

Lessons Learned: Defense in Depth Security Strategies for Education Networks

Norman whitepaper, May 2011

A decorative graphic at the bottom of the page consists of a dense field of teal circles of varying sizes, arranged in a pattern that resembles a network or a data visualization. The circles are more concentrated in the lower right and fade out towards the upper left. There are also several teal hexagons scattered throughout the field, some overlapping the circles.

Contents

Introduction.....	3
The Cost of Malware Infections and Data Breaches	3
Defense in Depth and Education Networks	4
Network Level Security.....	5
Endpoint Level Security	7
Anti-virus Endpoint Protection is Not Enough	8
Conclusion	10
About Norman.....	11
Further Information.....	11

Introduction

Computer viruses and data breaches pose a serious threat to primary, secondary, and post-secondary educational institutions throughout the country. The types of information available on school networks, coupled with extensive use of social media and peer to peer networking among students makes these networks a favorite target for cyber criminals. The situation is already a significant problem for the nation's public schools, and it is getting worse every year - in 2009, more than half [55 percent] of all U.S. school districts reported a security breach such as unauthorized user access, hacking or viruses, up substantially from 2008.¹

The situation is even more dire at this country's colleges and universities; there were 14 reported breaches amongst higher education institutions in the first three months of 2011 alone, including one at the University of South Carolina where 31,000 records were compromised.²

Over 200 colleges and universities have been compromised to date. These institutions have lost control of more than 22 million data and information files. These files contain more than just student and faculty information - they often include information on contractors, prospective applicants, parents and even donors. Since most schools' financial, administrative, research, and clinical systems are accessible through a campus network, that information can include social security numbers, credit card data, health records, student records, and employment-related records.³

The Cost of Malware Infections and Data Breaches

There are many potential economic impacts associated with virus infections and data breaches in school networks.

For example, when malware affects computers in a school network, there are costs associated with faculty members who are impacted by the malware, costs related to downtime for the computers that are infected, and IT or service costs associated with removing the malware from computers that have been infected. If many computers in a network become infected, the costs can quickly multiply into thousands of dollars to address a single incident.

When malware, student tampering, or outside hacker activities result in a data breach, the costs can be significantly higher. Consider the financial damages related to faculty members and students whose information has been compromised; in many cases the educational institution bears the cost of securing credit protection for compromised individuals. A data breach investigation can easily cost millions of dollars, as in the Ohio State University data

¹ Survey of 400 K-12th-grade IT managers, CDW Government, May 18, 2009

² eWeek, Friday Apr 1st, 2011, Fahmida Y. Rashid

³ "The College Cyber Security Tightrope", SecurityWeek, Apr 28th, 2011, Rod Rasmussen

breach in December 2010, where the social security numbers and other personal information for 760,000 current and former students and faculty members was compromised by hackers who were able to break into a campus server. The breach cost the university an estimated \$4 million in expenses related to forensic investigation and credit protection services for those individuals that were affected by the incident.

Data breaches can also harm a school's reputation. The University of Hawaii had so many data breaches over the past five years that a national watchdog group gave the university a failing grade for inadequate protection of online student and faculty information, and prompted Phillippe Gross (a former student and faculty member) to file a class action lawsuit against the university.⁴

Primary and secondary schools are also at risk - Churchill High School in Maryland, Brooklyn High School in New York, the Seattle Public School system, and many other high schools around the country have seen their names in the newspapers and television over the past year after data breaches occurred in those schools.

Given the costs associated with malware infections and data breaches, educational institutions must develop security policies that will protect their faculty and students from cybercrime and protect their reputations. Due to the magnitude and complexity of today's malware and attacks, traditional defenses like intrusion prevention systems, firewalls, and anti-virus software are no longer an adequate defense against cybercrime. A more sophisticated 'defense in depth' strategy is now required.

Defense in Depth and Education Networks

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.

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, antivirus/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 at the network level. 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.

