WEBROOT
Smarter Cybersecurity™

20 CRITICAL SECURITY CONTROLS FOR MSPS

This list of 20 critical security controls[1] shows what measures you and your clients need to implement for an effective security posture.

Today's threats use multiple vectors to attack, from malicious email attachments to infected web ads to phishing sites. Criminals combine a range of threat technologies, deployed in numerous stages to infect computers and networks. This blended approach increases the likelihood of success, the speed of contagion, and the severity of damage.

The only way to keep your clients safe is through an ecosystem of layered security that covers any gaps or vulnerabilities across endpoint protection, application protection, network protection, and end user controls.

1. Device inventory

Determine which devices are being used, as well as where, how, and by whom.

2. Software inventory

Determine which applications are being used, as well as where, how, and by whom.

3. Secure configuration for hardware and software

Shore up all settings on mobile devices, laptops, work stations and servers.

4. Vulnerability assessment and remediation

Use automated utilities to regularly (and continuously) scan for vulnerabilities.

5. Controlled use of administrative privileges

Maintain an inventory of administrative accounts, change all default passwords, and enable 2-factor authentication.

6. Maintenance, monitoring, & analysis of audit logs

Activate audit logging and consider deploying a security information and event management (SIEM) or log analysis tool.

7. Email and web browser protections

Make sure only fully supported email clients and web browsers are in use, disable unnecessary/unauthorized plugins, and limit use of scripting languages.

8. Malware defenses

Use automated, next-gen tools to continuously monitor and protect endpoint computers, servers, and mobile devices with antivirus, antimalware, personal firewalls, etc.

9. Limitation and control of network ports, protocols, and services

Perform regular automated port scans and ensure only approved ports, protocols, and services are running.

10. Data recovery

Make sure your clients have regular, automated, encrypted backups and full system backups, and be sure to test them often.

11. Secure configuration for network devices

Check all firewalls, routers, and switches, update firmware, change default passwords, etc.

12. Boundary defense

Take and maintain an up-to-date inventory of all the network boundaries, scan for unauthorized connections, and block communications with malicious IPs.

13. Data protection

Make sure end users don't (or can't) send sensitive or critical information outside the corporate network.

14. Controlled access

Review and re-review access permissions based on the “need to know”.

15. Wireless access control

Encrypt wireless traffic, ensure all wireless access points are manageable using management tools, and configure scanning tools to detect wireless access points.

16. Account monitoring and control

Ensure all accounts have an expiration date, disable dormant accounts, and monitor attempts to access deactivated accounts.

17. Security skills assessment and training

Understand any skills shortages and implement appropriate training to fill the gaps.

18. Application software security

Ensure sure all applications are up to date, patched, hardened, and encrypted (where applicable).

19. Incident response and management

Develop incident response processes, keep up-to-date documentation, and make sure all personnel understand their duties for incident response.

20. Penetration tests and Red Team exercises

Develop a penetration test program that includes a full scope of blended attacks.

[1] Center for Internet Security Critical Security Controls for Effective Cyber Defense, version 7.1 (April 2019)

About Webroot

Webroot, a Carbonite company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers to protect small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, Australia and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.