

# SACHET

# BluSapphire

<ul style="list-style-type: none"><li>• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&amp;CK Matrix mapping and highly customizable dashboards through simple configuration.</li></ul>	<ul style="list-style-type: none"><li>• Predictive, Powerful &amp; Scalable Analytics, MITRE ATT&amp;CK Matrix mapping and Rich Customizable Dashboards using simple configurations.</li></ul>
<ul style="list-style-type: none"><li>• Utilizes Big Data Analytics to proactively detect and prioritize threats.</li></ul>	<ul style="list-style-type: none"><li>• Leverages technologies like Advanced AI, ML &amp; Big Data Analytics to detect and prioritize threats.</li></ul>
<ul style="list-style-type: none"><li>• Risk Scoring based on contextual vulnerability and business impact.</li></ul>	<ul style="list-style-type: none"><li>• Real time Correlation of Events, Log Management &amp; Scalable and Flexible Log Collection.</li></ul>
<ul style="list-style-type: none"><li>• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.</li></ul>	<ul style="list-style-type: none"><li>• Support for Integration with third-party cloud APIs to facilitate ingestion of logs.</li></ul>
<ul style="list-style-type: none"><li>• Third-Party Cloud API Integration to streamline log ingestion from external sources.</li></ul>	<ul style="list-style-type: none"><li>• Flexible for Threat Intelligence &amp; other third-party application integrations(Cloud Services, SaaS Apps).</li></ul>

<ul style="list-style-type: none"><li>• Instant IOC Correlation against up to one full year of security telemetry.</li></ul>	<ul style="list-style-type: none"><li>• Infrastructure, Standard/Custom Apps) with 3000+ built-in uses cases.</li></ul>
<ul style="list-style-type: none"><li>• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).</li></ul>	<ul style="list-style-type: none"><li>• 24X7 Live Support is offering by Blusapphire.</li></ul>
<ul style="list-style-type: none"><li>• 24/7 Live Support provided by a dedicated support team.</li></ul>	<ul style="list-style-type: none"><li>• Comprehensive threat detection, investigation and workflow along with rich reporting for compliance use cases.</li></ul>
<ul style="list-style-type: none"><li>• Custom Log Parsing Framework, enabling fast and flexible parsing options.</li></ul>	<ul style="list-style-type: none"><li>• Large Enterprise and Managed Service Provider Ready — “Multi-Tenant Architecture”.</li></ul>
<ul style="list-style-type: none"><li>• Efficient and Scalable Architecture designed for seamless expansion.</li></ul>	<ul style="list-style-type: none"><li>• Easy Scale Out Architecture.</li></ul>
<ul style="list-style-type: none"><li>• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.</li></ul>	<ul style="list-style-type: none"><li>• Out-of-the-Box Compliance Ready &amp; Automated Reporting.</li></ul>

# SACHET

# Google Chronicle

<ul style="list-style-type: none"><li>• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&amp;CK Matrix mapping and highly customizable dashboards through simple configuration.</li></ul>	<ul style="list-style-type: none"><li>• Predefined rules mapped to specific threats, suspicious activity, and security frameworks like MITRE ATT&amp;CK.</li></ul>
<ul style="list-style-type: none"><li>• Utilizes Big Data Analytics to proactively detect and prioritize threats.</li></ul>	<ul style="list-style-type: none"><li>• Risk scoring based on contextual vulnerability, and business risk.</li></ul>
<ul style="list-style-type: none"><li>• Risk Scoring based on contextual vulnerability and business impact.</li></ul>	<ul style="list-style-type: none"><li>• Custom use case building functionality.</li></ul>
<ul style="list-style-type: none"><li>• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.</li></ul>	<ul style="list-style-type: none"><li>• Instant correlation IOCs against one full year of security telemetry.</li></ul>
<ul style="list-style-type: none"><li>• Third-Party Cloud API Integration to streamline log ingestion from external sources.</li></ul>	<ul style="list-style-type: none"><li>• Support for Integration with third-party cloud APIs to facilitate ingestion of logs.</li></ul>

<ul style="list-style-type: none"><li>• Instant IOC Correlation against up to one full year of security telemetry.</li></ul>	<ul style="list-style-type: none"><li>• 24X7 Live support is not offering by Google Chronicle .</li></ul>
<ul style="list-style-type: none"><li>• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).</li></ul>	<ul style="list-style-type: none"><li>• No Option for Live Online and In Person Training.</li></ul>
<ul style="list-style-type: none"><li>• 24/7 Live Support provided by a dedicated support team.</li></ul>	<ul style="list-style-type: none"><li>• Comprehensive threat detection, investigation and workflow along with rich reporting for compliance use cases.</li></ul>
<ul style="list-style-type: none"><li>• Custom Log Parsing Framework, enabling fast and flexible parsing options.</li></ul>	<ul style="list-style-type: none"><li>• Rapidly normalize data with pre-built parsers into a unified data model.</li></ul>
<ul style="list-style-type: none"><li>• Efficient and Scalable Architecture designed for seamless expansion.</li></ul>	
<ul style="list-style-type: none"><li>• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.</li></ul>	

# SACHET

# Fortinet

- Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&CK Matrix mapping and highly customizable dashboards through simple configuration.

