CONSOLIDATION OF CYBER SECURITY SOLUTIONS

Lt Col Ashwin Yakkundi

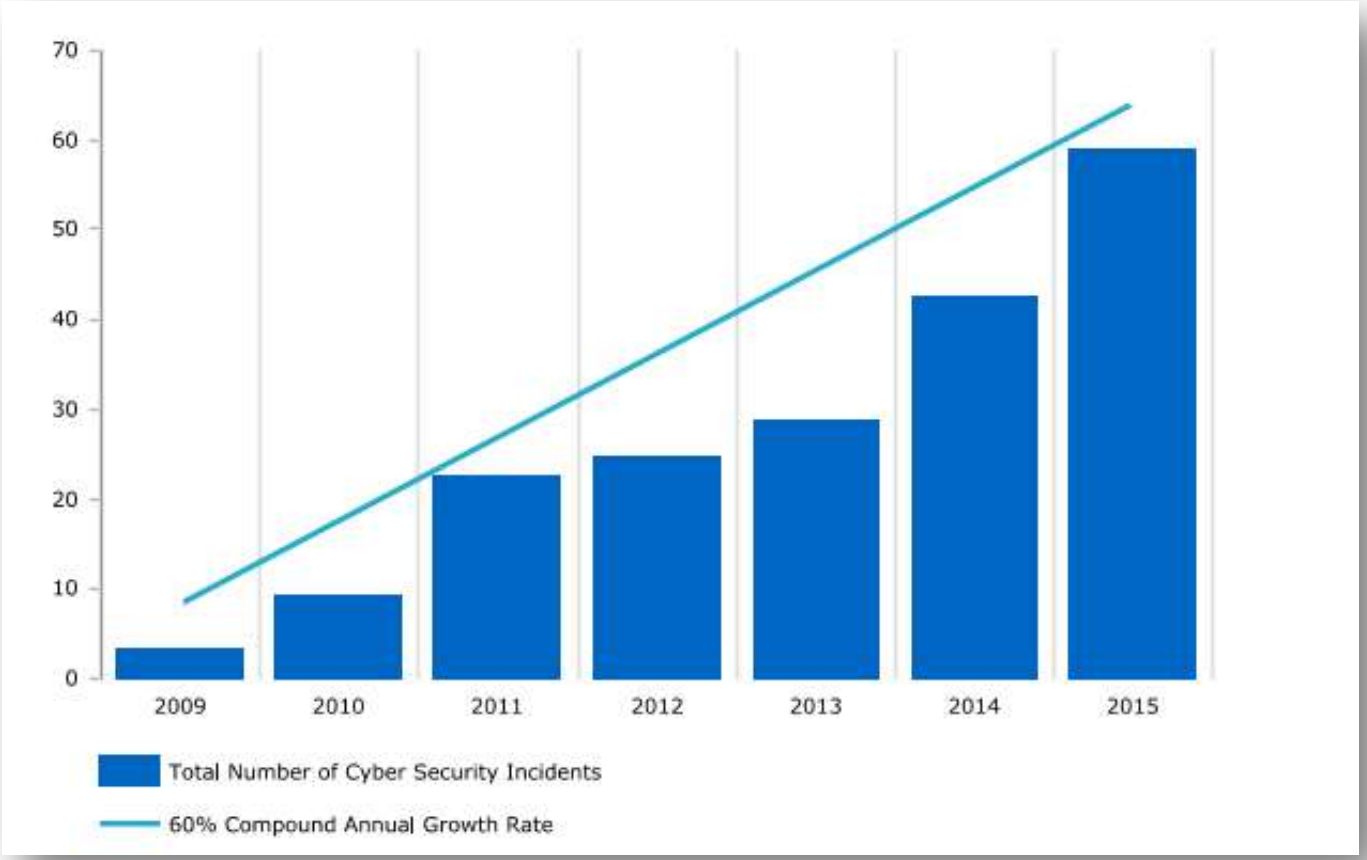
Background

- Security is not one device solution
- Layered Approach
  - Defence in depth
- Classification according to layers
  - Layers 1 to 7
- Classification according to functions
  - Network Security
  - Host Security
  - Access Control
  - Data Security
  - Security Operations

