Today your organization is faced with protecting critical information in a multifaceted threat landscape that includes malicious insiders, negligent users, compromised accounts, and advanced persistent threats.

In 2016, more than 1.1 billion identities were stolen in data breaches, mainly due to malicious insiders’ actions disguised as legitimate business activities, according to Symantec’s “2017 Internet Security Threat Report.” Unpredictable in nature, these bad actors first locate sensitive or valuable information through reconnaissance, followed by persistent data exfiltration attempts through various channels of communication.

Manual sorting and prioritization of security alerts often doesn’t identify real threats until it’s too late. To level the playing field, your security team needs automated tools to discover and prevent the escalation of risky behaviors and stop malicious users.

Solution overview

Symantec™ Information Centric Analytics, powered by Bay Dynamics, is a software analytics platform that provides an integrated, contextually enriched view of cyber risks in your enterprise. It ingests, correlates, and distills large amounts of security event data from Symantec Data Loss Prevention and other products. Many types of data are collected across multiple sources, including all data exfiltration channels (data telemetry), user access (identity telemetry), corporate asset data, and alerts from other security systems (threat telemetry).

Symantec Data Loss Prevention provides detailed information about each violation of sensitive corporate data policy, including the responsible source. Data telemetry sources can also include Symantec CloudSOC cloud access security broker; Symantec Information Centric Encryption; and Symantec Information Centric Tagging. Microsoft® Active Directory® provides identity telemetry, while threat telemetry sources can 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, which can unveil persistent threats and risky activities.
Information Centric Analytics does the heavy lifting for you: analyzing large amounts of security alerts to deliver a prioritized list of users whose behaviors are elevating your risk level. Now you can quickly remediate potential data breaches and account takeovers, allowing your investigation team to focus on other important tasks. Information Centric Analytics can generate reports on the most risky users or IP addresses, for example, in a format that meets the needs of your security team and the C-suite. Rapid identification of sensitive data exposure that could potentially violate compliance rules enables your business to take immediate action to reduce regulatory risk.

New security approach

Symantec’s information-centric security approach uniquely combines and implements information 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 or user-driven classification detects sensitive data automatically, 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 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, visit www.symantec.com/solutions/information-centric-security.

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

Copyright 2017 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, and the Checkmark logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.