nemertes
RESEARCH

Data Leak Prevention (DLP) Implementation Strategy

John E. Burke
Principal Research Analyst
john.burke@nemertes.com

Agenda

- About Nemertes
- DLP Adoption Trends and Architecture
- Implementation Considerations
- Conclusion and Recommendations

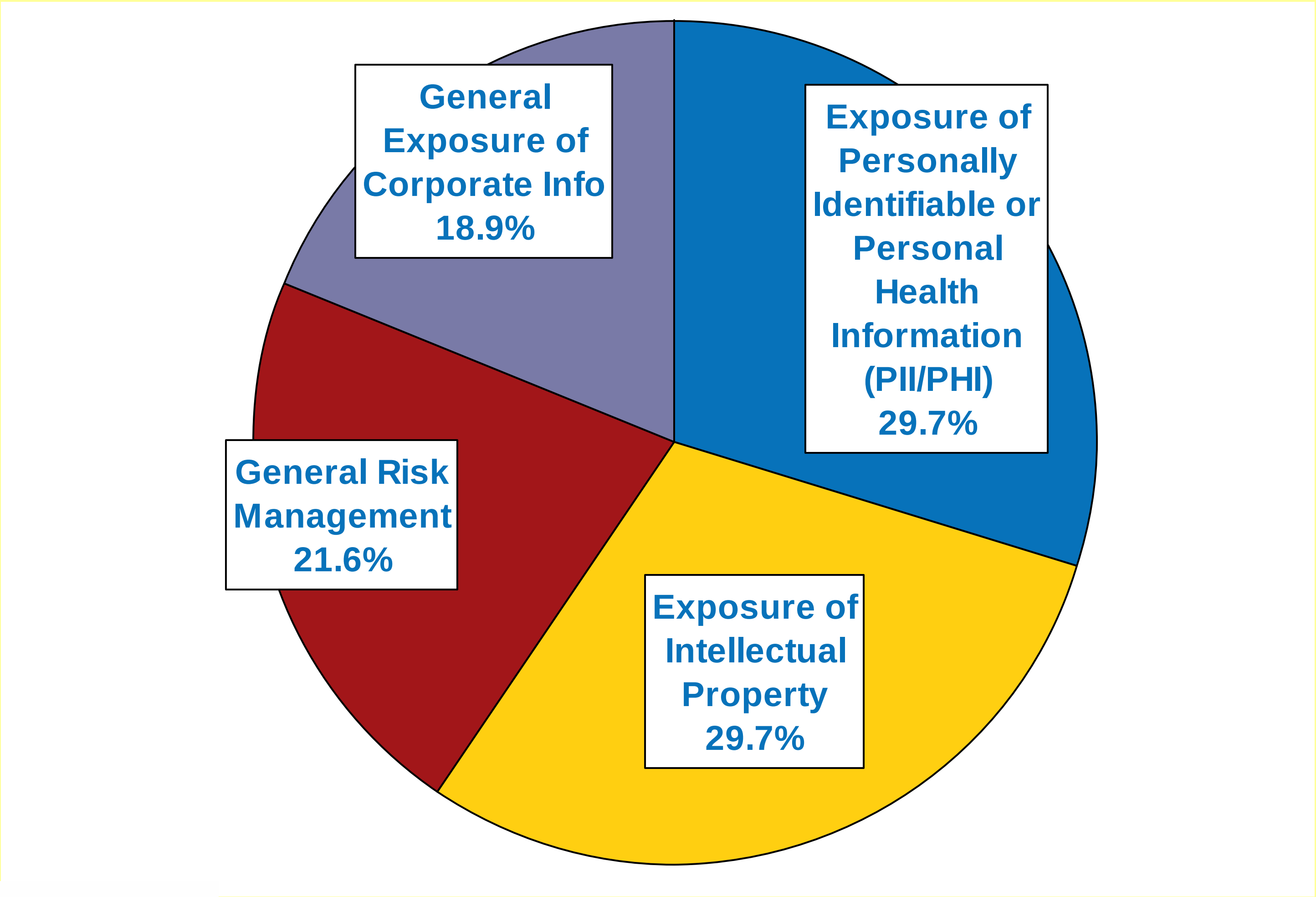
About Nemertes

- Quantifies the business impact of emerging technologies
- Conducts in-depth interviews with IT professionals
- Advises businesses on critical issues such as:
  - Unified Communications
  - Social Computing
  - Data Centers & Cloud Computing
  - Security
  - Next-generation WANs

