual patch
  - On critical servers for virtual patch protection
  - Make Sure you monitor outgoing traffic as well as incoming
- Strengths
  - IDS helps identify malicious use
  - IPS can block many exploits
- Weakness
  - A lot of information generated requiring security expertise
  - Proper tuning to the environment and vulnerabilities is key
- Future
  - Blending of security technology into multifunction edge appliances

Design - Anti-Virus

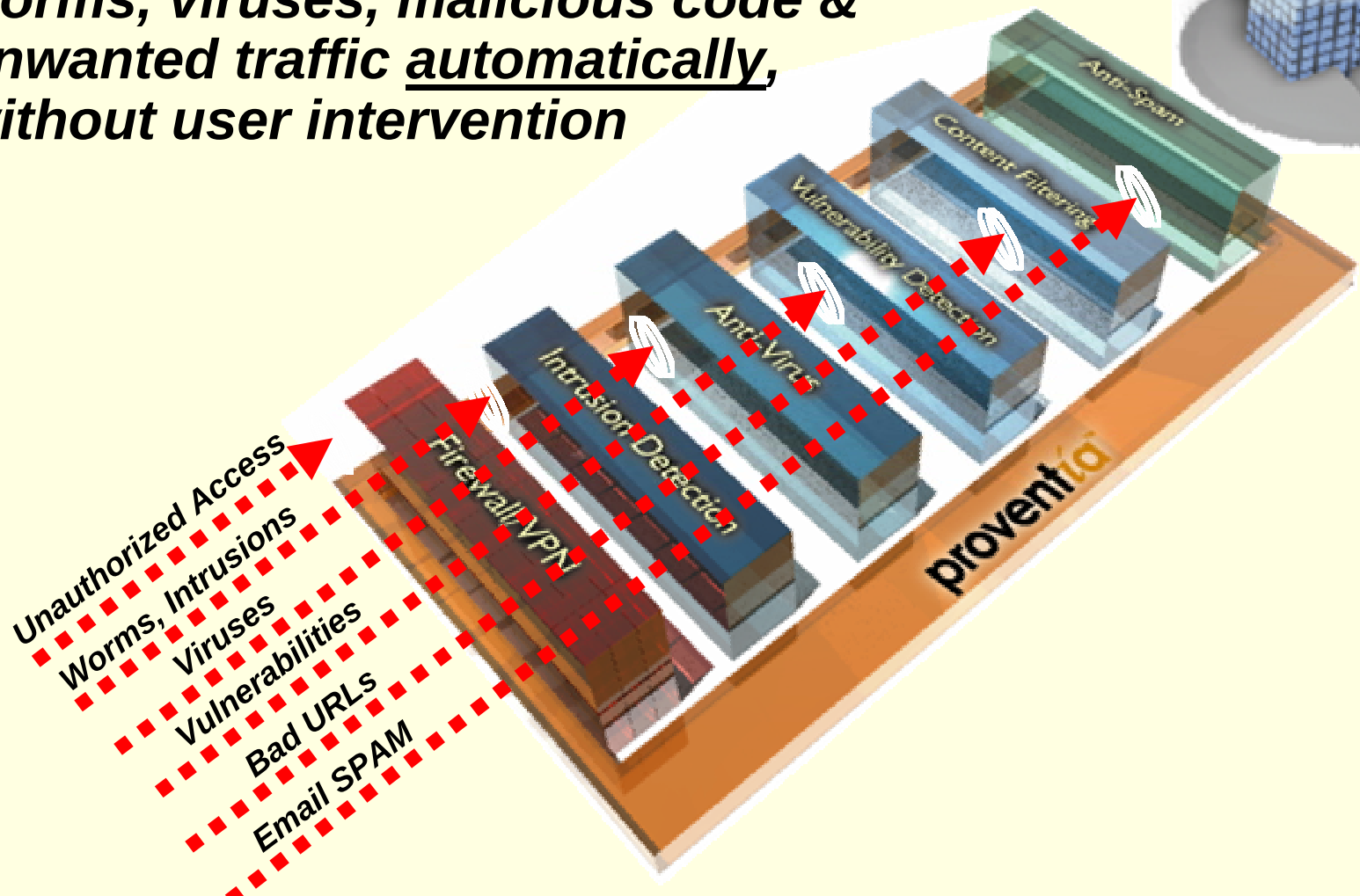
- Where – Gateway and Desktop
- Strengths
  - Effective and mature technology
  - Accepted as a must have security technology
- Weaknesses
  - Traditional signature AV not good at stopping true day zero exploits that travel quickly such as Worms
  - Polymorphic malware

