DATA SHEET

Symantec Information Centric Analytics

Identify and Act on Cyber Risks

At a glance

- Integrated behavioral analytics capable of analyzing alerts and telemetry from diverse security sources, including DLP – connecting the dots between violations, users, accounts and assets
- Detection of risky user behaviors and identification of malicious insiders and outsiders via comparative risk scoring
- Advanced investigation capabilities and response workflows delivered via clear dashboards and a intuitive user interface

Today's organizations face countless obstacles in seeking to protect their critical data from numerous risks, including malicious insiders, negligent workers, compromised accounts, and advanced persistent threats.

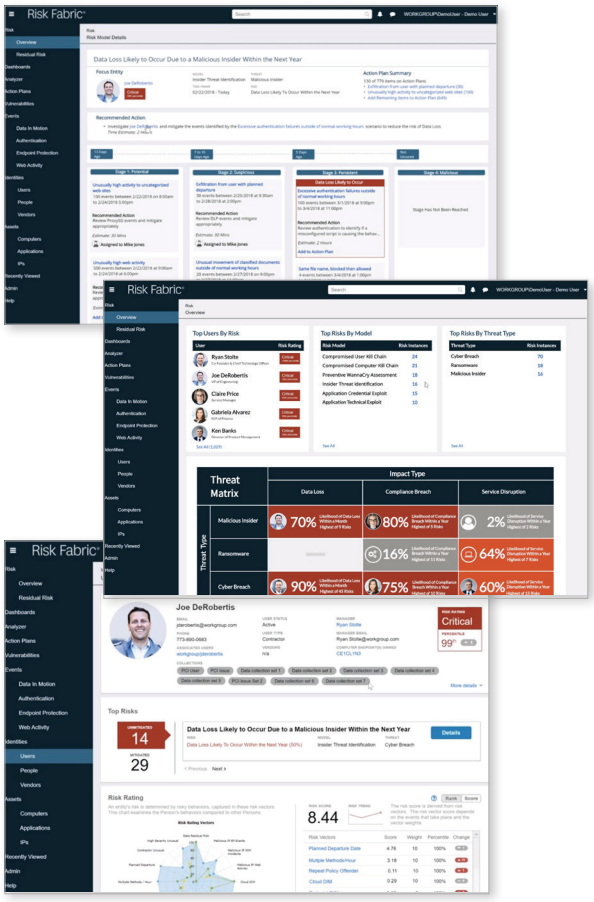
In 2017, over 90 percent of targeted threats sought to identify and steal organizations' sensitive information, with the vast majority of those efforts focused on hijacking the privileges of specific individuals, according to Symantec's "2018 Internet Security Threat Report." Combined with internal attacks, employee errors and inadequate policies, security practitioners remain acutely challenged to pinpoint those user and entity behaviors that represent material risks.

Manual sorting and prioritization of security alerts often fails to escalate crucial security alerts until it's too late. To improve threat detection and mitigation, your organization needs advanced automation to help rapidly prioritize risky behaviors and identify malicious users on a continuous basis.

Solution overview

Symantec™ Information Centric Analytics, powered by Bay Dynamics, is a User and Entity Behavior Analytics (UEBA) platform that provides an integrated, contextually enriched view of cyber risks in your enterprise. It collects, correlates and analyzes large amounts of security event data from across diverse sources, including all data exfiltration channels (data telemetry), user access (identity telemetry), corporate asset data, and alerts from other security systems (threat telemetry). Backed by patented machine learning, ICA delivers rapid identification and prioritization of user and entity based risks.

Symantec Data Loss Prevention provides detailed information about violations of sensitive corporate data, including the responsible source. Data telemetry sources also include Symantec Information Centric Encryption; Symantec Information Centric Tagging and cloud security. Identity telemetry is provided via solutions like Microsoft® Active Directory®, while threat telemetry sources include Symantec Endpoint Protection, Symantec ProxySG™, and Symantec Web Security Service. When sorted, correlated, and analyzed together, this vast amount of data gives invaluable insight into user behaviors.



ICA's adaptive risk models, customizable dashboards and point and click interface allow analysts to address the specific users and risks that matter most to your organization.

Thanks to a flexible and intuitive user interface, ICA allows analysts to rapidly differentiate between malicious and otherwise risky activities. ICA is able to pinpoint both real threats and prevalent issues created by broken business processes, and automatically generate remediation recommendations that measurably accelerate response.

Information Centric Analytics delivers an advanced datacentric UEBA approach providing centralized integration and analysis of large, complex data sets to create clear visibility into those behaviors that demand immediate investigation. ICA does the heavy lifting for you: by enabling rapid prioritization of alerts that represent emerging risks across multiple platforms, along with categorizing those incidents tied to misaligned policies or user mistakes, ICA allows analysts to optimize their time and effort, making the most of related resources.

Additionally, ICA's unsupervised and supervised machine learning capabilities automatically create baselines for comparative analysis, while constantly observing and informing future investigation based on analyst input. Through automated generation of recommended remediation workflows ICA empowers cross-functional teams to partner easily to execute, track and validate risk mitigation through a unified, closed loop process.

Finally, ICA offers dedicated analysis related to leading security compliance measures such as the EU's General Data Protection Regulations (GDPR), providing critical insight into user and entity-based interactions with affected data sets and applications.

Key benefits

- Centralized analysis and reporting of cross-platform, crosspolicy data security risks
- Continuous assessment and prioritization of emerging threats
- Optimization of resources, analyst work cycles, security tooling and policies
- Reduced risk of regulatory noncompliance including GDPR

New security approach

Symantec's information-centric security approach uniquely combines and implements information protection across data loss prevention, data classification, data analytics, encryption, and user authentication technologies. Your data can flow anywhere, yet remain firmly within your organization's control—viewable only by intended recipients, irrespective of device, location, or user's association. Data loss prevention content-aware policies with user-driven classification identifies and locates sensitive data, regardless of whether the data is stored on-premises, on a user's device, or in the cloud. Symantec Information Centric Encryption protects it with its leading identity based encryption schemes.

Only authorized, authenticated users can access the data, thanks to the strong access controls of Symantec Validation and ID Protection Service. The ability to dynamically alter user access (remotely revoking privileges) gives you even more control, enabling you to share even the most sensitive data with confidence. Finally, Information Centric Analytics collects and analyzes incident data to provide insights into risky user behaviors and insider threats.

To learn more about Information Centric Security

To learn more about Information Centric Analytics

System requirements

Primary architectural components

- Server operating system: Microsoft Windows® Server 2012 R2
- Application and web server: Internet Information Server
- Primary database store: SQL Server® 2016 cu5 or above
- Multidimensional database: SQL Server Analysis Services

Typical production database server specifications

- 128 GB RAM, 8–12 cores
- 250 GB minimum disk space

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

19A166399_ds_ICA