- Cost models, RFPs, Architectures, Strategies

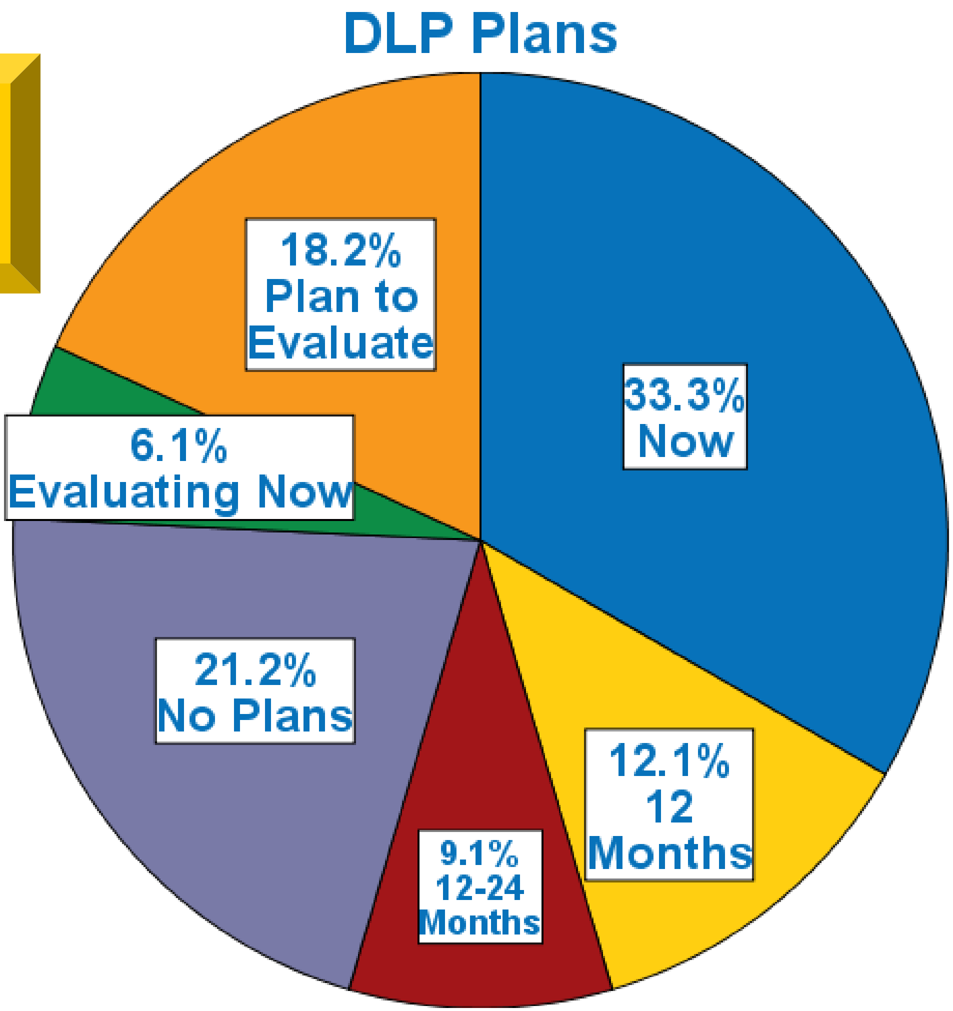
DLP Adoption Trends and Architecture

Protection of What?

