SOLUTION BRIEF

Securonix and Cylance Improve Endpoint Visibility and Response

The cyber security landscape continues to increase in complexity. Hackers continue to innovate, business technologies generate increasing amounts of data, and legacy perimeter defenses struggle with modern insider and cyber threats.

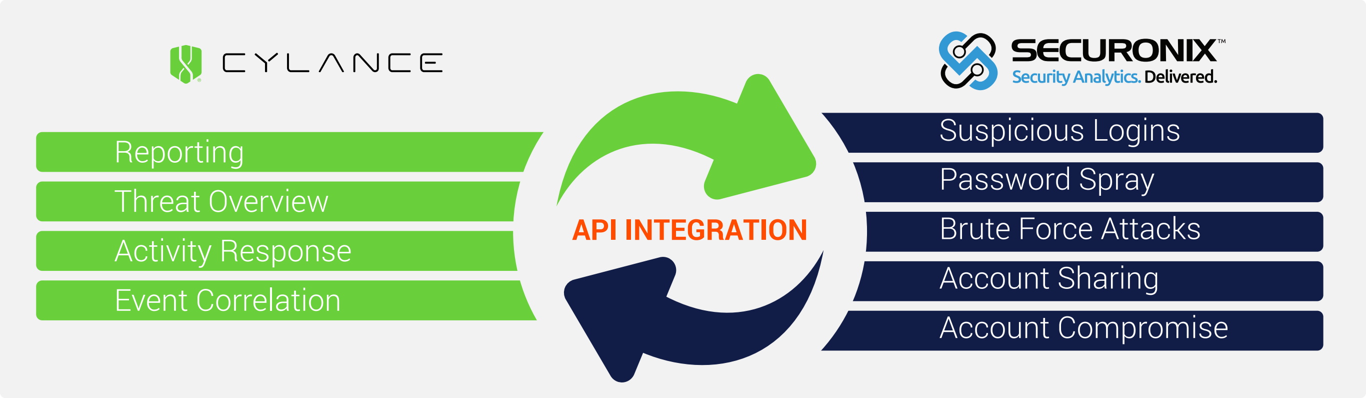
The next generation of SIEM, the Securonix Security Analytics Platform, combines log management, security incident and event management (SIEM), and user and entity behavior analytics (UEBA) into a complete, end-to-end platform that can be deployed in its entirety or in flexible, modular components. It collects massive volumes of data in real time, uses patented machine learning algorithms to detect advanced threats, and provides actionable security intelligence for quick response.

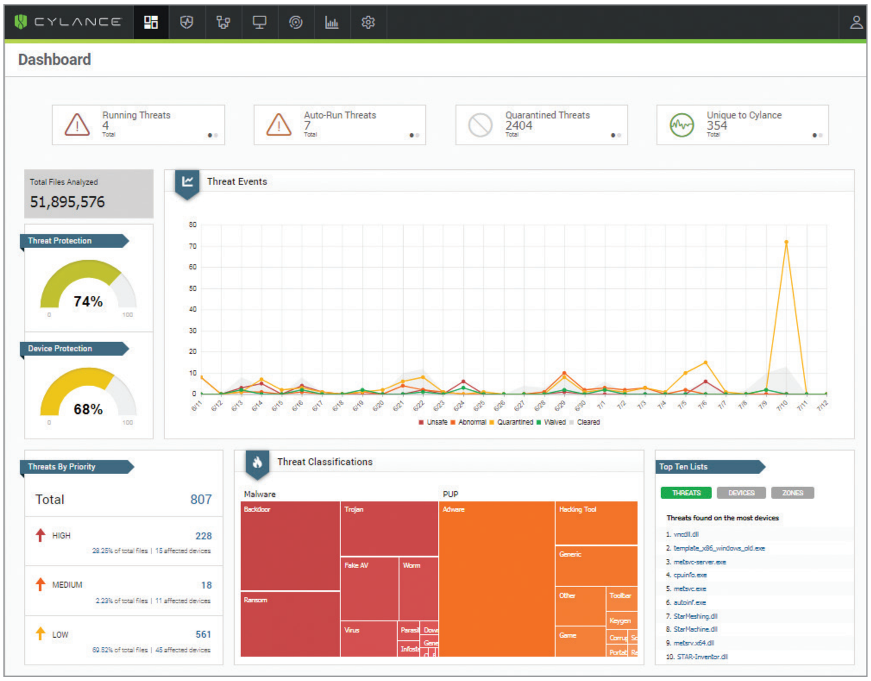
CylancePROTECT is threat prevention solution that combines the power of artificial intelligence (AI) to block malware infections with additional security controls that safeguard against script-based, fileless, memory, and external device-based attacks. It unifies the technologies required to successfully stop breaches, including next-generation antivirus, endpoint detection and response, IT hygiene, 24/7 threat hunting, and threat intelligence.

