UTMStack® is a Unified Threat Management Platform that delivers all essential security services. It includes threat detection and response, compliance management, log management (SIEM), vulnerability management, network/host IDS/IPS, Asset Discovery, Endpoint Protection, Identity Management, Incident Response, File Classification, Dark Web Monitoring, and threat Intelligence. UTMStack is designed for hybrid environments and can be easily deployed across on-premises and cloud providers.

Simpler and Cost-Effective

UTMStack bundles several cybersecurity products under a single platform. This approach makes the solution cost-effective and simpler. It reduces the learning curve for security professionals and the costs of buying different tools from multiple vendors. Having all the data in a single place increases the effectiveness of correlation engines and machine learning algorithms. The platform also includes a powerful dashboard and report builder that can be used to personalize your monitoring experience or for advanced compliance auditing and reporting.

Asset Discovery

- Network devices discovery and inventory.
- Software assets inventory.
- Asset basic information collection.

Vulnerability Scanner

- Application vulnerability assessments.
- Network devices Vulnerability Assessment.
- Azure and AWS Vulnerability scans.

Log Management (SIEM)

- Log collection and correlation.
- Log management.
- Dashboard and Report Builder.
- Log and event explorer for forensic analysis.

Network and Host Intrusion detection

- Rule-based Network Intrusion Detection.
- Rule-based and heuristic analysis-based Host Intrusion detection System with ATP capabilities.
- Network traffic, protocol, and DNS analysis.

Compliance management

- HIPAA, GLBA, SOC, and GPDR Compliance reports.
- Compliance status dashboards.
- Custom compliance reports builder.

Access Rights Auditor

- Active Directory Explorer.
- User Activity and permissions tracking.
- Suspicious activity monitoring.

Incident response and Endpoint Protection

- Host lockdown, IP block, and remote control console.
- Antivirus, OSSEC and Wazuh Integration

File Clasification

- File Changes and access Tracking.
- Activity monitoring.
- File Integrity monitoring.

Dark Web Monitoring

- Monitor for compromised or stolen employee and customer data.
- Domain and Individual email addresses monitoring.

Threat Intelligence

- Spam, malware, botnets, service abuse IP related.
- Denial of service and Brute force attack and scanner IPs.

Compliance

Compliance with the latest regulations often requires generating reports for internal use and auditors. UTMStack simplifies compliance management by combining essential security tools into a single database and providing several built-in reports and interactive dashboards. It is reinforced by an event and logs explorer for advanced analysis and a report/dashboard builder that helps visualize and display data.

Compliance	Report description
HIPAA	Security management process and audit controls report include accounts validation, relevant security alerts, login reports, relevant windows events, file and system access, cloud reports (Azure, AWS), Office365 threat Intelligence, account validations, firewall relevant activity, relevant system statistics, unsuccessful logon, privilege escalation.
GDPR	Logon Activity, Logon failure, vulnerability report, potential data exposure, relevant Security alerts, data retention, and potential data privacy compromises.
GLBA	§§6801(b)(3) Successful Login / Logoff, §§6801(b)(1) File Access, §§6801(b)(2) Policy Changes in Active Directory, §§6801(b)(2) New and enabled user Accounts in Active Directory, §§501B(2)(3) GLBA Login section
SOC	CC3.2 Assets report, CC3.2 Vulnerabilities report, SOC 2 CC3.2 Network, Host and Cloud Threat detection report

Threat Detection Technology

UTMStack threat detection engine comprises several rule-based correlation systems, scanners, and AI-powered machine learning algorithms. Modules operate independently, and sometimes their functionalities overlap and interact to generate a holistic analysis of events.

Heuristic and Rule-based analysis engine	UTMStack leverages powerful correlation engines for a total of 154 000 detection rules. They aggregate, correlate, and analyze log data, network traffic, and system internal activity generated by on-premises and cloud devices or SaaS.
Machine Learning Anomaly-based engine	Analyzes the environment and defines custom rules and baselines. This learning mechanism allows the system to learn from the environment and gain the ability to identify abnormal and threatening behavior.
Threat Intelligence Database correlation	Analyses all available security IP feeds, mainly related to online attacks, online service abuse, malware, botnets, command and control servers, and other cybercrime activities.

Advanced-Data Visualization and Reporting

Not all environments are the same, and every organization has unique use cases that might customs dashboards and reports. While traditional SIEM solutions usually come with a fixed set of pre-created dashboards and reports intended to fit most clients' most common compliance needs, this is usually not enough. UTMStack dashboards and reports can be created, modified, and deleted without writing a single line of code. The entire solution has been built on a proprietary data visualization and analysis engine that provides the flexibility to build the entire stack from the ground by any advanced user.

The UTMStack data visualization system facilitates managing the following use cases:

Investigate Suspicious Activities

- Aggregate and summarize sets of data.
- Filter, track, and export log data.
- Perform forensic analysis.

Monitor and analyze security data

- Build customized dashboards or use existing ones.
- Explore systems data in near real-time and respond to incidents.

Audit and compliance support

- Generate custom reports for audits or compliance checks and assessments.
- Create compliance dashboards for continuous monitoring
- Leverage existing reports for HIPAA, GLBA, GPDR, and SOC compliance.

Reduce downtime

- Create up-time reports
- Review proactive alerts for misconfigurations or misconfigured systems.
- Monitor and analyze devices performance and resources utilization.

Integrations

UTMStack monitors the following systems and platforms. Integrations can be configured inside the system panel and do not require custom coding or complicated configurations.

- Azure and AWS
- Windows and Linux servers and endpoints
- Hypervisors (KVM, HyperV, VMWare, etc.)
- PaaS and SaaS applications like Office365
- Physical Infrastructure datacenter
- Proprietary devices like CISCO and Sophos
- Software like SharePoint and SQL Server
- Container orchestration (Kubernetes, Docker)

For additional questions, please send an email to support@utmstack.com or start a contact request from our website: https://utmstack.com.