⁴ Gross et al. v University of Hawai'i et al., <http://www.uhdatabreachlawsuit.com/>

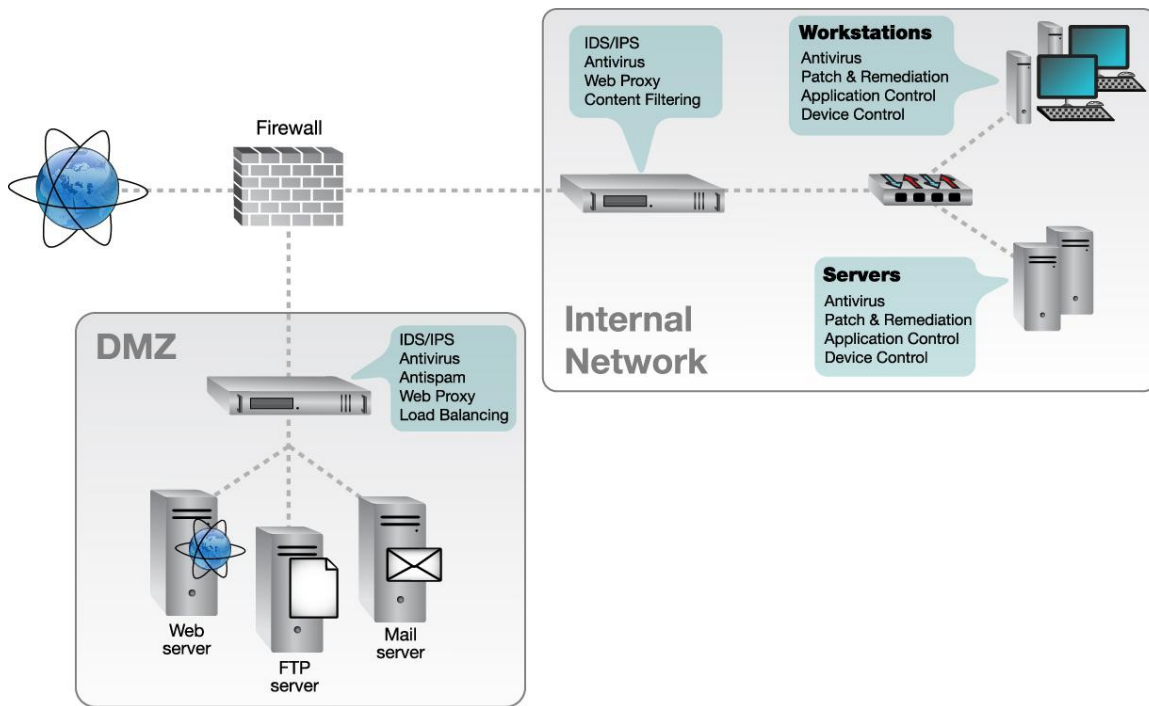


Figure 1 - Layered Approach to Network Security - Protection applied at network and endpoint layers

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.⁵

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

⁵ NSSLABs, Norman Network Protection (NNP) Network Anti-Malware Assessment: Q2 2010

they do not allow unnecessary protocols to pass through to the internal network, or the perimeter of the school'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. 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, especially in school networks where students often share files stored in Windows file systems.