Design - Content

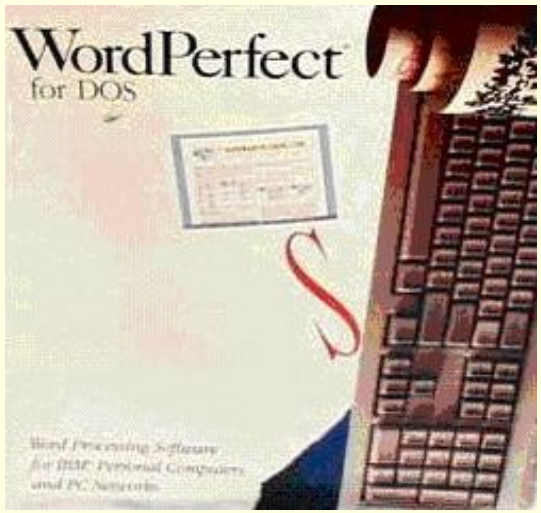
- Have Corporate Policies in place before technology implementation
- 60% of all email is now SPAM
- Phishing
- URL Screening
- SpyWare/AdWare
- What is next and what new solution will we want to sell you to solve it?

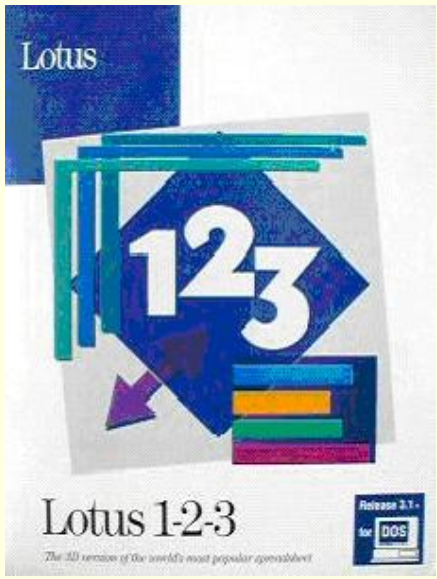
Design - Next Generation Internet Security

Unified protection technology that identifies and blocks hackers, worms, viruses, malicious code & unwanted traffic automatically, without user intervention