Consolidation of Cyber Security Solutions

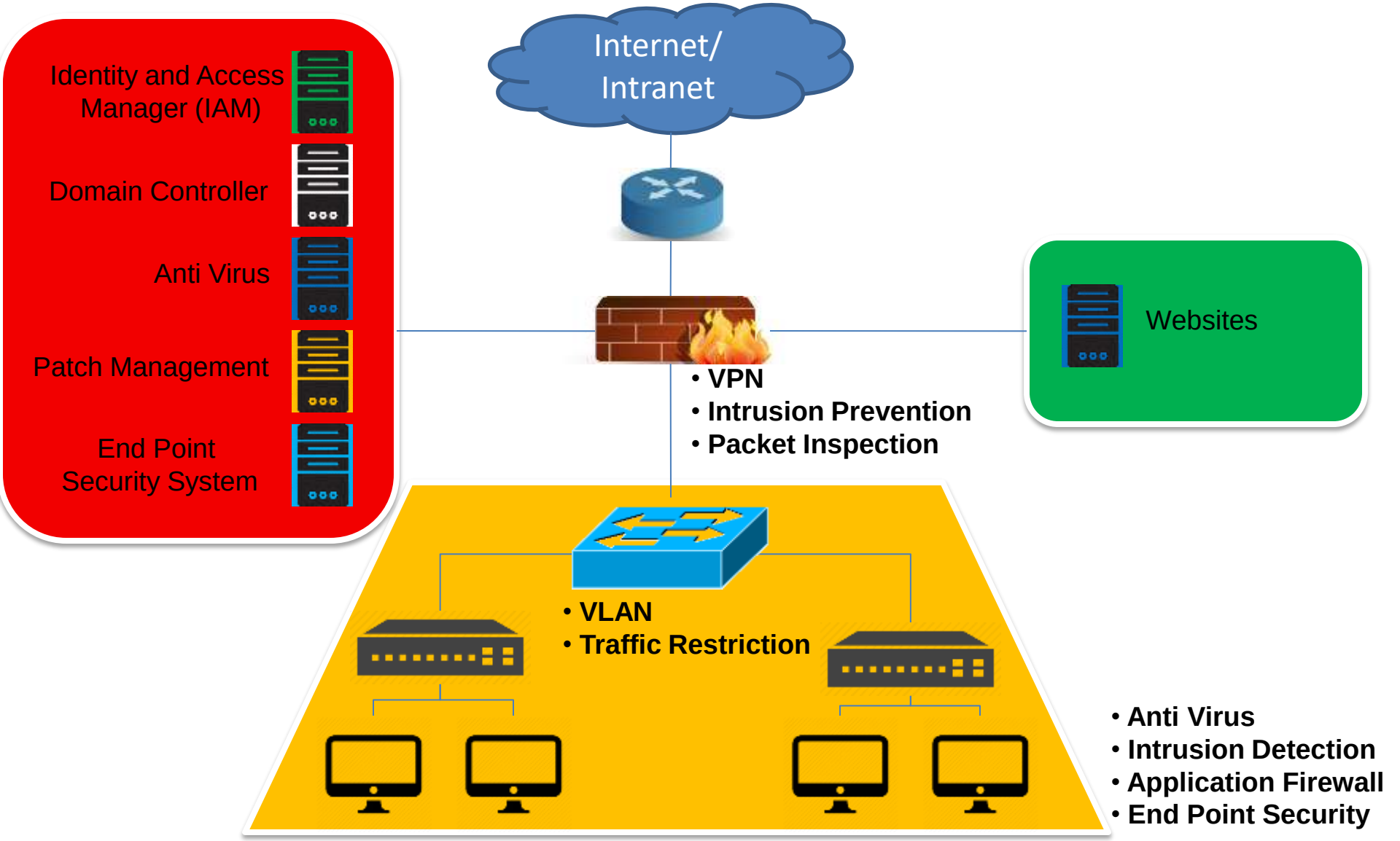
Source: https://blogs.cisco.com/security/less-is-more-fewer-cybersecurity-vendors-yield-more-effective-security