- Utilizes Big Data Analytics to proactively detect and prioritize threats.

- Risk Scoring based on contextual vulnerability and business impact.

- Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.

- Third-Party Cloud API Integration to streamline log ingestion from external sources.

- Passive & active discovery methods, use of agents, **FortiGates**, & OT asset management systems.

- Correlation, UEBA ML engine, and over 1600 rules provide robust threat detection.

- FortiAI uses GenAI to guide, simplify, and automate security analyst activities.

- Seamless integration provides extended endpoint investigation and forensic monitoring.

- Security Fabric integration across the Fortinet portfolio, and third-party solutions via robust APIs.

<ul style="list-style-type: none"><li>• Instant IOC Correlation against up to one full year of security telemetry.</li></ul>	<ul style="list-style-type: none"><li>• FortiSIEM as SaaS lets Fortinet take on the burden of deployment and software administration.</li></ul>
<ul style="list-style-type: none"><li>• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).</li></ul>	<ul style="list-style-type: none"><li>• FortiSIEM offers hardware and highly scalable virtual machines for those who prefer these solutions.</li></ul>
<ul style="list-style-type: none"><li>• 24/7 Live Support provided by a dedicated support team.</li></ul>	<ul style="list-style-type: none"><li>• Easy-to-manage automation in a single pane of glass integrates public and private cloud protections.</li></ul>
<ul style="list-style-type: none"><li>• Custom Log Parsing Framework, enabling fast and flexible parsing options.</li></ul>	<ul style="list-style-type: none"><li>• Hybrid approach enables combining SaaS, cloud, VM, and HW in whatever combination you need.</li></ul>
<ul style="list-style-type: none"><li>• Efficient and Scalable Architecture designed for seamless expansion.</li></ul>	<ul style="list-style-type: none"><li>• FortiSIEM's inbuilt CMDB synchs to OT asset systems and uses passive techniques for no-impact discovery, plus Purdue classification context.</li></ul>
<ul style="list-style-type: none"><li>• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.</li></ul>	<ul style="list-style-type: none"><li>• FortiSIEM's lightweight agent is perfect for collecting telemetry to track user behavior anomalies—even when disconnected and working remotely.</li></ul>

# SACHET

# splunk>

<ul style="list-style-type: none"><li>• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&amp;CK Matrix mapping and highly customizable dashboards through simple configuration.</li></ul>	<ul style="list-style-type: none"><li>• Enhanced GUI with dashboards.</li></ul>
<ul style="list-style-type: none"><li>• Utilizes Big Data Analytics to proactively detect and prioritize threats.</li></ul>	<ul style="list-style-type: none"><li>• Faster troubleshooting with instant results.</li></ul>
<ul style="list-style-type: none"><li>• Risk Scoring based on contextual vulnerability and business impact.</li></ul>	<ul style="list-style-type: none"><li>• Best suited for root cause analysis.</li></ul>
<ul style="list-style-type: none"><li>• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.</li></ul>	<ul style="list-style-type: none"><li>• Get access to create dashboards, graphs, and alerts.</li></ul>
<ul style="list-style-type: none"><li>• Third-Party Cloud API Integration to streamline log ingestion from external sources.</li></ul>	<ul style="list-style-type: none"><li>• Enhanced GUI with dashboards.</li></ul>

<ul style="list-style-type: none"><li>• Instant IOC Correlation against up to one full year of security telemetry.</li></ul>	<ul style="list-style-type: none"><li>• Monitor business metrics for informed decision making.</li></ul>
<ul style="list-style-type: none"><li>• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).</li></ul>	<ul style="list-style-type: none"><li>• Log management from multiple sources.</li></ul>
<ul style="list-style-type: none"><li>• 24/7 Live Support provided by a dedicated support team.</li></ul>	<ul style="list-style-type: none"><li>• Accepts data in multiple formats.</li></ul>
<ul style="list-style-type: none"><li>• Custom Log Parsing Framework, enabling fast and flexible parsing options.</li></ul>	<ul style="list-style-type: none"><li>• Can create one central repository for Splunk data collected from multiple sources.</li></ul>
<ul style="list-style-type: none"><li>• Efficient and Scalable Architecture designed for seamless expansion.</li></ul>	
<ul style="list-style-type: none"><li>• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.</li></ul>	

