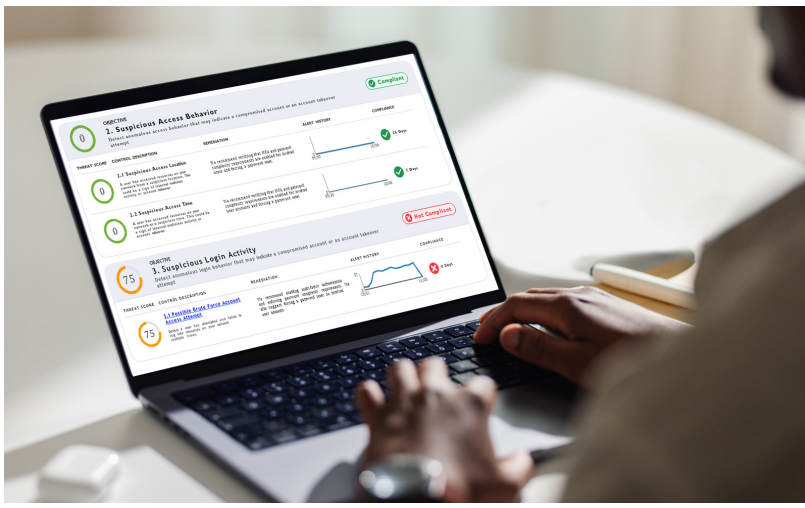
Microsoft 365 Risk and Threat Visibility



Introduction

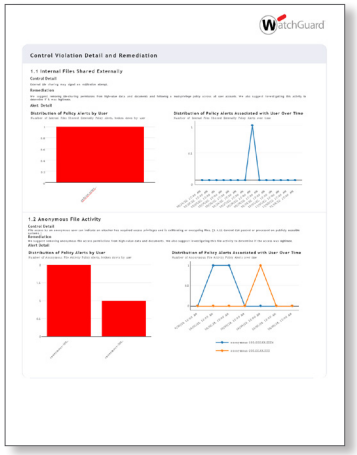
Understanding the risks and threats hidden in your organization's Microsoft 365 (M365) deployment is no easy task. The security capabilities native to M365 are significant, but they are also complex and challenging to manage. Understanding the risks and threats in M365 activities is crucial for protecting your entire organization and your suppliers, partners, and customers.

By actively monitoring your M365 deployment with automated risk and threat reporting, you can identify vulnerabilities or cyberattacks that get lost in the complexity of Microsoft Defender. This proactive approach empowers you as a cybersecurity professional to address M365 issues before damage occurs, thereby boosting your cybersecurity hygiene and defenses.

M365 Risk and Threat Reporting

ThreatSync+ SaaS includes M365 Risk and Threat Reporting. The report provides a detailed look at risky and threatening activity and policy control violations across M365 users. It begins with a visualization and timeline of your overall M365 threat score and trends based on fifteen best-practice control policies. It provides a detailed look at each of the fifteen controls actively monitored by the system. Each control effectiveness section shows the individual threat score and trend line for the control being monitored, and if any gaps or failures are found, guidance on how to remediate them is provided.

The report is easily configurable to meet the specific needs of organizations or cyber defense programs. New controls can be easily built in ThreatSync+ SaaS and added to the M365 report. Its purpose is to quickly and accurately highlight M365 issues, provide managers with a way to establish M365 security objectives, and track progress and improvements toward them.

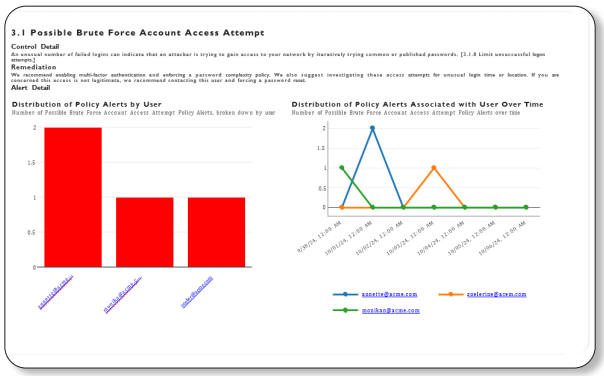


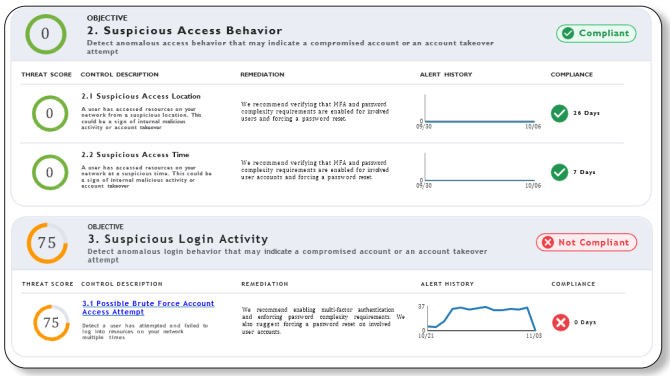
The Microsoft 365 Risk and Threat report is a comprehensive resource that offers detailed insights into the activities within your Microsoft 365 deployment. It provides a thorough overview of the risks and threats related to all fifteen critical controls and objectives, ensuring that your Microsoft 365 environment and users are safeguarded. These insights are crucial for your cybersecurity program as they furnish the necessary information to comprehend your security position and identify steps for enhancing it. The specific information included in the report may vary based on the deployed controls but typically encompasses:

- A prioritized view of top threats to your M365 environment.
- The criticality level of each risk, typically classified as critical, high, or medium.
- A description of each risk, including the type, severity, and potential impact.
- Recommendations for removing each risk, such as installing security updates, removing malware, isolating devices, changing credentials, or configuring security settings.

Examples of specific security risks that may be identified in the assessment:

- Internal files share externally
- Suspicious file activity by rate
- Anonymous file activity
- Internal files made public
- Brute force password attack
- Suspicious admin changes, rate
- Suspicious admin changes, time
- Suspicious access location
- Suspicious access time
- Impossible travel/access
- Suspicious access rate





To learn more about WatchGuard M365 Risk and Threat reports, please get in touch with your WatchGuard representative.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com