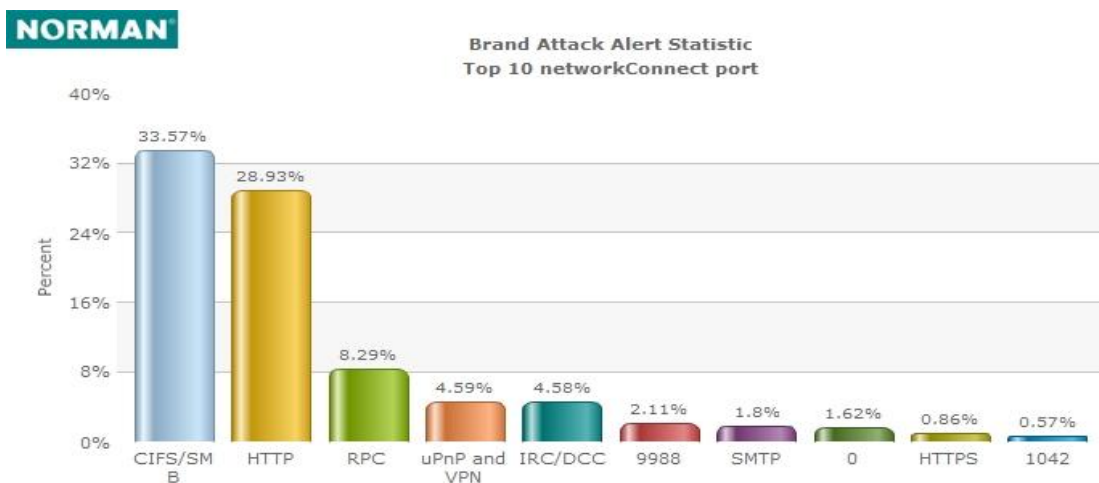


Figure 2 - Malware Attacks by Protocol - Largely CIFS/SMB, HTTP, and RPC

In some cases, security personnel may also 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 case of a security breach.

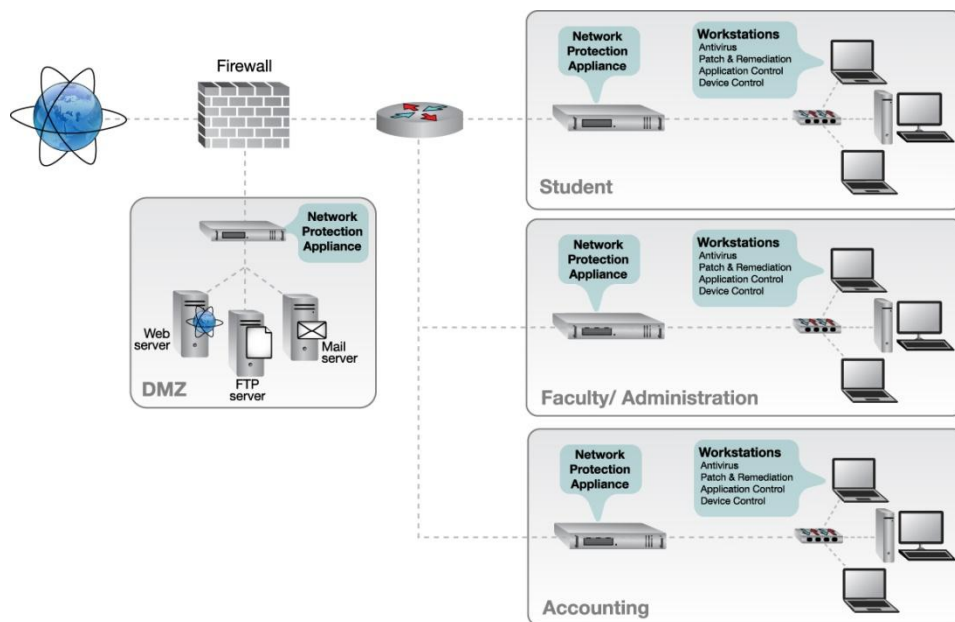


Figure 3 - Network Subnets in Educational Institution

Segmented networks are especially useful for securing school networks. In primary and secondary schools, student computer laboratories can be very difficult to protect - peer to peer applications, instant messaging, and file sharing through USB devices are typical vectors for malware contamination. These computer labs can be isolated into their own subnet, confining student computers and activities to a network that is separate from staff workstations and servers. In college and university environments, financial, administrative, research, and clinical systems can be organized into a separate departmental subnet. The advantage of this type of network topology is that each segment can be protected with a dedicated network level security appliance to prevent viruses and malware from crossing network boundaries, and subnets can be physically isolated in the event of a serious malware infection.

