SECURONIX™

SOLUTION BRIEF

Securonix Content Manager

Faster Detection of Advanced Threats

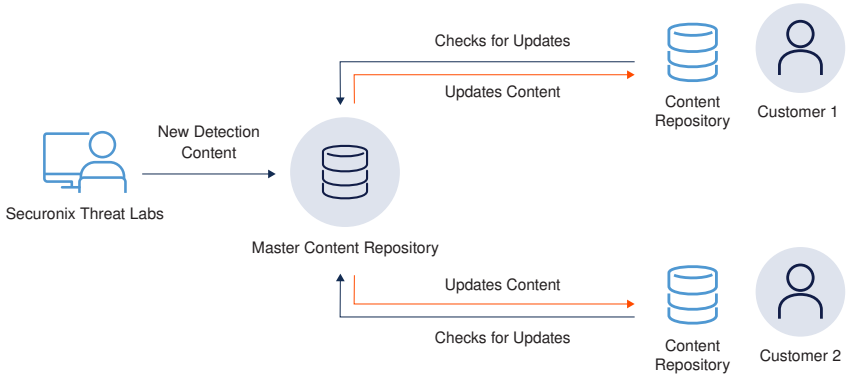
Stay Ahead of Rapidly Evolving Threats

As technology evolves to help enterprises detect and respond to attacks, threats are also evolving at a rapid pace. Threat detection content needs to keep up, enabling security teams to detect and respond to sophisticated threats as they evolve.

Most security teams don't have the time or resources to create their own security analytics content. Creating, managing, and updating threat content takes time away from detecting and responding to threats. Additionally, ease of use and management can be challenging when updates are not seamless.

Simplified Detection Content Management

Securonix created Content Manager to provide detection content 'as-a-service' and simplify threat detection content creation, management, and update process. Securonix Content Manager empowers security teams with consistently updated threat content delivered seamlessly to ensure rapid detection against constantly evolving threats.



Automate and Streamline Your Detection Content

Secuornix Content Manager provides security teams with out-of-the-box content including connectors, parsers, reports, dashboards, policies, and threat models for data sources. Additionally, Content Manager delivers the latest research from Securonix Threat Labs as detection content. To simplify implementation, Securonix Data Dictionary provides standardized labels mapped to attributes to improve your search abilities.

Security teams can selectively opt in for updates that are relevant for their organization. That way, they can tag their company-specific business challenges and automatically find SOC content that matches their company's threat profile. MSSPs can also proliferate local content across their customer tenants with a click of button as needed.

Solution Benefits

- Detect the latest cloud-based threats by leveraging the content updates from Securonix Threat Labs.
- Simplify the management of detection content across multi-cloud environments.
- Rapidly deploy and update content across different tenants with a single click of a button.
- Gain a more consistent search experience with Data Dictionary.

With Securonix Content Manager's automated updates, your security teams can enjoy seamless content deployment and reduce the time it takes them to detect new threats.

Securonix Content Manager includes new detection rules that are primarily aligned with the MITRE Cloud Matrix. This unifies threat content across various cloud service providers like Google Cloud Platform, Microsoft Azure, and Amazon Web Services for ease of content management.

Provides important threat coverage including:

- **Compute:** AWS EC2, EKS, and Lambda; GCP Compute Engine, GKE, and Cloud Functions; Azure VM, Container Service, and Event Grid
- **Storage:** AWS S3, Google Cloud Storage, Azure Storage – Block/Page Blobs
- **Networking and Content Delivery:** AWS VPC, BYOIP, and API Gateway; GCP VPC, Hybrid BYOIP, and Cloud VPN; Azure Virtual Network, ExpressRoute, and VPN Gateway
- **Database Management and Monitoring:** AWS CloudWatch and CloudTrail; GCP Stackdriver, Cloud Shell, and Cloud Audit Logs; Azure Portal, Monitor, and Log Analytics
- **Security:** AWS IAM, WAF, and GuardDuty; GCP Cloud IAM, and Cloud Armor; Azure Active Directory, Application Gateway, and ATP

Securonix Content Manager Gives SOC Teams More Power

Securonix Content Manager simplifies threat content management so your SOC teams can focus on detecting and responding to threats. Automated updates deliver the latest detection content seamlessly, so that you can immediately move to detecting those threats that might be lurking within your environment. Securonix Content Manager aligns threat detection content with the MITRE ATT&CK framework and supports a vast majority of threat detection content policies, threat models, look-ups, parsers, workflows, and threat intelligence. This best-in-class threat detection and response not only simplifies day-to-day security operations, but also provides security teams with greater efficiency.

For more information about how Securonix can improve your search and threat hunting capabilities visit us at www.securonix.com or schedule a demo www.securonix.com/request-a-demo.

Use Cases

- **Network Based Threats:** Includes network scanning and enumeration, brute force, suspicious geolocation, and threat intelligence correlation.
- **Storage Based Threats:** Includes storage object modification, user data modification, cloud service discovery, cloud storage sabotage, cloud storage/ infrastructure sabotage, data (collection) from cloud storage objects, weak permissions, open buckets, and account discovery.
- **Cloud Infrastructure Threats:** Including modify cloud compute, account discovery, resource hijacking, Brute force, and more.
- **EDR Threats:** Including powershell, phishing, malware, ransomware, lateral movement, privilege escalation, account/resource discovery, suspicious network activity, and more.

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

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