The Securonix platform combined with CylancePROTECT provides continuous protection and prevention in a single agent that proactively detects and responds to virus, malware, ransomware, and other known and unknown threats. Securonix gathers real-time intelligence from your endpoints using the Cylance API. This information provides additional context used to assist threat detection and investigation. User behavior information collected by Cylance is also used to enrich Securonix's behavioral analytics.

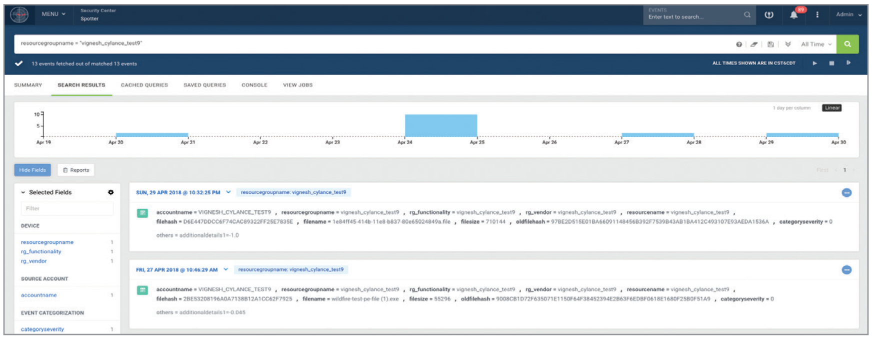
Integration Benefits

- AI driven prevention, 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
- Continuous endpoint protection without disrupting the end-user
- Use endpoint user behavior data to enrich behavioral analysis and add additional depth to your analytics.





The CylancePROTECT dashboard provides an overview of threats.



```
resourcegroupname = "vignesh_cylance_test9"
13 events fetched out of matched 13 events

SUN, 29 APR 2018 @ 10:32:25 PM   resourcegroupname: vignesh_cylance_test9
accountname = VIGNESH_CYLANCE_TEST9 , resourcegroupname = vignesh_cylance_test9 , rg_functionality = vignesh_cylance_test9 , rg_vendor = vignesh_cylance_test9 , resourcename = vignesh_cylance_test9 ,
filehash = D6E447DDCC6F74CAC89322FF25E7835E , filename = 1e84ff45-414b-11e8-b837-80e65024849a.file , filesize = 710144 , oldfilehash = 97BE2D515E01BA66091148456B392F7539B43AB1BA412C493107E93AEDA1536A , categoryseverity = 0
others = additionaldetails1=-1.0

FRI, 27 APR 2018 @ 10:46:29 AM   resourcegroupname: vignesh_cylance_test9
accountname = VIGNESH_CYLANCE_TEST9 , resourcegroupname = vignesh_cylance_test9 , rg_functionality = vignesh_cylance_test9 , rg_vendor = vignesh_cylance_test9 , resourcename = vignesh_cylance_test9 ,
filehash = 2BE53208196A0A7138B12A1CC62F7925 , filename = wildfire-test-pe-file (1).exe , filesize = 55296 , oldfilehash = 9008CB1D72F635071E1150F64F38452394E2B63F6EDBF0618E1680F25B0F51A9 , categoryseverity = 0
others = additionaldetails1=-0.045
```

Securonix API integration with the CylancePROTECT API gathers and enriches event details. Securonix assigns a risk score to the event and, depending on the context of the user's other behaviors, can elevate the risk score or enact predefined threat playbook actions to further mitigate the threat.

How it Works

- CylancePROTECT analyzes, identifies, and blocks suspected malicious activity.
- Securonix uses RESTful APIs to gather data from CylancePROTECT.
- Securonix behavior analytics use self-learning to baseline normal behavior patterns in your endpoint data and detect anomalous threats.
- Threats with a risk score above a set threshold can trigger automated playbook responses.
- Securonix uses endpoint data from CylancePROTECT to create data insights and visualize cybersecurity threats, risks, and compliance metrics.
- Securonix initiates response action on endpoints through Cylance via incident response playbooks.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.

About Cylance

Cylance uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security. For more information visit www.cylance.com.

SECURONIX™
Security Analytics. Delivered.

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000