**Critical Control 5: Malware Defenses**

[20 Critical Security Controls](http://www.sans.org/critical-security-controls/) | [Guidelines](http://www.sans.org/critical-security-controls/guidelines.php) [[previous control](http://www.sans.org/critical-security-controls/control/4.php)previous control](http://www.sans.org/critical-security-controls/control/4.php)[next control[next control](http://www.sans.org/critical-security-controls/control/6.php)](http://www.sans.org/critical-security-controls/control/6.php)

*The processes and tools used to detect/prevent/correct installation and execution of malicious software on all devices.*

**How do attackers exploit the absence of this control?**

Malicious software is an integral and dangerous aspect of Internet threats, targeting end-users and organizations via web browsing, e-mail attachments, mobile devices, the cloud, and other vectors. Malicious code may tamper with the system's contents, capture sensitive data, and spread to other systems. Modern malware aims to avoid signature-based and behavioral detection, and may disable anti-virus tools running on the targeted system. Anti-virus and anti-spyware software, collectively referred to as anti-malware tools, help defend against these threats by attempting to detect malware and block its execution.

**How to Implement, Automate, and Measure the Effectiveness of this Control**

1. Quick wins: Employ automated tools to continuously monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers. The endpoint security solution should include zero-day protection such as network behavioral heuristics.

2. Quick wins: Employ anti-malware software and signature auto-update features or have administrators manually push updates to all machines on a daily basis. After applying an update, automated systems should verify that each system has received its signature update.

3. Quick wins: Configure laptops, workstations, and servers so that they will not auto-run content from USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, Firewire devices, external serial advanced technology attachment devices, mounted network shares, or other removable media. If the devices are not required for business use, they should be disabled.

4. Quick wins: Configure systems so that they conduct an automated anti-malware scan of removable media when it is inserted.

5. Quick wins: Scan and block all e-mail attachments entering the organization's e-mail gateway if they contain malicious code or file types unneeded for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes e-mail content filtering and web content filtering.

6. Quick wins: Apply anti-virus scanning at the Web Proxy gateway. Content filtering for file-types should be applied at the perimeter.

7. Quick wins: Deploy features and toolkits such as Data Execution Prevention (DEP) and Enhanced Mitigation Experience Toolkit (EMET), products that provide sandboxing (e.g., run browsers in a Virtual Machine), and other techniques that prevent malware exploitation.

8. Quick wins: Limit use of external devices to those that have a business need. Monitor for use and attempted use of external devices.

9. Visibility/Attribution: Block access to external e-mail systems, instant messaging services, and other social media tools.

10. Visibility/Attribution: Ensure that automated monitoring tools use behavior-based anomaly detection to complement and enhance traditional signature-based detection.

11. Visibility/Attribution: Utilize network-based anti-malware tools to analyze all inbound traffic and filter out malicious content before it arrives at the endpoint.

12. Advanced: Perform continuous monitoring on all inbound and outbound traffic. Any large transfers of data or unauthorized traffic should be flagged and, if validated as malicious, the computer should be moved to an isolated VLAN.

13. Advanced: Implement an incident response process that allows the IT support organization to supply the security team with samples of malware running undetected on corporate systems. Samples should be provided to the security vendor for "out-of-band" signature creation and deployed to the enterprise by system administrators.

14. Advanced: Utilize network-based flow analysis tools to analyze inbound and outbound traffic looking for anomalies, indicators of malware, and compromised systems.

15. Advanced: Deploy "reputation-based technologies" on all endpoint devices to cover the gap of signature-based technologies.

16. Advanced: Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.

17. Advanced: Apply proxy technology to all communication between internal network and the Internet.

**Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls**

SC-18, SC-26, SI-3 (a, b, 1, 2, 5, 6)

**Associated NSA Manageable Network Plan Milestones and Network Security Tasks**

Virus Scanners and Host Intrusion Prevention Systems (HIPS)

Personal Electronic Device (PED) Management

Network Access Protection/Control (NAP/NAC)

Security Gateways, Proxies, and Firewalls

Network Security Monitoring

**Procedures and Tools to Implement and Automate this Control**

Relying on policy and user action to keep anti-malware tools up to date has been widely discredited, as many users have not proven capable of consistently handling this task. To ensure anti-virus signatures are up to date, organizations use automation. They use the built-in administrative features of enterprise endpoint security suites to verify that anti-virus, anti-spyware, and host-based IDS features are active on every managed system. They run automated assessments daily and review the results to find and mitigate systems that have deactivated such protections, as well as systems that do not have the latest malware definitions.

