

# Defense in Depth Approach to Securing Federal Computer Networks

Norman whitepaper, May 2011



## Contents

Introduction.....	3
What Is Defense in Depth?.....	3
Defense in Depth in Federal Computer Networks .....	4
Network Level Security.....	4
Endpoint Level Security .....	6
Anti-virus Endpoint Protection is Not Enough .....	7
Conclusion .....	8
About Norman.....	8
Further Information.....	8

## Introduction

Computer viruses and malware are a serious threat to our national security - new viruses appear daily, ever more creative types of malware are regularly created and released, and 'blended threats' are becoming increasingly difficult to detect and remove. Cybercrime has become a serious threat to the Federal government; in fact, the FBI has identified the capability to "inflict damage or death, illicit acquisition of assets, and unauthorized access to privileged military, intelligence and economic information" as most significant cyber threats facing the United States today.<sup>1</sup>

Historically, Federal agencies were able to adequately protect themselves from cyber attack by installing intrusion prevention systems on the network perimeter and anti-virus software on each network server and workstation. Unfortunately, the magnitude and complexity of today's malware renders this strategy inadequate. A more sophisticated 'defense in depth' strategy is required.

## What Is Defense in Depth?

'Defense in depth' is the principle of using a layered approach to network security to provide the best possible protection for a computer network. The defense in depth security approach was originally conceived by the National Security Agency (NSA), and it was developed from a military strategy meant to delay the advance of an attacker long enough for an appropriate defense to be implemented.<sup>2</sup>

Defense in depth calls for protection mechanisms, procedures and policies that increase the dependability of an IT system. Multiple layers of defense prevent espionage and direct attacks against critical systems. Defense in depth measures not only prevent security breaches; they also buy an organization time to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach.

---

<sup>1</sup> Gordon M. Snow, the Assistant Director for Cyber Division, Federal Bureau of Investigation, appearing before Senate Subcommittee on Crime and Terrorism, 4/26/2011.

<sup>2</sup> For more information on the NSA's defense in depth approach, see:  
<http://www.nsa.gov/ia/files/support/defenseindepth.pdf>

## Defense in Depth in Federal Computer Networks

The basic premise of defense in depth is to use a layered approach to network security - deploy one or more layers of protection at network boundaries (firewalls, anti-virus/malware appliances, and intrusion prevention devices), and additional layers of protection at the individual computer workstations or endpoints. This defense strategy is most effective when using multiple UNIQUE defense mechanisms – such as using multiple vendor solutions for anti-virus control. Any gaps in one vendor’s security solution are addressed by the second vendor’s solution. This approach leverages multiple layers of defense to augment and extend protection against cyber threats.

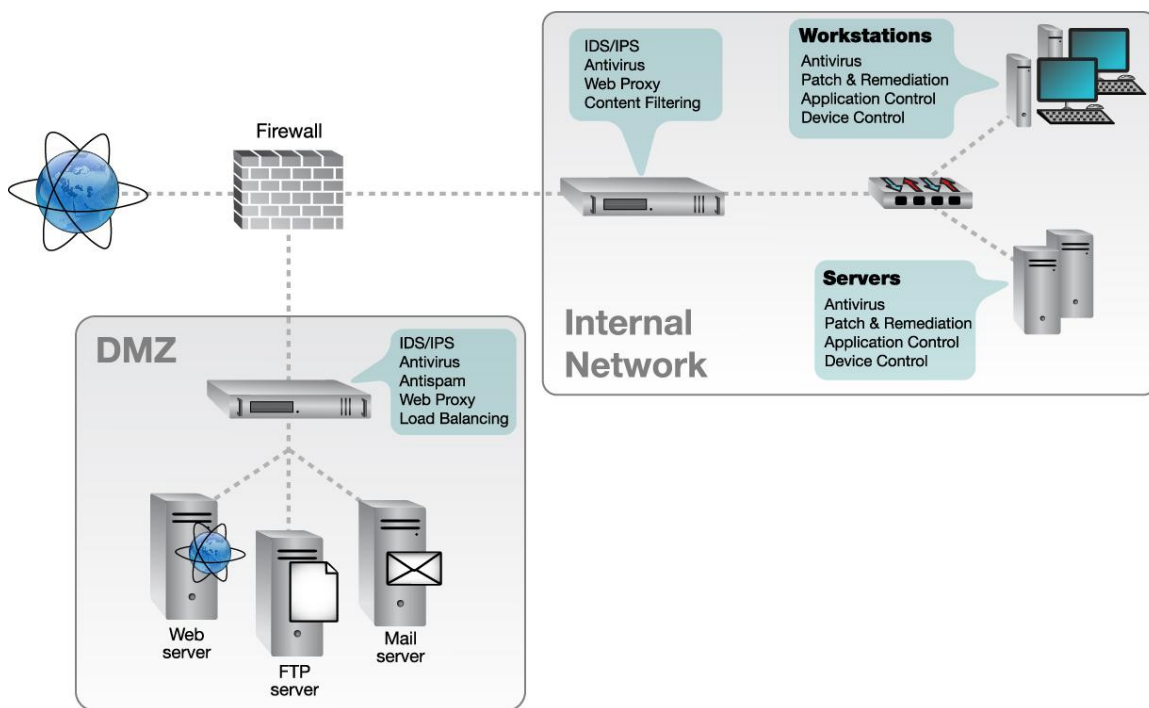


Figure 1 - Layered Approach to Network Security - Protection applied at network and endpoint layers