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 antivirus

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 antivirus 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.

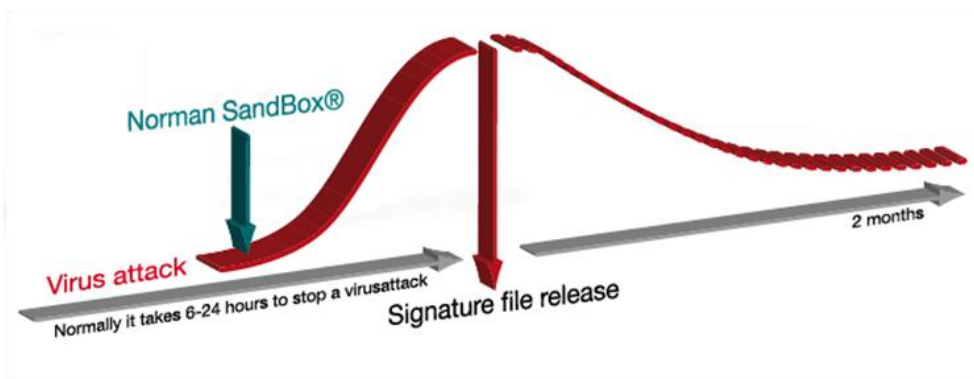


Figure 4 - SandBox Value - Malicious code identified through behavior profile before a signature file can be created

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 available⁶. For example, for months the Conficker worm continued to spread to millions of computers worldwide through a security hole in Windows Server Service, despite Microsoft publishing a patch for this vulnerability.

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 cybercriminals to compromise the resource. When properly implemented, patch and remediation solutions ensure that system and software vulnerabilities are patched before they can be exploited.

A comprehensive patch and remediation solution should have vulnerability auditing capabilities and remediation, and it should support all major operating systems (including Microsoft Windows, Linux, MacOS, Sun Solaris and HP) so that risk can be managed for all systems from a single operating console. The solution should have the ability to patch operating systems and popular applications from vendors like Microsoft, Adobe, and Apple, and also patch custom applications through a straightforward and intuitive interface. 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 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 applications are permitted on the school's 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 student and faculty workstations and on mission critical servers. Desktop and server management are improved by eliminating the support 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 your endpoint security policy for compliance reporting. Such a solution should

⁶ Gartner Research report, May 2002.

implement endpoint agents that are tamper-proof and protected against unauthorized removal.

- *Device Control Software* - Device control solutions are a critical component of a comprehensive defense in depth approach to network security. This software protects networks from internal threats like data theft by enforcing which removable media are allowed in the school's network, and controlling the data that is copied to and from the network through policy-enforced encryption. This ensures that sensitive information is unreadable if it falls into the wrong hands.

Device control solutions should provide a detailed audit trail of all device mounts, tracking data that is copied to and from removable devices and by controlling what data is allowed to be copied to a device at the file level. As with application control solutions, all data transfers must be logged for security and compliance reporting, and endpoint agents must be tamper-proof and protected against unauthorized removal.

Conclusion

A defense in depth approach to network security will provide the most comprehensive protection against malware threats and other forms of cyber-crime. 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 comprehensive protection at network endpoints.

A defense in depth architecture will also provide security teams with many of the reports necessary to demonstrate compliance with the regulations facing schools today, including Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), the Fair and Accurate Credit Transactions Act (FACTA), and other federal and state laws and regulations that penalize institutions when they do not adequately protect the personal data on their networks.

Security professionals are encouraged to review their school's security implementations periodically to identify areas of vulnerability and implement 'defense in depth' network strategies where appropriate to ensure that their school'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 and their partners can offer the depth and breadth of solutions to assist educational institutions 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



www.norman.com