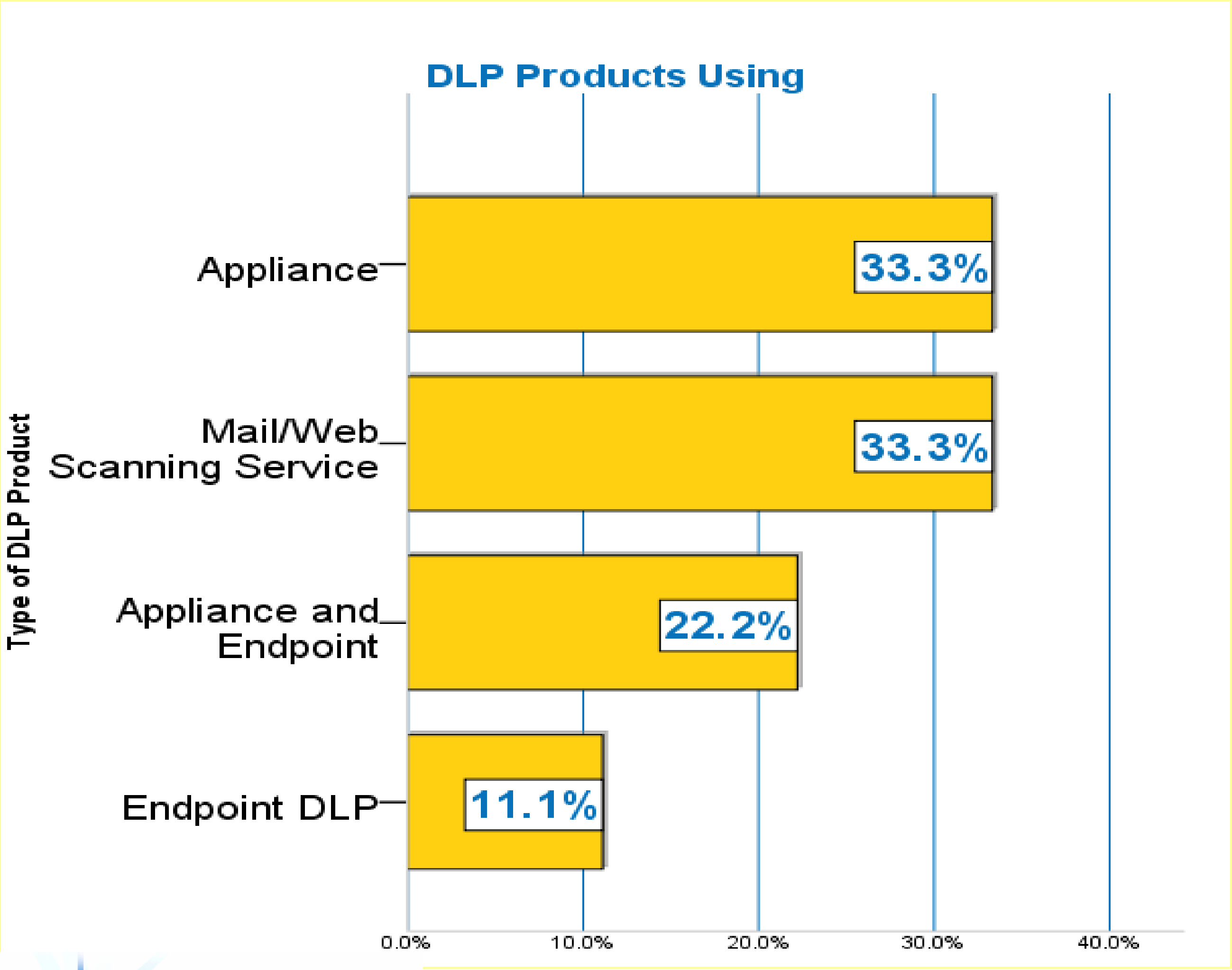


Enterprise DLP Plans

Average start is 2007

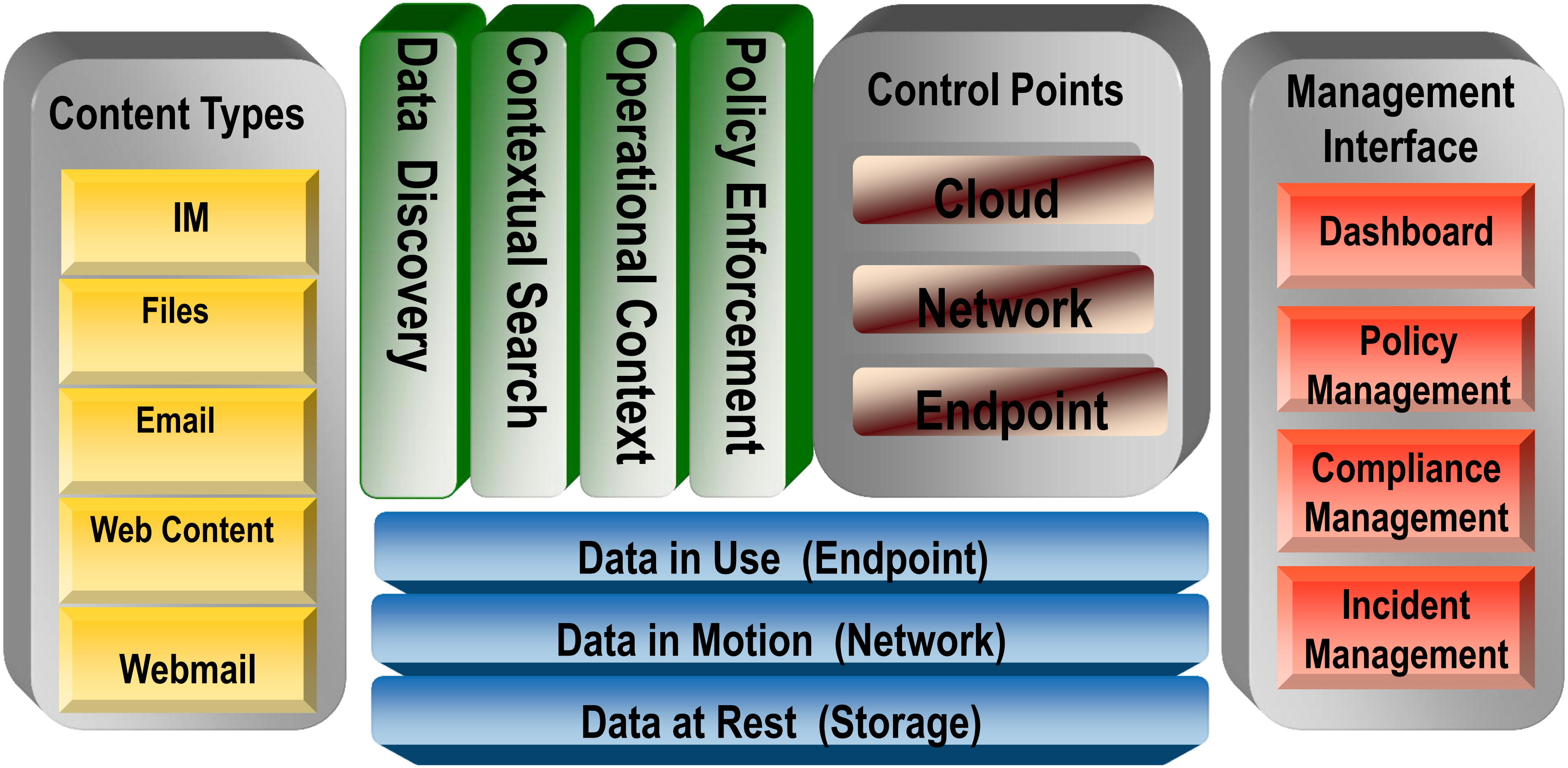


DLP Products In Use



Average spend of $95/employee

DLP Architecture



Implementation Considerations

People Dynamics of DLP

- Education is a critical success factor
  - Identification of PII, PHI and corporate confidential information
  - Understanding of processes to protect above
  - Understanding risks of the web
    - Phishing and spear phishing
    - The importance of keeping anti-X current
  - Understanding social engineering
- Significant risk is staff thinking they are doing “the right thing”
  - Example: “Emails down so I’ ll send you the sales forecast via my webmail account…..”

DLP Process Considerations

- Disturbing Lack of Process?
  - Often, implementation is piecemeal and a knee-jerk reaction to a breach or near-breach
- DLP needs to follow a risk-based process – top down
  - Define assets and assign values to loss
  - Define vulnerabilities and assess probability of exploit
  - Define all risks, their probability and impact
  - Determine the preventive and detective DLP controls necessary
- Focus on continual improvement
  - Follow a plan, do, check, act process to continually review DLP
  - Every data loss prevented needs a root cause analysis and establishment of process to prevent a repeat

