

Zero Day Protection:

The new Zero Day Initiative in The SecPoint Protectors makes it the key component in your network defence system.

SecPoint offers Zero Day Protection in the Unified Threat Management Protector appliance, preventing new and unknown attacks.

What is a Zero Day attack?

A Zero Day vulnerability is a known term in the black hat community for new exploits that the application vendor is not yet aware of and therefore has not released a patch for.

It is a known term to trade for Zero Day vulnerabilities in the black hat community.

Zero Day vulnerabilities are unknown or new attacks for vulnerabilities for which no patch has yet been released.

When you have Zero Day Protection you are protected against unknown and new vulnerabilities and closing the windows of vulnerability waiting time. Where signature only based products are relying on the database.

Several techniques are applied to protect for Zero Day attacks:

- Connections in the black hat community.
- Pattern matching removes high risk dangerous files by inspecting the entire packet.
- Stops suspicious behaviour from systems probing a target system.
- Stops traffic that does not match protocol standards.
- Zero Day signatures.

Zero Day Protection part of the UTM features of the Protector.

The real-time bi-directional architecture of the Protector combines key security capabilities able to defend against classes of attacks, and to protect against variants even before they are known.

Some of these capabilities include:

- Protocol anomaly detection blocks malicious traffic that does not conform to established protocol standards.
- Pattern matching flags and removal of high-risk files, such as .exe and scripting files, viruses, spyware, and trojans from the system by fully inspecting the entire packet.
- Behaviour analysis identifies and stops traffic from hosts exhibiting suspicious behaviours, including DoS and DDoS attacks, port scans, and address scans.

The Attack Window:

From the time a new vulnerability is identified and until a patch is created, there is a when your systems are at risk. It is therefore important to implement different techniques to protect against Zero Day exploits.

Even a few minutes without Zero Day protection can be a huge security risk.

Sometimes it can take the vendor hours, days or even weeks to create a patch. In some cases the patch will not work correctly and the system would still be subject to attack.