Proofpoint and Microsoft Defender for Endpoint

Microsoft Defender for Endpoint

How Proofpoint and Microsoft work together to provide multilayered protection against email-borne threats

Products

Proofpoint

- Targeted Attack Protection
- Proofpoint Threat Response Auto-Pull (TRAP)

Microsoft

- Microsoft Defender for Endpoint

Key Benefits

- Gain immediate visibility and context into threats
- Reduce time taken to remediate threats
- Achieve multilayered threat protection
- Secure organizations' devices and data against sophisticated attacks

A powerful integration of Proofpoint and Microsoft products gives you enhanced protection against email-borne threats. It combines Proofpoint's expansive threat intelligence with Microsoft Defender for Endpoint's deep visibility on user devices. It guards against targeted attacks and protects against both malicious emails and URLs delivered to your people. The integration is free to all joint customers of Proofpoint and Microsoft Defender for Endpoint.

The integration offers many benefits. These include improved threat protection across email and endpoints. It also leads to a reduced workload for the security operations center (SOC) team, less time spent investigating incidents and assistance prioritizing remediation efforts.
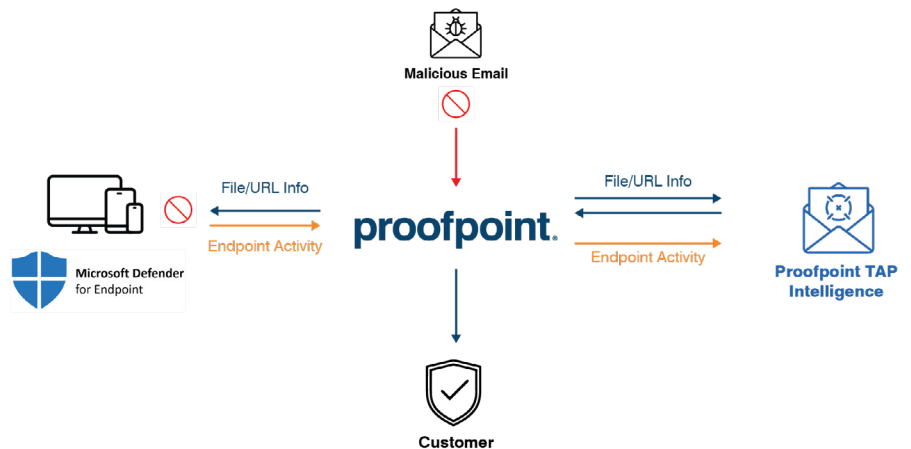

Figure 1: How Proofpoint TAP and Microsoft Defender for Endpoint keep customers secure from malicious files and URLs.

The Solutions

To deal with all the types of threats your organization can face, you must have a multilayered defense in place. The solutions in the Proofpoint and Microsoft integration give you what you need.

Proofpoint Targeted Attack Protection

Proofpoint Targeted Attack Protection (TAP) uses our world-class threat intelligence to provide you with a clear view of the threat landscape. We constantly analyze and correlate a trillion data points across email, cloud, network, endpoint and social networking sources to build this intelligence and keep it up to date.

We offer unrivaled analysis and protect against emails that contain malicious URLs, attachments or business email compromise (BEC) threats. If you also have Proofpoint Threat Response Auto-Pull (TRAP), you can remediate emails that have turned malicious post-delivery.

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is the most widely used endpoint protection solution in the industry. It protects the endpoint by managing vulnerability and defending against mobile threats. It provides deep visibility into activity on your users' devices.

How It Works

With solutions designed mostly for the cloud, Proofpoint's visibility into activity on user devices is not as extensive as that of Defender for Endpoint. So, Proofpoint products are not as well-equipped to know if, say, a user has saved a malicious file to a device that then spread to other parts of the system. This is where working with Defender for Endpoint comes into play.

Malicious File Deliveries

TAP detects a malicious file that was delivered through email. It alerts Proofpoint TRAP to quarantine related messages. Proofpoint then shares the file hash with Defender's Custom Indicator list for endpoint protection. Defender provides TAP visibility into file activity on endpoints. This information may include affected users and devices. It can also include metadata about file activity on each device.

Malicious URL Deliveries

TAP detects a malicious non-rewritten URL that was delivered through email. It alerts Proofpoint TRAP to quarantine related delivered messages. Defender then provides TAP with visibility into endpoint activity for the SOC team to use. This information may include users who clicked on the URL. It can also include impacted devices and metadata about file activity on each device.

LEARN MORE

For more information, visit **proofpoint.com**.

proofpoint.