To help you better defend and digitally assure your own Microsoft Office 365 environment, Bamboo digital assurance team offers 10 recommendations:

BAMBOO
CONNECT GROW

1

Understand your privileged accounts.

You need to understand which accounts can access sensitive data or use powerful Microsoft Office 365 tools such as eDiscovery. Such accounts will be prime targets for cyber criminals. Strictly limiting system and tool access to required job roles will contain the damage from a compromised account.

BAMBOO
CONNECT GROW

2

Measure the right metrics.

Any metrics you use to measure security effectiveness must pass the “so what?” test. It must trigger a specific action and not merely inform. Make sure you measure the time it takes to acknowledge a threat and the time required to respond to one. You should also measure repeated incidents and reinfection rates. All of this information will reveal how effectively your team is identifying and mitigating threats.

BAMBOO
CONNECT GROW

3

Implement MFA.

Multi-Factor authentication may not be the golden ticket of securing accounts, but it's still an important tool for slowing down attackers. If you don't already, ensure that all accounts are using MFA.

BAMBOO
CONNECT GROW

4

Minimise configuration complexity.

Transitioning hybrid cloud environments can open up security, redundancies and blind spots that can be exploited. Lengthy and complex transitions can also strain your IT and security resources and increase risk. Simplified configuration will streamline your environment and shorten periods of heightened risk.

BAMBOO
CONNECT GROW

5

Conduct regular testing.

Exercises such as penetration testing and digital reconnaissance (Helix) will help you assess the foundation of your security defences by identifying vulnerabilities and attack paths. Repeat these tests regularly to ensure that any changes actually improve your security stature.

BAMBOO
CONNECT GROW

6

Train all your staff, including security professionals.

As you shift your operations to the cloud, make sure that your workforce knows how to use all tools safely and securely. Educate employees about specific threats too, such as adversaries who try to impersonate the IT team in phishing emails. And, ensure that your security staff understand the new environment and can switch from traditional perimeter-based strategies to those that work for the more open borders of the cloud.

BAMBOO
CONNECT GROW

7

Understand how tools are being used.

Microsoft Office 365 tools like eDiscovery and Power Automate can be devastating in the wrong hands. You need to learn how these tools are used in the context of their normal behaviour. Suspicious or malicious activity should be identified immediately and stopped before any damage can be done.

BAMBOO
CONNECT GROW

8

Gain a unified view across your environments (Bamboo Helix)

Adversaries will freely move between your traditional environment and cloud networks, challenging you to look for threats across the board. You need to be able to identify malicious behaviours throughout your IT network, SaaS cloud environment, data center and other areas that could be exploited. You must monitor your entire digital attack surface.

BAMBOO
CONNECT GROW

9

Use Artificial Intelligence to accelerate and automate your response times.

You aren't the only one benefiting from the increased speed and scale of the cloud. Threat actors are as well. Enhanced analytics derived from AI and machine learning can help you identify malicious activity sooner and then automate your response.

BAMBOO
CONNECT GROW

10

Cut through the noise.

Rapid response capabilities are essential but they're only half the story. You need a way to cut through the noise so that you're not overwhelmed by too many false positives. Using an AI-powered network detection and response tool that's accurate and reliable can help achieve this.

BAMBOO
CONNECT GROW