## Network Level Security

The first level of security to consider when implementing a defense in depth strategy is network level security. Proper attention to security at the network level will provide benefits to all downstream resources. For example, use of a network protection appliance at the network switch in conjunction with a traditional anti-virus solution at the network endpoints adds up to 38% additional anti-malware protection vs. utilizing anti-virus endpoint protection alone.<sup>3</sup>

- *Network Perimeter* - The network perimeter or edge is where Internet traffic enters and exits the agency's network(s). Various types of protection can be deployed,

<sup>3</sup> NSSLABs, Norman Network Protection (NNP) Network Anti-Malware Assessment: Q2 2010

including malware protection, spam filtering, content filtering, network firewalls, and intrusion detection and prevention.

The network perimeter is often protected by Unified Threat Management (UTM) technology. This solution is typically deployed as a network appliance, and it combines multiple security functions into a single solution with a unified management interface. These devices are especially valuable at the edge of the internal network where most external 'brute force' attacks are going to occur.

UTM solutions are a critical component of network level security, and they need to be implemented carefully. For example, network firewalls must be configured so that they do not allow unnecessary protocols to pass through to the internal network, or the perimeter of the agency's network will be open to attack through open firewall ports. Care should also be taken when using a UTM's anti-malware capabilities - implementing so many security functions can compromise throughput, especially when the device's anti-virus and malware analysis is file-based and proxy-based. Reduced throughput will cause network congestion, slow delivery of email, and slow responsiveness when accessing Internet resources. In these cases, security officers often deploy dedicated anti-virus devices to offload some of the processing to dedicated hardware.

Additionally, the anti-virus analysis of many UTMs is applied only to Internet-based protocols like http, ftp, and smtp. Some dedicated anti-malware solutions also analyze Windows-based protocols like CIFS and SMB, which represent a significant vector for both internal and external malware attacks.

In some cases security officers may choose to deploy an anti-malware appliance from a different security vendor in-line with the UTM to provide a second analysis vector on incoming data packets - this is another element of a defense in depth security strategy.

- *Segmented Networks* - Large internal networks are often organized into groups of smaller networks. This type of network topology reduces congestion and improves network performance by reducing the amount of traffic flowing through any one network segment.

Segmented networks also provide a high level of security - broadcast traffic is contained within each local network, and network segments can be quickly isolated in the event of a security breach. In a segmented network topology, each segment can be protected with a dedicated network level security appliance to prevent viruses and malware from crossing network boundaries.

## Endpoint Level Security

An effective security infrastructure must protect all network endpoints (servers, workstations, et al.) from cyber attack. The accepted way to protect these network resources is by installing anti-virus software and enabling a firewall at each endpoint.

Anti-virus software is used to prevent, detect, and remove malware (including computer viruses, computer worms, trojan horses, spyware and adware). There are a number of strategies that can be employed by an anti-virus solution:

- *Signature-based detection* - This strategy involves searching for known patterns of data within executable code. These patterns are regularly updated by the anti-virus company's research team. It is critical that all endpoints with anti-virus software receive updated signature files regularly. These signature files serve as the first line of defense when identifying malware.
- *Heuristic detection* - This strategy is used to identify new malware for which no signature is known. The anti-virus software identifies new viruses or variants of existing viruses by looking for patterns that are similar to those of known malicious code, or slight variations of such code.
- *Sandbox detection and analysis* - This strategy executes unknown files in a protected environment and analyzes the results of that execution to see if the files trigger any malicious actions in the host environment. Sandbox solutions can identify new and undiscovered malicious code that may pass through signature-based and heuristic detection methods undetected, and stop the code before it damages computer networks and compromises confidential data.