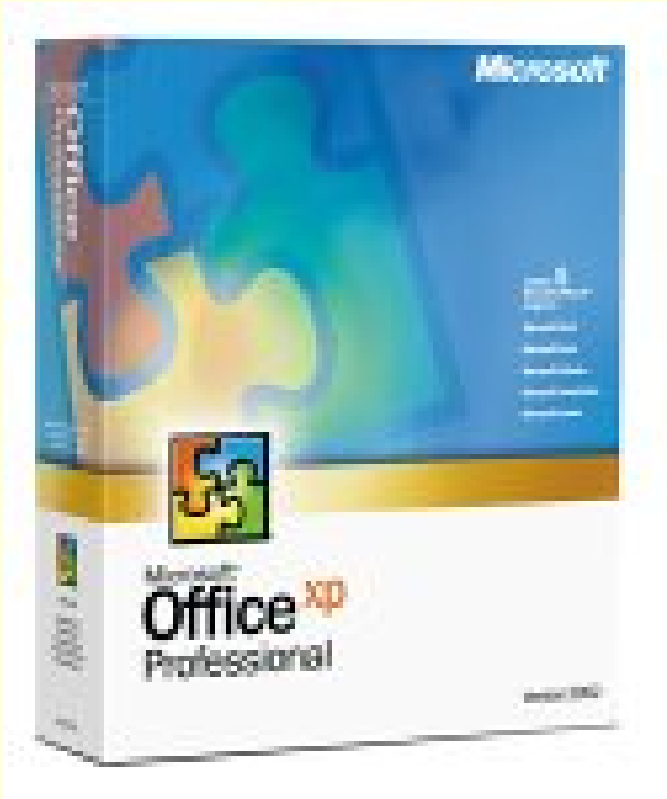


Design - Point Products vs. Unified Solutions

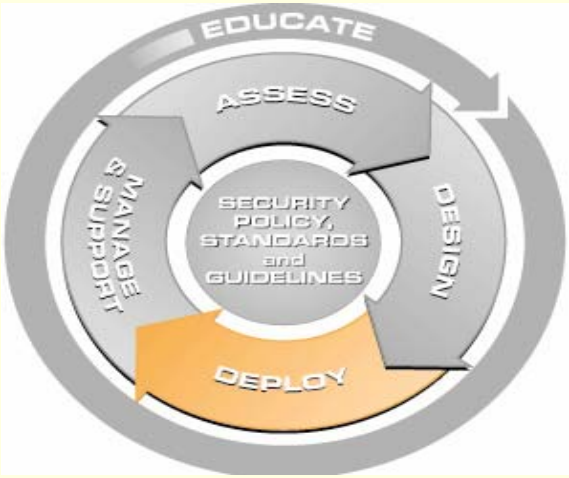




Design - Point Products vs. Unified Solutions



Deployment



How do I get there?

Value Proposition

- Make good use of the technology
- Communication and Coordination
- Project Manager
- Steering Committee
- Do not forget these costs
- Unless you have solid expertise dedicated consider external resources to assist

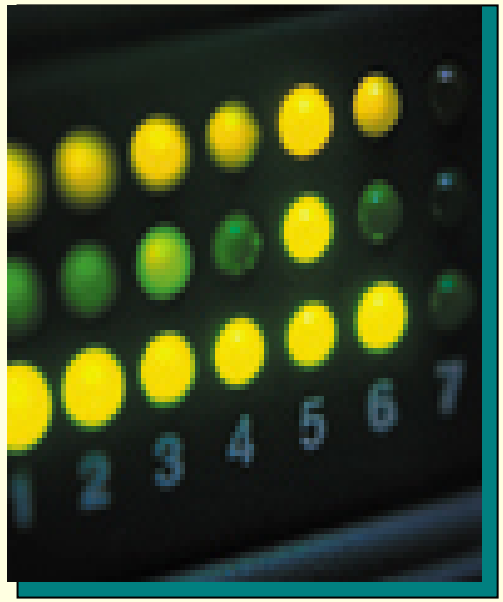
Deployment

- Vulnerability Remediation
- Virtual Patch
- Network team
- Security team
- Desktop team
- Virtual team

Manage & Support

Should you Consider Outsourcing?

- **Do you require 24x7x365**
- **What is the value of the asset you need to protect**
- **Do you have sustainable expertise**
- **Is your expertise better utilized in a more strategic role**
- **What is your expectation for quality and reporting**
- **Is it important to have openness about security problems**



Manage & Support - Outsourcing

- Things to look for in a MSSP
  - What visibility will you have – Portal
  - Service Level Agreement
  - Professional Services Capability
  - Security Intelligence
  - Relationship Management Strategy
  - How do they do… What they do
  - Understand where and how your people fit in

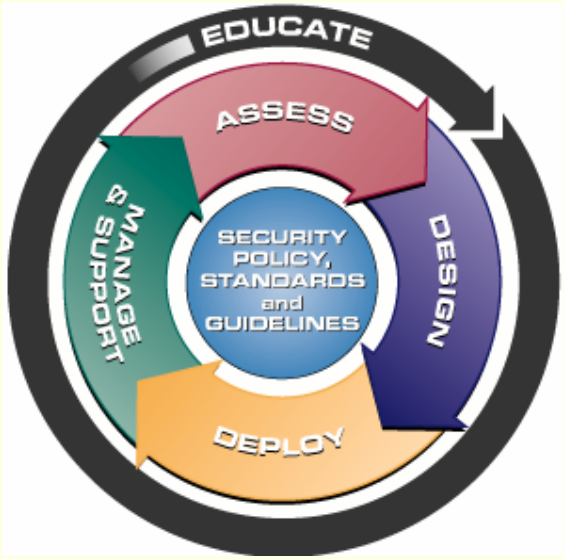
Manage & Support - Portal

- Security Incident Report for each escalation
- Trend Reporting
- Vulnerability Posture
- Security information that you can use
- View Raw & Normalized Data
- View and Interact with work logs
- SLA reporting
- Event Trends/ other reports
- View Sites / Devices / Contacts

Manage & Support

- Keep abreast of new Laws
- Keep abreast of new threats
- What about patching?
- Ongoing Assessment
- Do you need a security czar?
- Do you need some help?

Educate – Why and What Value



Value Proposition

- Prepares staff for security issues
- Empowers staff to maintain Solutions
- Provides understanding of information
- security environment
- Ensures the ability to understand the threat
- Generate relevant reports and alerts
- Lower overall total cost of ownership
- Certification

What do I need to know?