

Cavelo Announces Expanded CIS Benchmark Misconfiguration Capabilities for Microsoft Office 365

New Capabilities Empower Security Practitioners with Office 365 Misconfiguration Detection and CIS Benchmark Implementation



KITCHENER, ONTARIO, CANADA,
December 3, 2024 /EINPresswire.com/

-- Attack surface management

technology provider [Cavelo](#) Inc. today announced the release of a feature to empower security teams to discover misconfigurations and apply Center for Internet Security (CIS) benchmarks to Microsoft Office 365 environments.

“

With applications like Office 365 being vital to business operations, consistent configuration visibility is critical for attack surface management teams.”

*James Mignacca, CEO at
Cavelo*

This capability aims to address the challenges that misconfigurations pose in cloud environments, helping organizations mitigate cyber risk by enabling better alignment with industry-recognized security standards.

The CIS benchmarks, developed by global cybersecurity experts, provide un-biased, consensus-based best practices for securing commonly used systems and applications. Covering over 100 benchmarks across 25 product families, including cloud services, CIS guidelines

prioritize critical areas like network security, data protection, and access management.

“With applications like Office 365 being vital to business operations, consistent configuration visibility is critical for attack surface management teams,” says James Mignacca, CEO of Cavelo. “Misconfigurations in cloud applications like Office 365 pose significant risk. The Cavelo [platform](#) enables security teams to identify and apply CIS benchmark controls to Office 365, ensuring their cloud services uphold the same best practices they maintain across their on-premises infrastructure.”

Cloud services introduce unique challenges for vulnerability management. Unlike traditional

infrastructure, where vulnerabilities stem primarily from software flaws, risk in the cloud is largely tied to misconfiguration.

Common misconfiguration types—such as default settings, insecure permissions, and outdated software—can expose sensitive data, including personally identifiable information (PII). The [2024 Verizon Data Breach Investigations Report](#) identifies misconfigurations as the cause of 10% of reported breaches, underscoring the need for rigorous cloud configuration controls.



James Mignacca - CEO at Cavelo

The Cavelo platform's expanded CIS benchmark capability complements its existing support for CIS Controls V8, which prioritizes safeguards aligned with compliance frameworks such as NIST CSF, CMMC, and PCI.

With this capability, the Cavelo platform helps practitioners align to key controls including:

Inventory and control of enterprise and software assets — Continuous and automated asset, device, and data discovery.

Access control management — Including data permissions automation, data access notifications and data access review.

Vulnerability management — Delivering accurate and thorough vulnerability reports.

Reporting — Providing high-level executive reporting as well as granular reporting for compliance purposes.

The CIS benchmark capability is particularly valuable for managed security service providers (MSSPs) seeking to deepen their understanding of their customers' threat landscape.

The capability enables MSSPs to offer added value by addressing Office 365 misconfiguration risks, strengthening their role as trusted advisors in cyber resilience.

“Our partnership with Cavelo reinforces our commitment to delivering cutting-edge cybersecurity solutions to our clients,” said Vinod Paul, President, Align Managed Services. “The new CIS benchmark capabilities for Microsoft Office 365 allow us to provide even greater value,

helping businesses mitigate cloud misconfigurations and align with industry standards to strengthen their overall security posture.”

The Cavelo CIS benchmark capability is now available to all Cavelo platform users. To learn more security practitioners can visit: <https://www.cavelo.com/platform/tour>

About Cavelo

Cavelo empowers businesses to proactively reduce their cyber risk and liability. Its consolidated attack surface management platform combines sensitive data and asset discovery, access management, and risk-based vulnerability management to simplify governance and compliance initiatives and risk remediation. Visit www.cavelo.com to learn more.

Mandy Bachus

Cavelo

+1 844-969-1616

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/764910541>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.