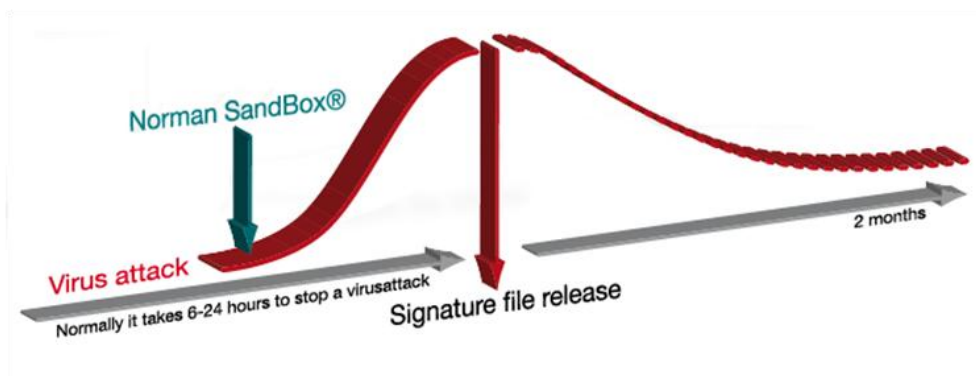


Figure 2 - SandBox Value - Malicious code identified through behavior profile before a signature file can be created

All anti-virus solutions will provide some level of protection for the network endpoints, but the best anti-virus solutions use a combination of all three techniques to protect endpoints from infection. Security personnel should periodically evaluate their anti-virus solutions to ensure that they are leveraging a solution with multiple layers of defense.

## Anti-virus Endpoint Protection is Not Enough

Anti-virus software is a critical component of endpoint security, and security personnel must ensure that the software is installed on every server and workstation on their networks. Endpoints with outdated virus definition files are a security risk, so procedures should be put in place to ensure that all endpoints are regularly updated with new virus definition files. Once a comprehensive anti-virus plan has been deployed, a more comprehensive strategy of endpoint security should be considered – one that ensures all endpoints are kept secure through application of regular vulnerability patches.

- *Patch and Remediation Software* - Over 90% of cyber attacks exploit known security flaws for which remediation is available<sup>4</sup>. In order for network endpoints to be completely secure, security personnel must also know what software is installed and operating on each endpoint. They must further ensure that the software and operating systems of every endpoint are regularly patched to eliminate attack vectors which could be utilized by cyber criminals to compromise the resource.

There are a number of security solutions available to assist security personnel in effectively managing patches and application vulnerabilities. Norman Patch and Remediation is one such solution; it streamlines patch management across heterogeneous environments, provides visibility into real-time patch status and overall security posture, and reduces operational costs by centralizing operating system and application patching and remediation activities.

- *Application and Device Control Software* - One aspect of endpoint security that is often ignored is application usage. By implementing a "whitelist" approach to managing application usage, security personnel can define which devices and applications are permitted on the network through user and/or machine-specific policy rules. Execution of unknown or malicious code is prevented because only authorized applications are allowed to run on agency laptops, PCs, and mission critical servers. Desktop and server management are improved by eliminating the unnecessary support calls and performance issues that come with managing unauthorized and illegal software.

A comprehensive application control solution should automatically determine what applications are in use throughout the network endpoints, enforce application usage policies across the entire network, and automatically log network events related to endpoint security policy for compliance reporting. Such a solution should implement endpoint agents that are tamper-proof and protected against unauthorized removal.

---

<sup>4</sup> Gartner Research report, May 2002.

Device control solutions protect networks from internal threats like data theft by enforcing which removable media are allowed in the agency network and controlling the data that is copied to and from the internal network through policy-enforced encryption. These solutions should also log all data transfers for security and compliance reporting purposes.

## Conclusion

A defense in depth approach to network security will provide the most comprehensive protection against malware threats and other forms of cybercrime. Security architectures with multiple layers of protection from multiple vendors provide the best protection, especially when deployed at multiple levels in the network. Likewise, a multi-layer endpoint management strategy with anti-virus, patch, remediation, and application and device controls will provide the most comprehensive protection at network endpoints.

Security professionals are encouraged to review their agency's security implementations periodically to identify areas of vulnerability and implement 'defense in depth' network strategies where appropriate to ensure that their agency's network resources are adequately protected.

## About Norman

Norman is a world leader and pioneer in proactive IT security solutions and forensic malware analysis tools. Norman can offer the depth and breadth of solutions to assist agencies in enhancing their security defenses without risking vendor lock-in. Norman's comprehensive portfolio includes patch and remediation, device control, application control, network security, and proactive malware detection (endpoint, server, mail server or gateway) as well as advanced malware analysis tools.

Norman is recognized as a leading authority in proactive anti-malware technology, with respected security companies including MessageLabs (Symantec), eEye Digital Security and Microsoft among others utilizing Norman's technology to help protect their customers.

## Further Information

For further information and advice on Defense in Depth please contact:

### **Norman Data Defense Systems (US)**

9302 Lee Highway, Suite 950A  
Fairfax, VA 22031

Tel: 703-279-6647

E-mail: [sales.us@norman.com](mailto:sales.us@norman.com)



[www.norman.com](http://www.norman.com)