Preventative security tools

CANADIAN CENTRE FOR CYBER SECURITY

May 2024 | ITSAP.00.058

Preventative security tools provide important layers of protection for your networks and devices. Security tools also can help your organization reduce the risks associated with malicious intrusions such as malware, spyware, and unauthorized users.

Examples of preventative security tools

Each of these security tools target specific areas to help prevent security breaches from happening to your organization's network and devices.

Firewalls are security barriers placed between two networks that control the amount and the kinds of traffic that may pass between them. They prevent the unauthorized flow of data from one area of a network to another through the following actions:

- Monitor incoming and outgoing traffic, then filter out the known bad sources
- Ensure downloaded data is part of a legitimate connection
- Decrypt and analyze downloaded data to ensure there is no trace of malicious content before forwarding the data on to your network

Anti-virus software defends devices against malware through the following actions:

- Scan files for viruses before they are downloaded to your device
- Block known malicious software from downloading
- Scan your system's files against a list of known viruses to remove if detected

Virtual private networks (VPNs) are private communications networks (referred to as tunnels) through an untrusted network. A VPN is used to establish a secure connection with authentication and protected data traffic. It sends and receives data through an encrypted tunnel to prevent observations by threat actors. You can use it within your organization or between several different organizations to communicate over a wider network.

For more details on VPN, refer to Virtual private networks.(ITSAP.80.101).

Ad blockers are a type of browser extension software that blocks advertisements, such as webpage displays and pop-ups, from your system while you browse the web.

Virtualization is a technique that creates an isolated environment for specific applications to run on your device. Virtualization can be used for the following purposes to improve security:

- Separate business and personal applications
- Isolate different applications and processes for specific groups and business lines
- Download malicious content for testing, using an isolated environment to prevent access to other applications

Application allow and deny lists are used to control which applications can run on a device. They can:

- approve specific applications and application components to run on organizational systems
- prevent users from installing unauthorized software

Anti-phishing software reports and blocks phishing emails to prevent attacks from occurring or spreading further through other recipients. You can use this software to prevent identity theft, credit card fraud, and financial loss.

You should also follow Domain-based Message Authentication, Reporting, and Conformance (DMARC) policies to prevent phishers from using your organization's domain to send spoof emails. These policies also authenticate domains to filter legitimate email domains from hidden phishing domains.

For more information on phishing prevention, refer to Spotting malicious email messages (ITSAP.00.100) and Don't take the bait: recognize and avoid phishing attacks (ITSAP.00.101).

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Cat No. D97-1/100-058-2024E-PDF

ISBN 978-0-660-70840-9

Canada

Preventative security tools

CANADIAN CENTRE FOR CYBER SECURITY

May 2024 | ITSAP.00.058

Cloud security subscriptions can provide protection services over your cloud network, data, and accounts. These services may include security features, such as:

- encryption and key management to protect your data
- traffic filtering based on rules you create like blocking HTTP addresses and common attack patterns
- detection of threatening network activity and account behaviour within your cloud environment
- anti-ransomware and anti-malware protection to prevent threat actors from stealing or damaging data

Cloud access security broker (CASB) software solution enforce your organization's security policy by:

- validating that the network traffic between your organization's devices and the cloud provider complies with your organization's security policies
- detecting threats and monitoring sensitive data in transit

Artificial intelligence enhanced security tools

Artificial intelligence (AI) introduces a more efficient and accurate application of security tools. Machine learning algorithms allow AI to adapt to new threats and react in real-time. Many traditional security tools rely on signature or rule-base detection systems, which work only for known threats. In AI -based security tools, algorithms use training data to learn how to respond to different situations. AI can improve cybersecurity in the following ways:

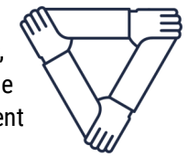
- Keep pace with emerging and unknown threats
- Streamline response process by automating routine tasks
- Log and analyse vast amounts of data
- Limit the amount of 'false positive' threat results and improve detection rates

However, AI is not without its faults. It is subject to its own bias based on its training data and AI threat detections should always be complemented by human expertise. Data that AI is trained on may be inaccurate or illogical. It can be subject to tampering and misinformation.

For more information on AI, see Artificial intelligence (ITSAP.00.040) and Generative artificial intelligence (AI) (ITSAP.00.041).

Unified threat management

Unified threat management (UTM) is a solution that incorporates multiple functions to address different types of threats. UTM often includes preventative security tools such as firewalls, VPNs, anti-phishing software, allow lists, and web content filtering. UTM analyzes content that enters the system to ensure it is clean before sending it to the user. UTM removes detected malicious content before the device accesses it and then sends a report to notify the user of the removal.



Additional security practices

Corporate security policies can help determine which of the preventative security tools described in this document are right for your organization. Although these security tools help reduce cyber security risks, there are still other ways for threat actors to gain access to your system. You should also implement the following security practices:

- Patch and update your security software frequently
  - Out-of-date software can raise the risks of your devices being infected by malicious content
  - For more information, consult How updates secure your device (ITSAP.10.096)
- Apply the principle of least privilege
  - You should only grant individuals the privileges they need to complete their jobs
  - This allows you to limit potential damage caused by accidental, incorrect, or unauthorized use of data and systems
  - Refer to Identity, Credential and Access Management (ICAM) (ITSAP.30.018) for more information
- Offer tailored training to employees
  - Promote awareness on current cyber security threats
  - Ensure employees know their responsibilities in using preventative security tools
  - Refer to Offer tailored cyber security training to your employees (ITSAP.10.093) for more information

Learn more

- Protecting your information and data when using applications (ITSAP.40.200)
- Network security logging and monitoring (ITSAP.80.085)
- Top 10 IT security action items: No. 10 Implement application allow lists (ITSM.10.095)
- Cybersecurity and Infrastructure Security Agency: Free cybersecurity services and tools

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Canada