# SACHET

# IBM QRADAR

<ul style="list-style-type: none"><li>• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&amp;CK Matrix mapping and highly customizable dashboards through simple configuration.</li></ul>	<ul style="list-style-type: none"><li>• Intelligent algorithms to apply multiple layers of risk scoring on each observable within a case.</li></ul>
<ul style="list-style-type: none"><li>• Utilizes Big Data Analytics to proactively detect and prioritize threats.</li></ul>	<ul style="list-style-type: none"><li>• All siloed data can be accessed to enrich threat investigations. Federated search provides cost-effective flexibility to choose between what mission- critical data is ingested into SIEM and searching data where it resides.</li></ul>
<ul style="list-style-type: none"><li>• Risk Scoring based on contextual vulnerability and business impact.</li></ul>	<ul style="list-style-type: none"><li>• native support for open source Sigma Rules, cloud- native QRadar SIEM creates a common shared language for security analysts to overcome the challenge of writing rules in proprietary SIEM platforms.</li></ul>
<ul style="list-style-type: none"><li>• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.</li></ul>	<ul style="list-style-type: none"><li>• Reduces analyst fatigue through automation that provides a summary of information and recommendations all in one place.</li></ul>
<ul style="list-style-type: none"><li>• Third-Party Cloud API Integration to streamline log ingestion from external sources.</li></ul>	<ul style="list-style-type: none"><li>• access to the latest evolving trends without having to spend hours on research.</li></ul>

<ul style="list-style-type: none"><li>• Instant IOC Correlation against up to one full year of security telemetry.</li></ul>	<ul style="list-style-type: none"><li>• Automatic enrichment from X-Force Threat Intelligence allows organisations to avoid emerging threats and exposure from the latest vulnerabilities.</li></ul>
<ul style="list-style-type: none"><li>• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).</li></ul>	
<ul style="list-style-type: none"><li>• 24/7 Live Support provided by a dedicated support team.</li></ul>	
<ul style="list-style-type: none"><li>• Custom Log Parsing Framework, enabling fast and flexible parsing options.</li></ul>	
<ul style="list-style-type: none"><li>• Efficient and Scalable Architecture designed for seamless expansion.</li></ul>	
<ul style="list-style-type: none"><li>• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.</li></ul>	

# SACHET

# McAfee

<ul style="list-style-type: none"><li>• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&amp;CK Matrix mapping and highly customizable dashboards through simple configuration.</li></ul>	<ul style="list-style-type: none"><li>• Advanced Correlation Engine supplements with two dedicated correlation engines.</li></ul>
<ul style="list-style-type: none"><li>• Utilizes Big Data Analytics to proactively detect and prioritize threats.</li></ul>	<ul style="list-style-type: none"><li>• Application Data Monitor decodes an entire application session to Layer 7 to detect fraud, data loss, and hidden threats.</li></ul>
<ul style="list-style-type: none"><li>• Risk Scoring based on contextual vulnerability and business impact.</li></ul>	<ul style="list-style-type: none"><li>• Enterprise Log Manager automates log management and analysis for all log types and integrates with Manager for analysis and incident management.</li></ul>
<ul style="list-style-type: none"><li>• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.</li></ul>	<ul style="list-style-type: none"><li>• Hunt faster by searching billions of events in seconds and get immediate access to raw logs for context.</li></ul>
<ul style="list-style-type: none"><li>• Third-Party Cloud API Integration to streamline log ingestion from external sources.</li></ul>	<ul style="list-style-type: none"><li>• Built for big security data.</li></ul>

<ul style="list-style-type: none"><li>• Instant IOC Correlation against up to one full year of security telemetry.</li></ul>	<ul style="list-style-type: none"><li>• Enterprise Security Manager delivers intelligent, fast, and accurate security information and event management (SIEM) and log management.</li></ul>
<ul style="list-style-type: none"><li>• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).</li></ul>	
<ul style="list-style-type: none"><li>• 24/7 Live Support provided by a dedicated support team.</li></ul>	
<ul style="list-style-type: none"><li>• Custom Log Parsing Framework, enabling fast and flexible parsing options.</li></ul>	
<ul style="list-style-type: none"><li>• Efficient and Scalable Architecture designed for seamless expansion.</li></ul>	
<ul style="list-style-type: none"><li>• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.</li></ul>	