Ten DLP Must Haves

- Universal search and automated discovery of sensitive data
  - Includes sensitivity to removable storage – USB drives, CDs and DVDs
- Minimal performance overhead
- Operational context to prevent leaks of specific data
  - Healthcare, financial, personnel, manufacturing, education, etc.
- Monitoring and blocking all data types and network protocols
- Automated reporting to support compliance and audit requirements

Ten DLP Must Haves Continued

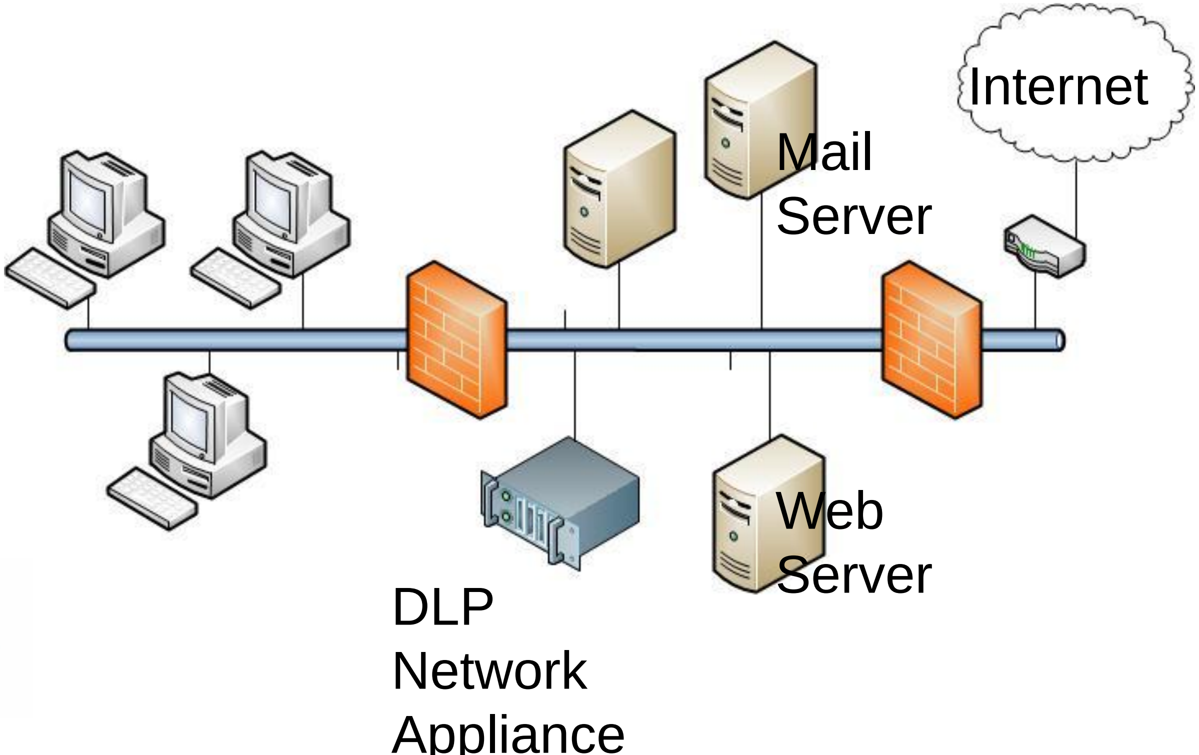
- Close tracking of false positives and negatives
  - False negatives → Data breach
  - False positive → Drain on management resources
- Visibility and control over encrypted data
  - Closely track non-VPN SSL traffic
- Role-based control over quarantined data
- Automation of policy enforcement and incident response
- Close integration with Security Information Event Management (SIEM) systems

Different Approaches: Endpoint DLP

	Advantage	Disadvantage
Endpoint DLP	▪ Local protection including USB lockout ▪ Offline protection ▪ Support of mobile devices	▪ Installation on every endpoint ▪ Susceptible to malware including rootkits ▪ Can require end-user actions

