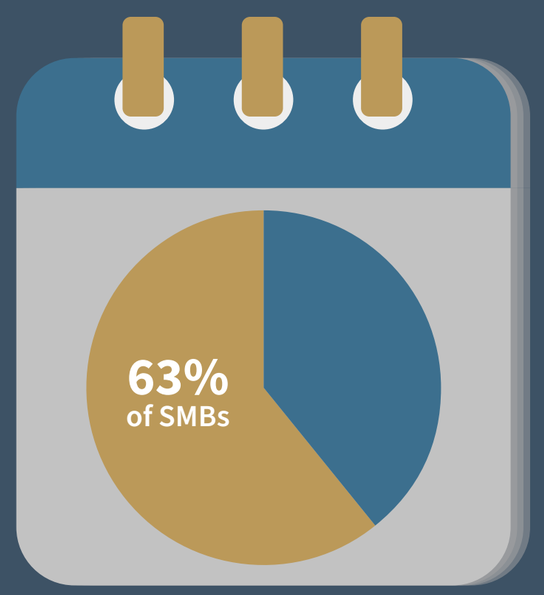
XANTRION

63% of SMBs Have Experienced a Data Breach in the Last 12 Months

It's no longer enough to just install antivirus software and think that you have a robust data and system protection installed and call it a security offering. Today, you need a cybersecurity strategy that stands toe-to-toe with the bad guys' methods, frequency, and vectors of attack. Rather than starting with solutions and working backwards, we recommend using a layered approach below and work towards solutions that fill the gaps.



12 months

Think of your security needs as layers. Each layer should represent an aspect of a cyberattack that needs to be addressed differently than the others, as well be seen as an opportunity to secure that part of the environment.

7 Critical Security Layers

- **Perimeter**: Think of this as the logical "edge" of your network, where potentially malicious data may enter or exit. Network appliances, network connectivity points, as well as email and web traffic all represent places that may need to be secured.
- **User**: The employee plays a role when they interact with potentially malicious content; either they are an unwitting victim or play a part in stopping attacks. This makes it necessary to pay attention to the user as part of your offering strategy.
- **Endpoint**: Think about both corporate and personal devices, laptops, tablets, servers, and mobile phones; every endpoint needs to be protected.
- **Identity**: Ensuring the person using a credential is the credential owner is another way to keep you secure.
- **Privilege**: Limiting elevated access to corporate resources helps reduce the threat surface.
- **Applications**: These are used to access information and valuable data, so monitoring their use by those with more sensitive access makes sense.
- **Data**: Inevitably, data is the target. Watching who accesses what provides additional visibility into whether an environment is secure.

For every one of these layers (shown above), there are specific methods and actions taken as part of a cyberattack, as well as types of solutions available to address cybersecurity concerns at that layer.

Attack Methods and Solutions

1. Vulnerabilities, email, web, phone.
Solution = Firewalls, email/web scanning, DNS filtering

2. Phishing, scams, social engineering.
Solution = Security awareness training

3. Malware, evasive techniques, fileless attack, RDG.
Solution = Antivirus, endpoint detection & response, application whitelisting, enterprise mobility management

4. Leveraging credentials, lateral movement.
Solution = Multi-factor authorization, Identity & access management

5. Elevation, permissions, persistence.
Solution = Privileged access/session management

6. Recon, leverage, access.
Solution = App-specific auditing, user activity monitoring, user behavior analytics

7. Exfiltration, encryption, fraud, espionage.
Solution = User activity monitoring, file auditing