Consolidation of Cyber Security Solutions

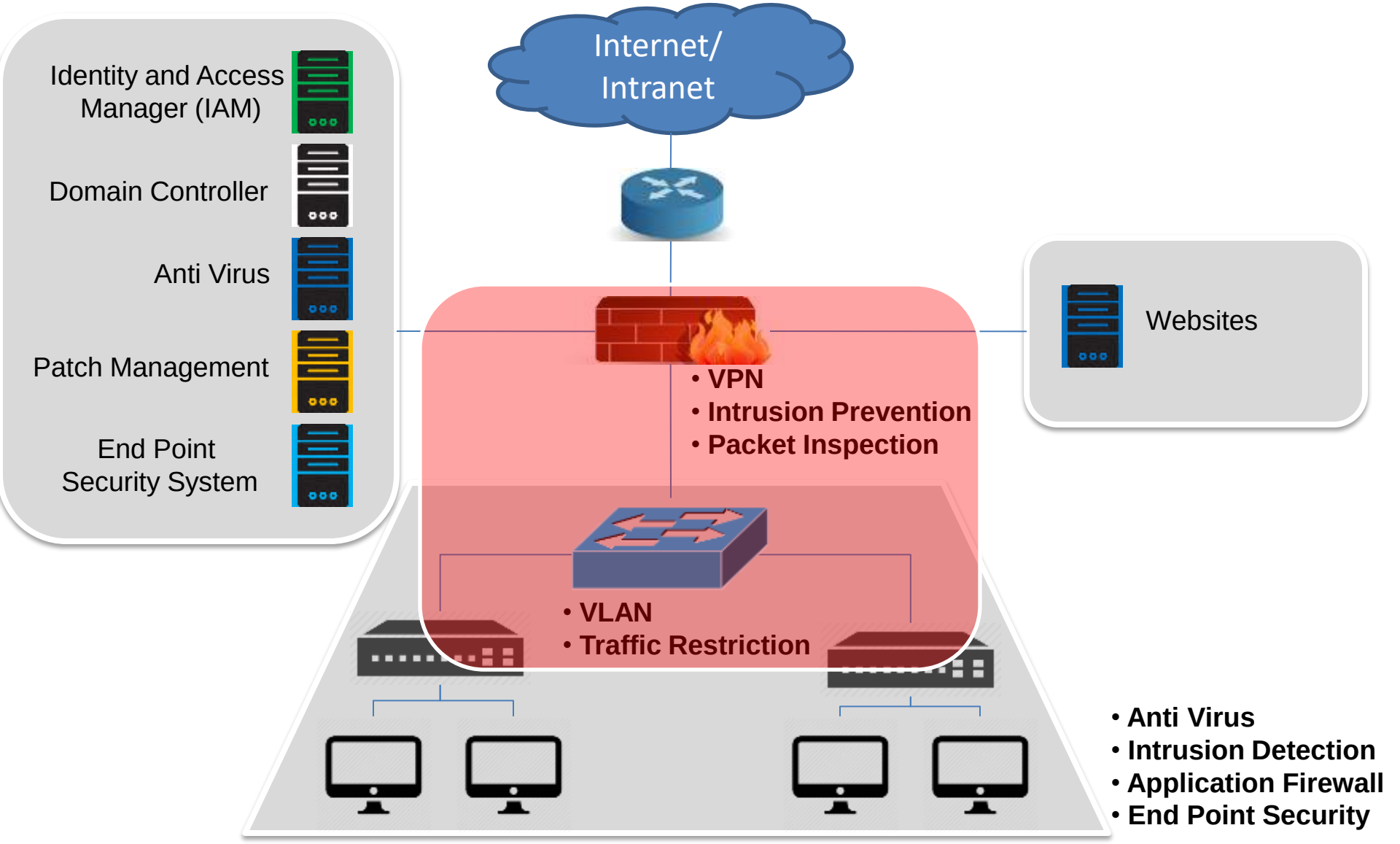


Source: https://www.morganstanley.com/ideas/cybersecurity-needs-new-paradigm

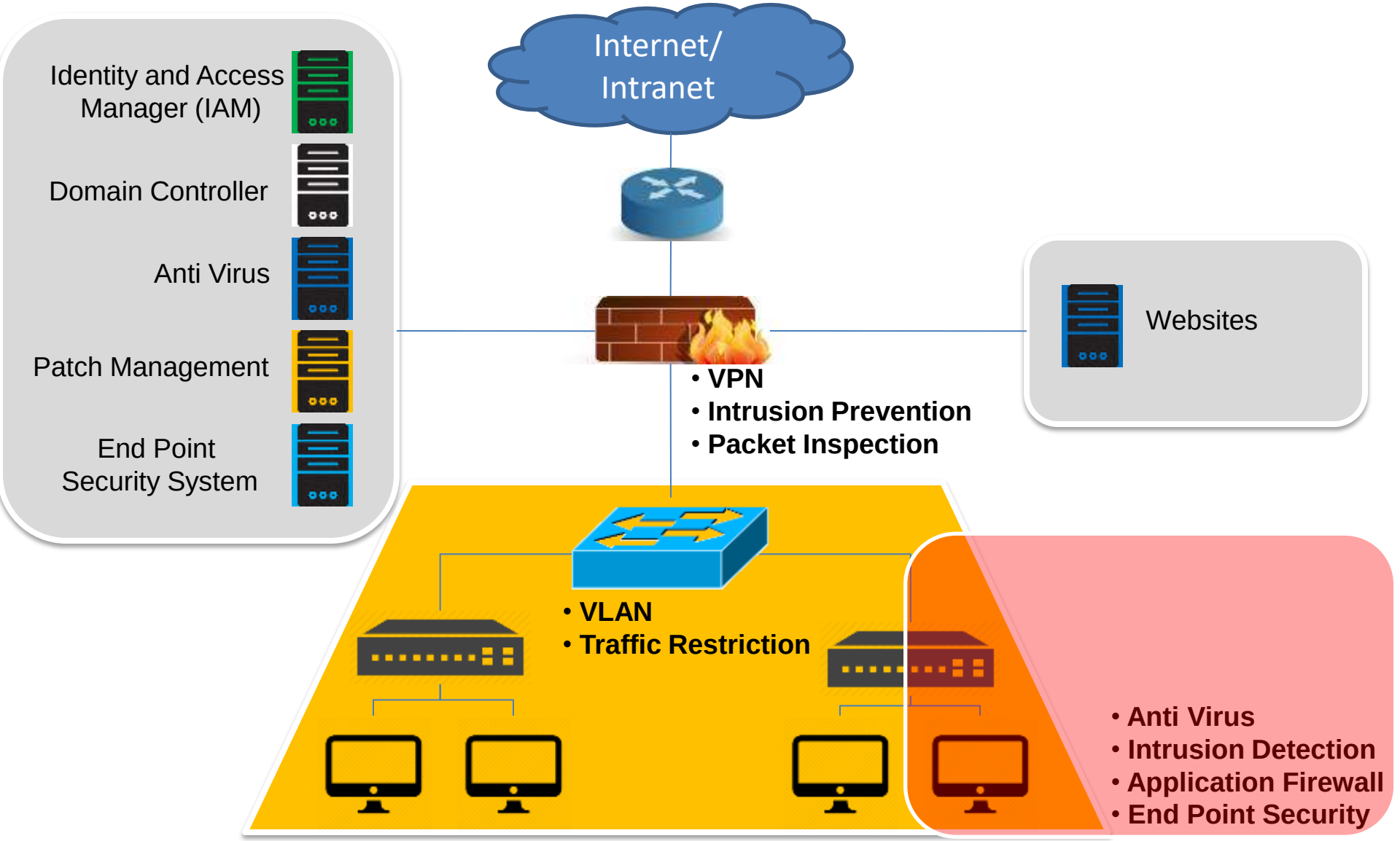
Typical Security Setup



