SECURONIX™ | CISCO

SOLUTION BRIEF

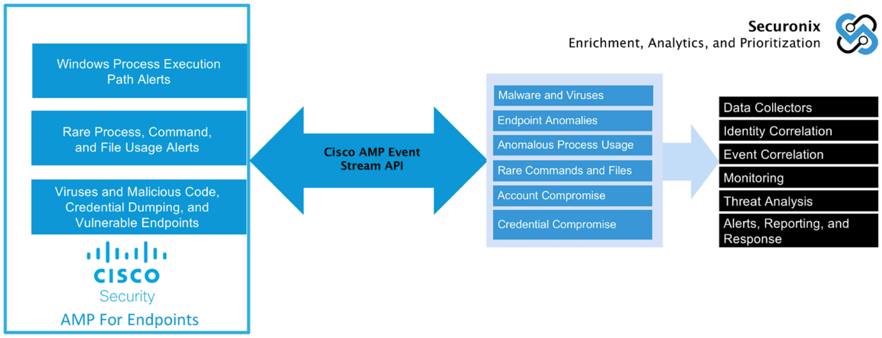
Advanced Endpoint Security and Visibility with Securonix and Cisco AMP

The cybersecurity landscape has become more complex. Hackers continue to innovate, and business technologies continue to generate increasing amounts of data. This makes legacy security monitoring solutions obsolete as they struggle with an inability to scale and weak rule-based threat detection techniques.

The Securonix platform delivers unlimited scale, powered by advanced analytics, behavior detection, threat modeling, and machine learning. It increases your security through improved visibility, actionability, and security posture, while reducing management and analyst burden.

Cisco Advanced Malware Protection (AMP) for Endpoints delivers cloud endpoint protection and advanced endpoint detection and response. AMP stops breaches, blocks malware, and rapidly detects, contains, and remediates advanced threats that evade your front-line defenses.

Antivirus, malware, and endpoint detection and response is one of the cornerstones of security. When integrated, Securonix ingests these security events from Cisco AMP while enriching the data to add greater context for security operations center (SOC) analysts when they investigate incidents. Furthermore, Securonix SOAR (Security Orchestration, Automation, and Response) empowers SOC analysts to quickly respond to malicious file behaviors.


Windows Process Execution Path Alerts
Rare Process, Command, and File Usage Alerts
Viruses and Malicious Code, Credential Dumping, and Vulnerable Endpoints
CISCO Security
AMP For Endpoints
Cisco AMP Event Stream API
Securonix
Enrichment, Analytics, and Prioritization
Malware and Viruses
Endpoint Anomalies
Anomalous Process Usage
Rare Commands and Files
Account Compromise
Credential Compromise
Data Collectors
Identity Correlation
Event Correlation
Monitoring
Threat Analysis
Alerts, Reporting, and Response

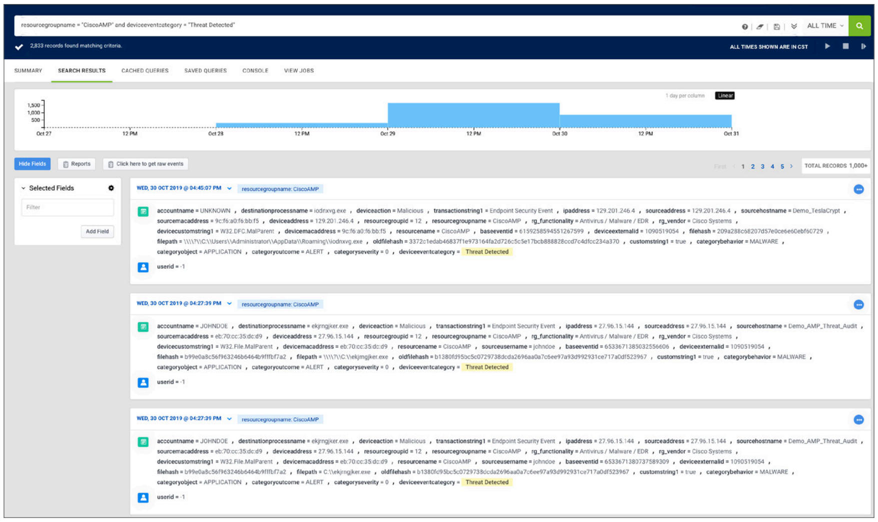
Solution Benefits

- Integrate alerts from Cisco AMP's powerful endpoint protection engine.
- Gain visibility and insight into user activity across your environment.
- Analyze a series of events over time using threat chain models in order to surface the highest risk events beyond a single incident.
- Automate incident response and reduce mean time to respond with access to real-time actionable intelligence.
- Multi-attack monitoring coverage, utilizing detailed syslog processing for comprehensive security.
- Enrich security data with additional context from on-premises data sources and other applications for threat modeling.

Multi-Attack Event Coverage

The Securonix platform captures events from Cisco AMP event sources, utilizing the AMP Event Streamer API to ingest events such as anomalous process and file usage, virus and malware detections, and Windows process execution linked alerts. It also captures other endpoint events such as rare file type usage, ransomware, and suspicious Windows registry activity, as well as network traffic events such as rare port usage and beaconing attempts.

