Think Beyond Traditional Antivirus

For years, prevention products’ primary threat protection was based on signatures. Assuming all attacks at a business had been seen before, using signatures made sense. Today, malware mutates daily, even hourly, making signature-based prevention tools obsolete.

It is time to think beyond traditional antivirus. Think CylancePROTECT.

CylancePROTECT is an integrated threat prevention solution that combines the power of artificial intelligence (AI) to block malware infections with additional security controls that safeguard against script-based, fileless, memory, and external device-based attacks.

Unlike traditional endpoint security products that rely on signatures and behavior analysis to detect threats in the environment, CylancePROTECT:

- Uses AI, not signatures, to identify and block known and unknown malware from running on endpoints
- Delivers prevention against common and unknown (zero-day) threats without a cloud connection
- Continuously protects the endpoint without disrupting the end-user

With unmatched effectiveness, minimal system impact, and zero-day prevention, CylancePROTECT protects endpoints and organizations from compromise.
CylancePROTECT Features

**True Zero-Day Prevention**
- Resilient AI model prevents zero-day payloads from executing.

**AI Driven Malware Prevention**
- Field-proven AI inspects any application attempting to execute on an endpoint before it executes.

**Script Management**
- Maintains full control of when and where scripts are run in the environment.

**Device Usage Policy Enforcement**
- Controls which devices can be used in the environment, eliminating external devices as a possible attack vector.

**Memory Exploitation Detection and Prevention**
- Proactively identifies malicious use of memory (fileless attacks) with immediate automated prevention responses.

**Application Control for Fixed-Function Devices**
- Ensures fixed-function devices are in a pristine state continuously, eliminating the drift that occurs with unmanaged devices.

Common CylancePROTECT Use Cases

CylancePROTECT provides full-spectrum threat prevention covering these common security use cases:

- The need to identify and block malicious executables
- Controlling where, how, and who can execute scripts
- Managing the usage of USB devices, prohibiting unauthorized devices from being used
- Eliminating the ability for attackers to use fileless malware attack techniques on protected endpoints
- Preventing malicious email attachments from detonating their payloads
- Predicting and preventing successful zero-day attacks

The Benefits of CylancePROTECT

<table>
<thead>
<tr>
<th>Comprehensive Security</th>
<th>Smooth Business Operations</th>
<th>Zero-Day Payload Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full-spectrum autonomous threat prevention simplifies the security stack</td>
<td>Whisper-quiet prevention ensures business operations are not disrupted</td>
<td>Eliminates the risk of an attack exploiting a zero-day from being successful</td>
</tr>
</tbody>
</table>