2WTECH
2W Technologies, INC

Advanced Threat Protection and Defender for Endpoint Protection

Your Security, Our Passion

You currently have Anti-virus protection and that alone will not protect your business. 2W Tech recommends adding Advanced Threat Protection and Defender for Endpoint Protection for a minimal fee each month to your current solution. This will give your business a complete endpoint security solution.

Core features of this software include:

Threat and Vulnerability Management: Simply put, there are gaps or weaknesses in every system that make threats possible and tempt threat actors(bad people) to exploit them. This feature will help find those gaps, so they can be fixed. Making you less vulnerable.

Attack Surface Reduction: Reducing this is critical to your business. Your 2 primary attack surfaces are your people and your devices. Your people and your devices are connecting to the internet, creating more gateways for cybercriminals to carry out cyberattacks. You can't eliminate people and devices, so instead, this software monitors the devices and people while using the internet and raises a flag when something or someone is exposing you to a threat.

Next-Generation Protection in Windows: The technology used in this software is sophisticated enough that in real-time it scans your files and apps to detect any threats. And because it runs on the cloud, the software remains updated, and constantly scans for new threats, without you having to take any steps to make it happen. A lot of threats that your business is exposed to comes in way of phishing emails or buried in your data that may not be visible to the naked eye. This feature helps you see things you can't.

Endpoint Detection and Response (EDR) Capabilities: Monitor and collect activity from your data that is coming in and going out over your network. This data is stored for up to 6 months so analysts can travel back in time to the start of an attack. Equipped with a pretty cool dashboard also.

Automation: Because this software doesn't take any chances, it produces a lot of alerts to be investigated and that could really test your bandwidth. Microsoft built in automated investigation and remediation (AIR) capabilities that when properly installed and tuned, these features can reduce the alert volume, so you only need to spend time on legit threats and increase response time in responding to these threats.

Secure Score: In your dashboard, you can see a secure score for all devices. The scores can give organizations a high-level view of their device configuration and overall strategy. It makes it easy for you to determine what devices and users are at risk and allow you to make adjustments only as needed, essentially saving your IT team time and hassle.

Microsoft Threat Experts: That's us, your 2W Tech team!

Run Attack Simulations: This feature can be cool if you want to test out and see how the software really works to protect your business. Within this evaluation lab, you can run attack simulations based on a few different options. Throughout the simulation, you can view the status of the virus and threat protections that were discovered. You can also view more details, alerts, machines, and evidence found during this investigation. If you don't truly understand how at risk your business is, running simulations can show you how important your security solution is for your business.

THREATS ARE NO MATCH

Threat & Vulnerability Management
Attack surface reduction
Next-generation protection
Endpoint detection and response
Automated investigation and remediation
Microsoft Threat Experts

Sales@2WTech.com
2WTech.com

CALL US:
(262)686-5070

Gold
Microsoft Partner
Microsoft