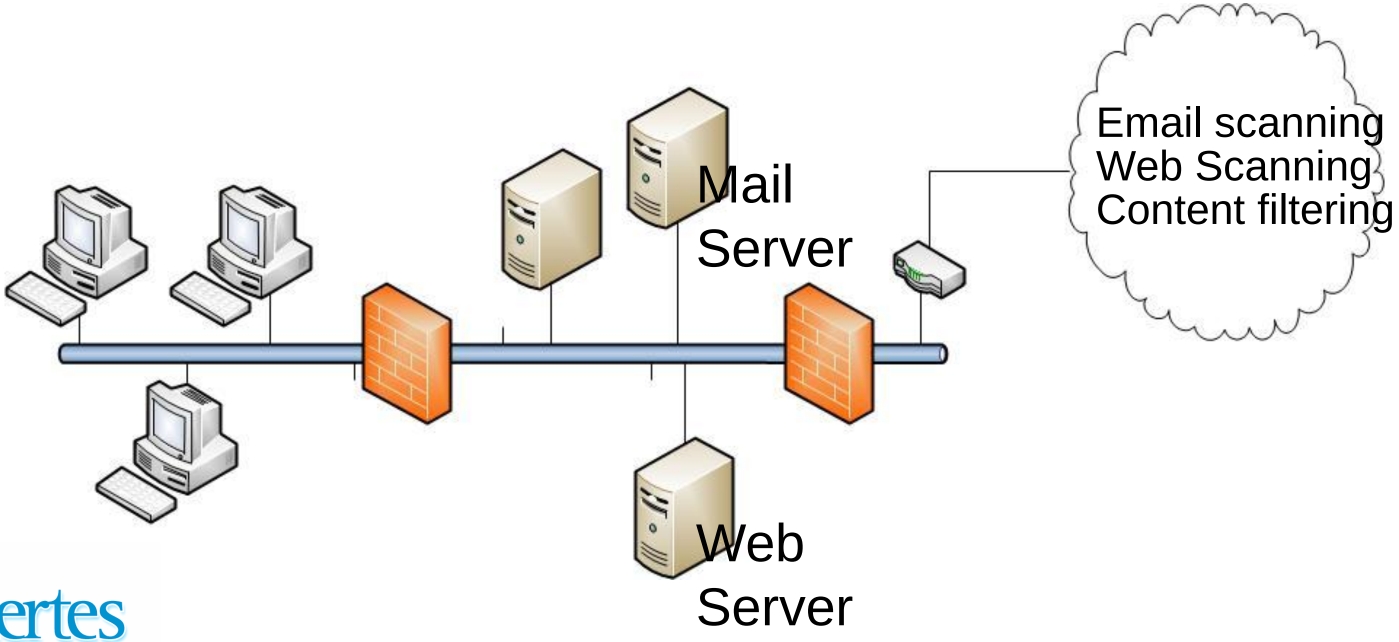
Different Approaches: Net Appliance DLP

	Advantage	Disadvantage
Network Appliance DLP	▪ Easy install and high performance ▪ Protection of all I/O including webmail ▪ Auto-discovery is typical	▪ No endpoint visibility - USB ▪ Cannot address offline users ▪ Requires redundancy for full protection



Different Approaches: Cloud-Based DLP

	Advantage	Disadvantage
Cloud-based DLP	- No CapEx - Supports mobile and teleworkers - Usually includes other features including AV and anti-SPAM	- No endpoint protection - USB - Cannot address offline users - Sensitive data in the cloud



Conclusion and Recommendations

Implementation Success with DLP

- Approximately 70% of organizations doing DLP rate their projects as very successful and just under 15% rate their projects as being extremely successful
  - Successful users stress the value of automated discovery and classification tools
  - Vendor support is critical to success – get references
- All organizations deploying appliance and endpoint solutions rate their DLP project as being very successful
  - A holistic and comprehensive approach is critical
  - Deploying only one type of solution limits the potential for catching potential leaks
- Highest success correlates with protection of PII and PHI. Organizations protecting corporate information were less successful
  - This relates to vendors tuning products to catch standard PII and PHI versus corporate information that varies greatly from company to company

Conclusions

- DLP is the protection of personally identifiable information (PII), protected health information (PHI) and confidential information
- The best approach is a risk-based approach
- Haphazard implementation is not much better than no implementation
- DLP is not just technology, it requires people (training and ownership) and process (continual improvement)
- Highest success is with implementation of multiple technologies
- Vendor support is a critical success factor

nemertes
RESEARCH

Thank You!

John E. Burke
Principal Research Analyst
john.burke@nemertes.com