Some enterprises deploy free or commercial honeypot and tarpit tools to identify attackers in their environment. Security personnel should continuously monitor honeypots and tarpits to determine whether traffic is directed to them and account logins are attempted. When they identify such events, these personnel should gather the source address from which this traffic originates and other details associated with the attack for follow-on investigation.

**Control 5 Metric:**

The system must identify any malicious software that is installed, attempted to be installed, executed, or attempted to be executed on a computer system within one hour, alerting or sending e-mail notification to a list of enterprise personnel via their centralized anti-malware console or event log system. Systems must block installation, prevent execution, or quarantine malicious software within one hour, alerting or sending e-mail when this action has occurred. Every 24 hours after that point, the system must alert or send e-mail about the status of the malicious code until such time as the threat has been completely mitigated on that system. While the one-hour timeframe represents the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid detection and malware isolation.

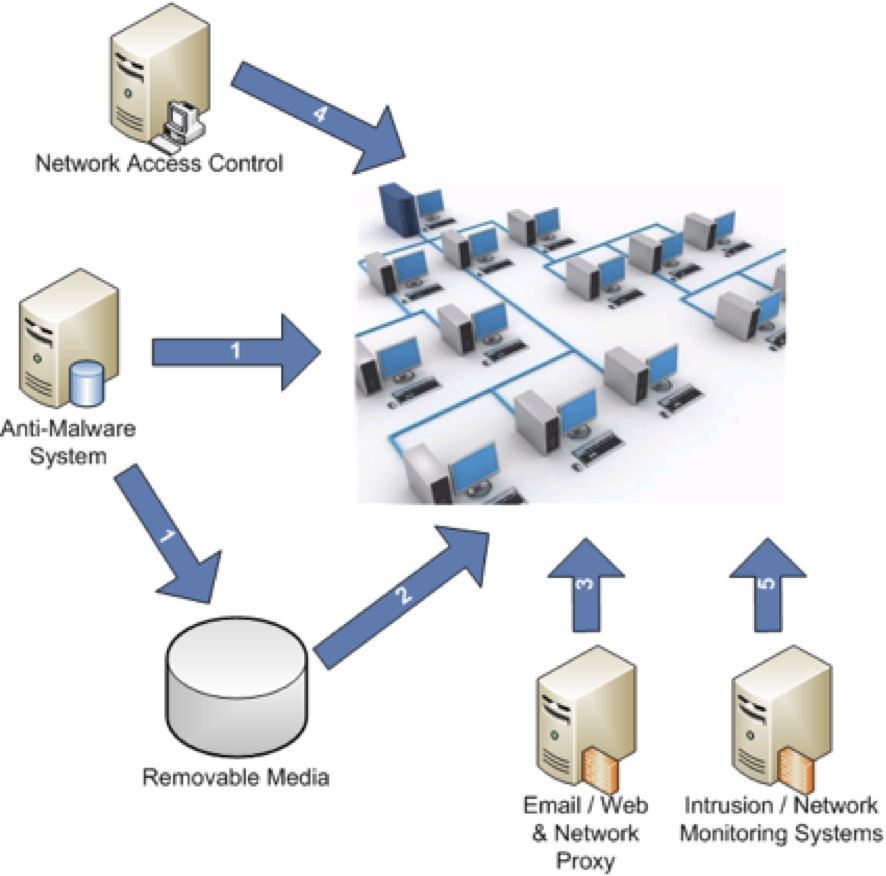
**Control 5 Test:**

To evaluate the implementation of Control 5 on a periodic basis, the evaluation team must move a benign software test program that appears to be malware (such as an EICAR file or benign hacker tools), but that is not included in the official authorized software list, to 10 systems on the network via a network share. The selection of these systems must be as random as possible and include a cross-section of the organization's systems and locations. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the benign malware within one hour. The team must also verify that the alert or e-mail indicating that the software has been blocked or quarantined is received within one hour. The evaluation team must verify that the system provides details of the location of each machine with this new test file, including information about the asset owner. The team must then verify that the file is blocked by attempting to execute or open it and verifying that it is not allowed to be accessed.

Once this test has been performed transferring the files to organization systems via removable media, the same test must be repeated, but this time transferring the benign malware to 10 systems via e-mail instead. The organization must expect the same notification results as noted with the removable media test.

**Control 5 System Entity Relationship Diagram:**

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining anti-malware systems and threat vectors such as removable media. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also delineates each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Anti-malware systems analyze production systems and removable media

Step 2: Removable media is analyzed when connected to production systems

Step 3: Email/web and network proxy devices analyze all incoming and outgoing traffic

Step 4: Network access control monitors all systems connected to the network

Step 5: Intrusion/network monitoring systems perform continuous monitoring looking for signs of malware.