With comprehensive event coverage, Securonix integrates a complete range of threat information from the Cisco AMP platform, utilizing this information for both threat identification and context definition, as well as threat model creation alongside existing threat events.



```
resourcegroupname = "CiscoAMP" and deviceeventcategory = "Threat Detected"
2,833 records found matching criteria.

WED, 30 OCT 2019 @ 04:45:07 PM   resourcegroupname: CiscoAMP
accountname = UNKNOWN , destinationprocessname = iodnxvg.exe , deviceaction = Malicious , transactionstring1 = Endpoint Security Event , ipaddress = 129.201.246.4 , sourceaddress = 129.201.246.4 , sourcehostname = Demo_TeslaCrypt ,
sourcemacaddress = 9c:f6:a0:f6:bb:f5 , deviceaddress = 129.201.246.4 , resourcegroupid = 12 , resourcegroupname = CiscoAMP , rg_functionality = Antivirus / Malware / EDR , rg_vendor = Cisco Systems ,
devicecustomstring1 = W32.DFC.MalParent , devicemacaddress = 9c:f6:a0:f6:bb:f5 , resourcename = CiscoAMP , baseeventid = 6159258594551267599 , deviceexternalid = 1090519054 , filehash = 209a288c68207d57e0ce6e60ebf60729 ,
filepath = \\\\?\\C:\\Users\\Administrator\\AppData\\Roaming\\iodnxvg.exe , oldfilehash = 3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370 , customstring1 = true , categorybehavior = MALWARE ,
categoryobject = APPLICATION , categoryoutcome = ALERT , categoryseverity = 0 , deviceeventcategory = Threat Detected
userid = -1

WED, 30 OCT 2019 @ 04:27:39 PM   resourcegroupname: CiscoAMP
accountname = JOHNDOE , destinationprocessname = ekjrngjker.exe , deviceaction = Malicious , transactionstring1 = Endpoint Security Event , ipaddress = 27.96.15.144 , sourceaddress = 27.96.15.144 , sourcehostname = Demo_AMP_Threat_Audit ,
sourcemacaddress = eb:70:cc:35:dc:d9 , deviceaddress = 27.96.15.144 , resourcegroupid = 12 , resourcegroupname = CiscoAMP , rg_functionality = Antivirus / Malware / EDR , rg_vendor = Cisco Systems ,
devicecustomstring1 = W32.File.MalParent , devicemacaddress = eb:70:cc:35:dc:d9 , resourcename = CiscoAMP , sourceusername = johndoe , baseeventid = 6533671385032556606 , deviceexternalid = 1090519054 ,
filehash = b99e0a8c56f963246b6464b9fffbf7a2 , filepath = \\\\?\\C:\\ekjrngjker.exe , oldfilehash = b1380fd95bc5c0729738dcda2696aa0a7c6ee97a93d992931ce717a0df523967 , customstring1 = true , categorybehavior = MALWARE ,
categoryobject = APPLICATION , categoryoutcome = ALERT , categoryseverity = 0 , deviceeventcategory = Threat Detected
userid = -1

WED, 30 OCT 2019 @ 04:27:39 PM   resourcegroupname: CiscoAMP
accountname = JOHNDOE , destinationprocessname = ekjrngjker.exe , deviceaction = Malicious , transactionstring1 = Endpoint Security Event , ipaddress = 27.96.15.144 , sourceaddress = 27.96.15.144 , sourcehostname = Demo_AMP_Threat_Audit ,
sourcemacaddress = eb:70:cc:35:dc:d9 , deviceaddress = 27.96.15.144 , resourcegroupid = 12 , resourcegroupname = CiscoAMP , rg_functionality = Antivirus / Malware / EDR , rg_vendor = Cisco Systems ,
devicecustomstring1 = W32.File.MalParent , devicemacaddress = eb:70:cc:35:dc:d9 , resourcename = CiscoAMP , sourceusername = johndoe , baseeventid = 6533671380737589309 , deviceexternalid = 1090519054 ,
filehash = b99e0a8c56f963246b6464b9fffbf7a2 , filepath = C:\\ekjrngjker.exe , oldfilehash = b1380fd95bc5c0729738dcda2696aa0a7c6ee97a93d992931ce717a0df523967 , customstring1 = true , categorybehavior = MALWARE ,
categoryobject = APPLICATION , categoryoutcome = ALERT , categoryseverity = 0 , deviceeventcategory = Threat Detected
userid = -1
```

Context-Driven Threat Modelling

The Securonix platform adds useful context to Cisco AMP events. Each event is linked to other related events that may have occurred elsewhere within the enterprise environment, creating a consolidated threat model that plots a threat as it evolves through the various threat stages. The platform allows analysts to take action to mitigate, prevent, or remediate as appropriate, and provides recommendations where possible.

Focus on Visibility and Information Access

Besides tracking threats, a key benefit of the Securonix platform is the detailed visibility into every aspect of enterprise security provided by the web interface. The dashboard provides a bird's eye view of current environment status, while an easy to access event search widget allows quick event access from the first page.

How It Works

- Cisco AMP monitors endpoint and web related threats before, during, and after an attack. Once an unknown file enters a system, AMP continues to record and analyze activity.
- Securonix integrates Cisco AMP alerts and correlates users' behaviors.
- Using threat chain modelling, Securonix brings to light the highest risk events in your organization.
- The Securonix intelligent orchestration engine centralizes operations by streamlining incident response and automation.

About Cisco

Cisco security products work together to deliver effective network security, incident response, and heightened IT productivity through automation. Our security innovations protect customers, employees, and brands by providing highly secure firewalls, web, and email services. Simplifying the complexity of network security, keep your business more secure, and make IT more productive with Cisco security services and solutions. For more information visit www.cisco.com.

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

©2020 Securonix

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