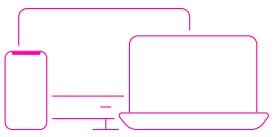
Cybersecurity Cheat Sheet

10 steps to protect your organization from today's growing threats

REQUEST A FREE TRIAL

Cybersecurity doesn't have to be complicated. Save time and resources by following these 10 steps to implement solid cybersecurity protections for your organization. By choosing the right cybersecurity providers you can make this happen even if you're short on budget, staff, and security expertise.

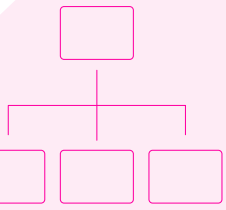


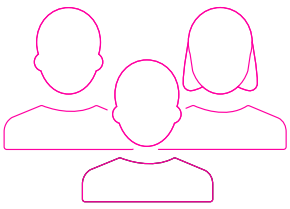
Step 1: Protect your Endpoints

Criminals use various malware to access valuable corporate data on endpoints and servers. Ransomware is used to lock endpoint and file access until payments are made. All strong cybersecurity programs start with endpoint protection. See the MITRE ATT&CK Evaluation to help evaluate endpoint solution providers.

Step 2: Keep your Network safe

Discover network attacks like port scanning and lateral movement to ensure criminals aren't lurking around your environment. Deception technologies can also help by deploying decoy files, users, and devices to trick into cybercriminals into exposing their presence on your network.



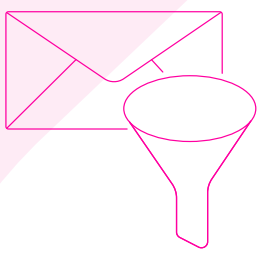


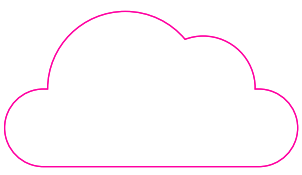
Step 3: Protect your Users

You should always use multifactor authentication, monitor user entitlements, and have specific plans for thoroughly decommissioning users who leave your organization. It's also important to protect user credentials from theft and prevent account takeover attacks.

Step 4: Filter your Email

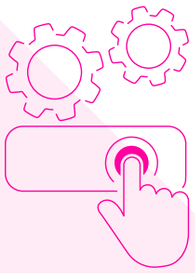
Many successful breaches begin with phishing attacks that lead to malware infections and credential theft, so implementing a strong email security solution is important. While endpoint, network and user protections can identify threats that begin with email, it's better to stop these threats at the source.





Step 5: Eliminate risks with SaaS and Cloud applications

Ensure all your SaaS and Cloud apps are always properly configured to minimize the risk of fraudulent access to your sensitive data. Given the volume and complexity of SaaS and Cloud apps used by most organizations, Cloud and SaaS Security Posture Management tools can help as this is almost impossible to do manually.

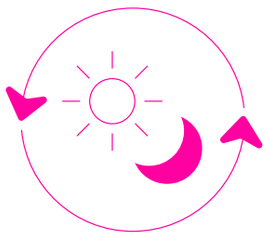


Step 6: Put your response actions on autopilot

It's very difficult for lean security teams to investigate and respond to all threat alerts consistently and thoroughly. Response automation can ensure all detected threats are addressed and handled correctly, especially if you don't have enough resources or deep cybersecurity expertise.

Step 7: Ensure you have 24/7 security coverage

Your organization must be protected around the clock, even when your security team is sleeping. A managed detection and response (MDR) service can ensure around the clock coverage, as well as provide deep cybersecurity expertise and advice any time it's needed.

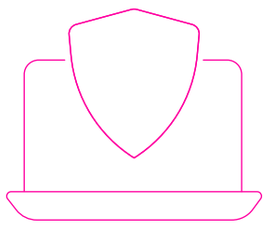


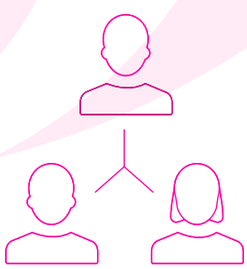
Step 8: Leverage your Log data

Almost all actions taken across your systems are logged in one way or another. Having a robust centralized log management (CLM) solution can help you hunt for threats and collect the data you need for compliance purposes.

Step 9: Get Cyber Insurance

You may have great protections in place, but cyber insurance helps transfer some of your risk and can be highly valuable in a "worst case scenario." Most insurers provide discounts when you have a strong cybersecurity program in place.





Step 10: Manage 3rd Party Risk

Even the best cybersecurity program can by subverted if your vendors and partners have lax protections. Audit your providers to ensure they have the appropriate protections in place and understand whether they are introducing risk into your environment.

REQUEST A FREE TRIAL