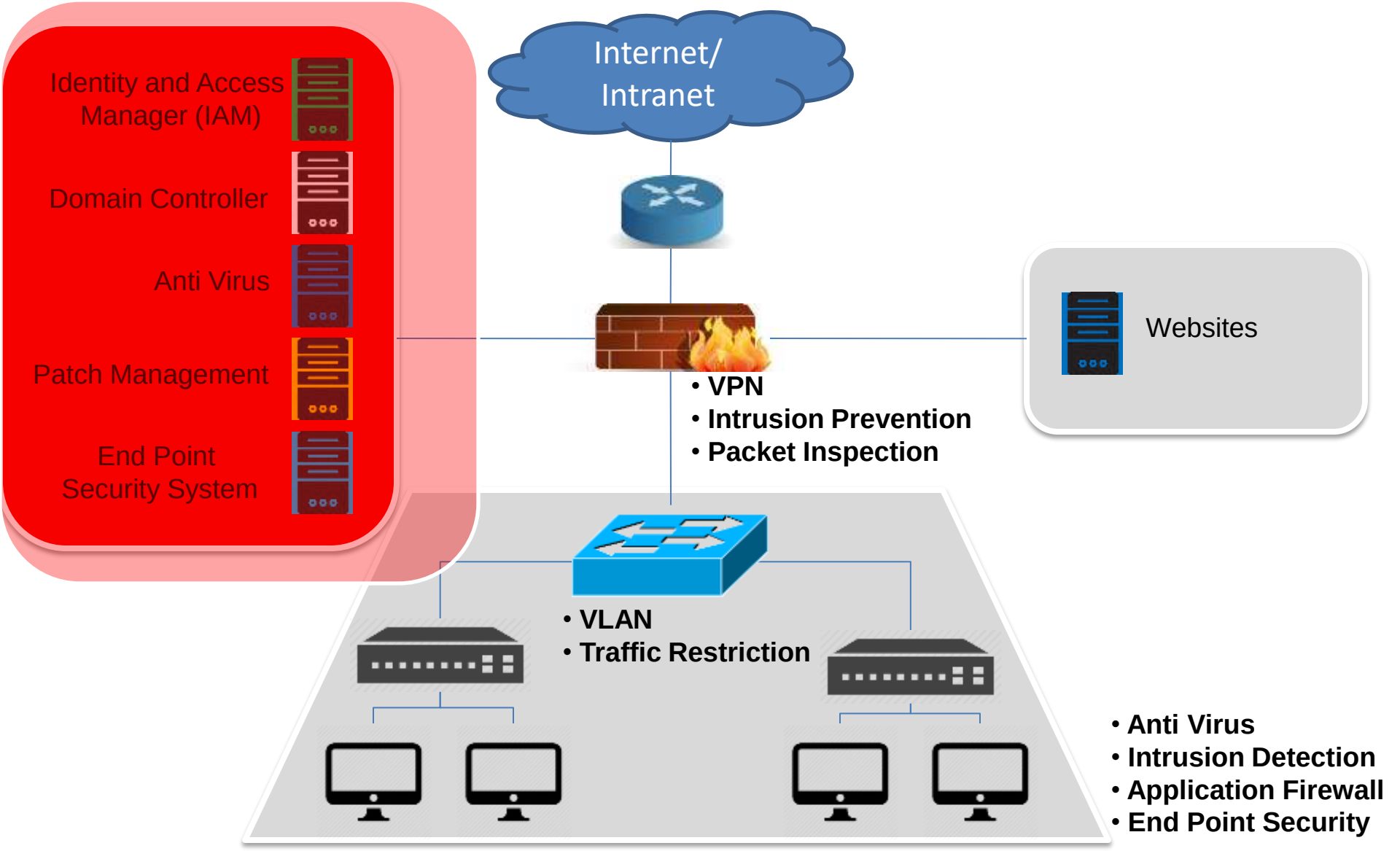
Typical Security Setup



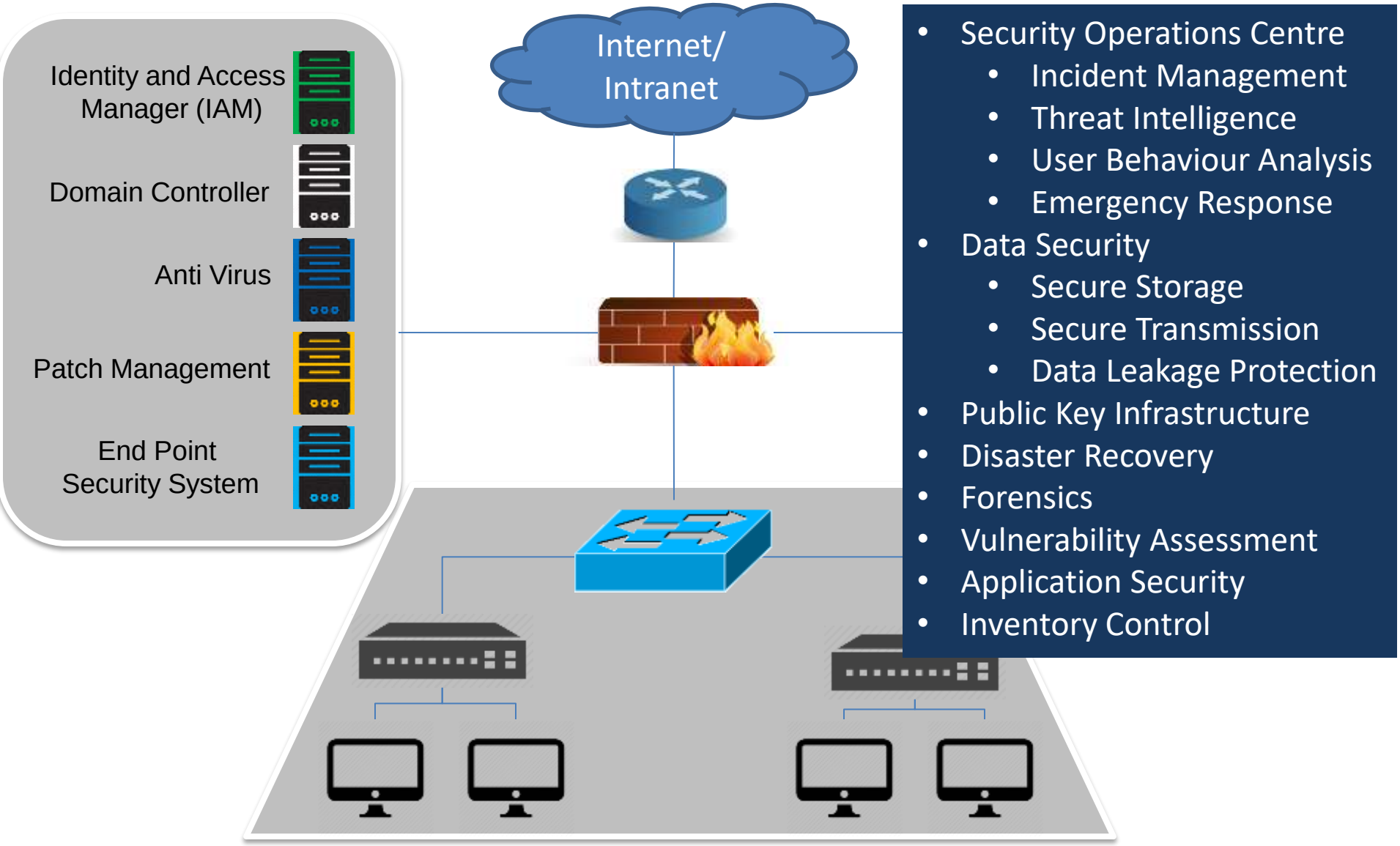
Typical Security Setup



Typical Security Setup

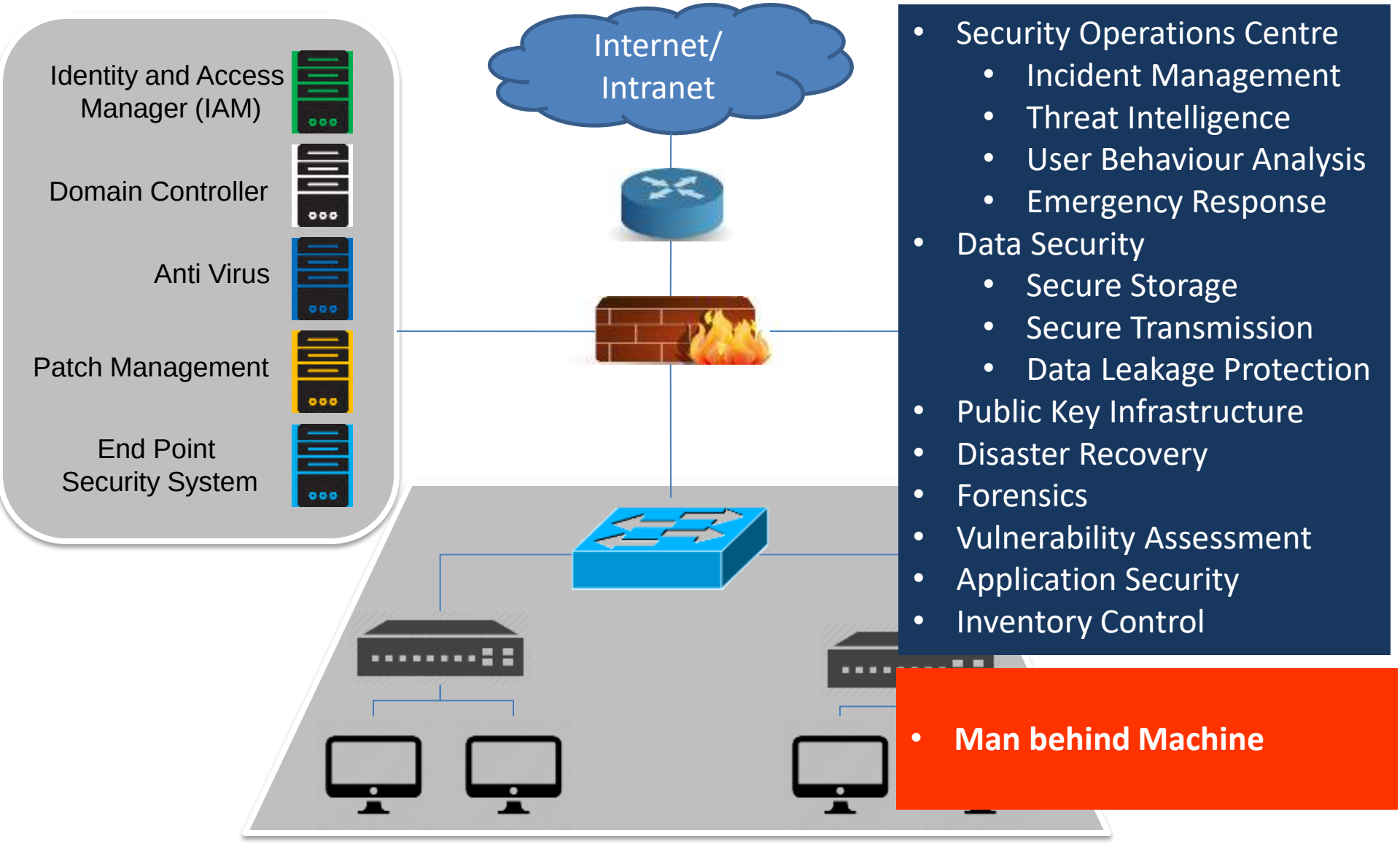


Typical Security Setup



- Security Operations Centre