# SACHET

# AlienVault

<ul style="list-style-type: none"><li>• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&amp;CK Matrix mapping and highly customizable dashboards through simple configuration.</li></ul>	<ul style="list-style-type: none"><li>• Central monitoring and configuration for Sensors, Agents, and Logger.</li></ul>
<ul style="list-style-type: none"><li>• Utilizes Big Data Analytics to proactively detect and prioritize threats.</li></ul>	<ul style="list-style-type: none"><li>• Over 100 Pre-Defined Compliance &amp; Threat Reports.</li></ul>
<ul style="list-style-type: none"><li>• Risk Scoring based on contextual vulnerability and business impact.</li></ul>	<ul style="list-style-type: none"><li>• spent on creating custom reports by reusing modules of existing reports.</li></ul>
<ul style="list-style-type: none"><li>• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.</li></ul>	<ul style="list-style-type: none"><li>• 3D network and security applications like Geo-location and botnet maps.</li></ul>
<ul style="list-style-type: none"><li>• Third-Party Cloud API Integration to streamline log ingestion from external sources.</li></ul>	<ul style="list-style-type: none"><li>• Multi-Tenant Management.</li></ul>

<ul style="list-style-type: none"><li>• Instant IOC Correlation against up to one full year of security telemetry.</li></ul>	<ul style="list-style-type: none"><li>• Open Extension API.</li></ul>
<ul style="list-style-type: none"><li>• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).</li></ul>	<ul style="list-style-type: none"><li>• Reduces time required to automate security operations.</li></ul>
<ul style="list-style-type: none"><li>• 24/7 Live Support provided by a dedicated support team.</li></ul>	<ul style="list-style-type: none"><li>• Wizard to Create Custom Correlation Rules.</li></ul>
<ul style="list-style-type: none"><li>• Custom Log Parsing Framework, enabling fast and flexible parsing options.</li></ul>	<ul style="list-style-type: none"><li>• Contextual Behavior Analysis.</li></ul>
<ul style="list-style-type: none"><li>• Efficient and Scalable Architecture designed for seamless expansion.</li></ul>	<ul style="list-style-type: none"><li>• Pattern Recognition &amp; Behavior Analysis.</li></ul>
<ul style="list-style-type: none"><li>• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.</li></ul>	<ul style="list-style-type: none"><li>• Interface to Open Threat Exchange.</li></ul>

# SACHET

# Securonix

<ul style="list-style-type: none"><li>• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&amp;CK Matrix mapping and highly customizable dashboards through simple configuration.</li></ul>	<ul style="list-style-type: none"><li>• on-demand scaling and zero infrastructure to manage.</li></ul>
<ul style="list-style-type: none"><li>• Utilizes Big Data Analytics to proactively detect and prioritize threats.</li></ul>	<ul style="list-style-type: none"><li>• Threat Chain Analytics.</li></ul>
<ul style="list-style-type: none"><li>• Risk Scoring based on contextual vulnerability and business impact.</li></ul>	<ul style="list-style-type: none"><li>• More than 500 integrations allow seamless integration and easily ingest of data from a wide variety of sources across hybrid infrastructures.</li></ul>
<ul style="list-style-type: none"><li>• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.</li></ul>	<ul style="list-style-type: none"><li>• Uncover blind spots with built-in API-based integrations with cloud applications, infrastructure, and services.</li></ul>
<ul style="list-style-type: none"><li>• Third-Party Cloud API Integration to streamline log ingestion from external sources.</li></ul>	<ul style="list-style-type: none"><li>• Achieve a fast time to-value with pre-built analytics modules for common threat scenarios.</li></ul>

<ul style="list-style-type: none"><li>• Instant IOC Correlation against up to one full year of security telemetry.</li></ul>	<ul style="list-style-type: none"><li>• Long-Term Search.</li></ul>
<ul style="list-style-type: none"><li>• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).</li></ul>	<ul style="list-style-type: none"><li>• Built-In SOAR.</li></ul>
<ul style="list-style-type: none"><li>• 24/7 Live Support provided by a dedicated support team.</li></ul>	
<ul style="list-style-type: none"><li>• Custom Log Parsing Framework, enabling fast and flexible parsing options.</li></ul>	
<ul style="list-style-type: none"><li>• Efficient and Scalable Architecture designed for seamless expansion.</li></ul>	
<ul style="list-style-type: none"><li>• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.</li></ul>	



**Thank You**

---