  - Incident Management
  - Threat Intelligence
  - User Behaviour Analysis
  - Emergency Response
- Data Security
  - Secure Storage
  - Secure Transmission
  - Data Leakage Protection
- Public Key Infrastructure
- Disaster Recovery
- Forensics
- Vulnerability Assessment
- Application Security
- Inventory Control

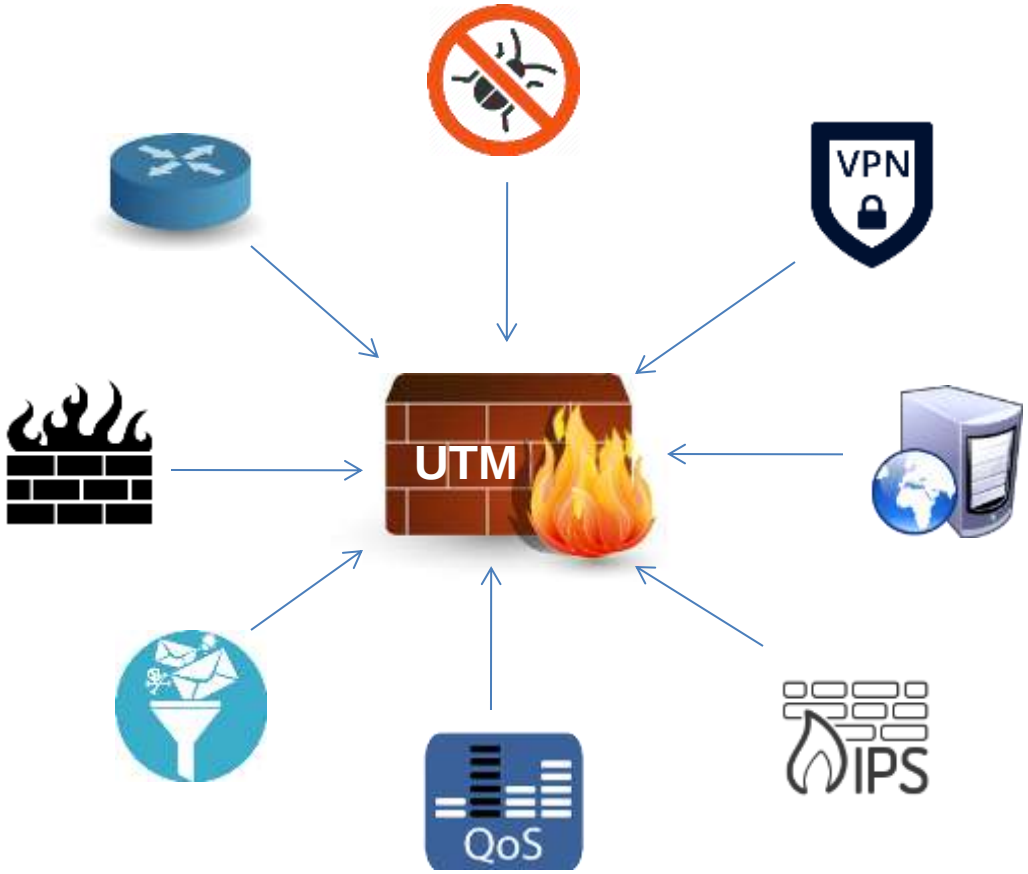
Typical Security Setup



- Security Operations Centre
  - Incident Management
  - Threat Intelligence
  - User Behaviour Analysis
  - Emergency Response
- Data Security
  - Secure Storage
  - Secure Transmission
  - Data Leakage Protection
- Public Key Infrastructure
- Disaster Recovery
- Forensics
- Vulnerability Assessment
- Application Security
- Inventory Control

- **Man behind Machine**

Unified Threat Management



- Protection from network threats
- Firewall/ IDS/ IPS/ NGFW/ Layer-7 FW
- Functions
  - Router
  - Gateway Anti Virus
  - VPN
  - Web Security
  - Intrusion Prevention
  - QoS Management
  - Content Filtering
  - Firewall

End Point Security System

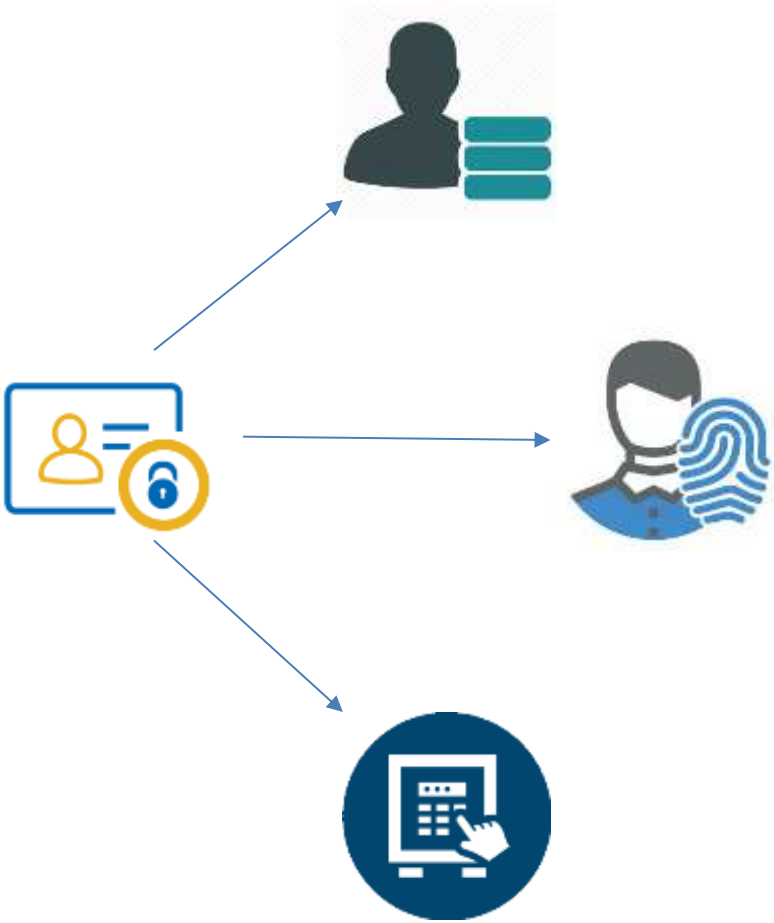
- Protection of end devices from threats and ensuring compliance.
- Host Anti Virus/ NAC
- Functions
  - Reporting
  - Network Access Control
  - Inventory Control
  - Patch Management
  - Intrusion Prevention
  - Anti Virus
  - Audit and Compliance Enforcement
  - Application Whitelisting

Network Access Control

- Attempts to unify endpoint security technology
- Functions
  - User Repository
  - User Authentication
  - Authorisation and Access Control
  - Audit Compliance
  - Policy Enforcement
  - End Point Security

Does an organisation require both EPSS ans NAC?

Identity and Access Management (IAM)



- Enables the right individuals to access the right resources at the right times and for the right reasons
- Functions
  - Central User Repository
  - Management of Users and Roles
  - User Authentication
  - Authorisation and Access Control

- **Domain Controller?**

Need for Consolidation

- Adding layers/ devices does not always add to security
  - Duplicate Functionalities
- Too many vendors, too many solutions
- Conflicting Policies/ Functionalities
- Reduced Performance
- Operational Complexities
- Non Availability of Skill Sets
- Cost Implications
- Integration Problems

Benefits Accrued

- Simpler Management
- Greater Visibility
- Eliminating Conflicting Policies/ Functionalities
- Reduced Operating Costs
- Faster Response to Threats
- Reduced Latency
- Template?
- Need for Better Security not More Security

Consolidation : Way Forward

- Identify Solutions with Overlapping Functions
- Less Vendors, Less Solutions
- Less Solutions, Better Trained Manpower
- Focus on Better Implementation

Any Questions?