Feature set & functionality in hotrock today and planned for future releases

Integrations	
implemented	planned
Logging & event sources - Linux SystemD - Linux STDOUT (incl. containers) - Linux File - Windows EventLog - Windows File - Application – .NET - Database – MSSQL Server/Audit Logs - Generic Network Device (syslog) - Cisco IOS - Cisco ASA - F5 BigIP - Access & Error Logs – IIS - Access & Error Logs – Apache/Tomcat - Linux Performance Metrics - Windows Performance Metrics (WMI) - Cloud – AWS – VPC Flows - Cloud – AWS – CloudWatch / S3 - Cloud – Azure – Cloud-App Security Cloud – Microsoft 365 Security	Elastic APM integration (initial support for Ruby, .NET, Java and Node) Logging & event sources - Cloud-based objects - Appliances - Storage devices - Palo Alto Firewall - Application-layer transaction logs - Various API integrations - Application – Java/Log4J - Application – Ruby/Rails - Message Queue – Kafka/JMS Performance metrics ingestion and dashboard updates/tuning for time-series data - Metric Beat - APM SaaS - NewRelic, Datadog, AppDynamics - AWS Cloudwatch Metrics - Azure Monitor - GCP Metrics / Stackdriver API worker orchestrator/scraping Extend cloud integration capability - Azure – CAS, Sentinel - GCP - Cloud Security Command Center - Extending AWS support (Security Hub) Ability to integrate with other SIEM/Log management platforms Packet Sniffing RSS Feeds

Feature set & functionality in hotrock today and planned for future releases

Security	
implemented	planned

• End-to-end encryption support
• Role-based access control
• SIEM-type functionality
• Alerting (email or API)
• Customized security (authentication, authorization)
• Agents
  • OSSEC
  • Windows Defender (via Microsoft Advanced Threat Protection)
	• Multi-tenancy use cases
	• Customizable rules engine (Elastic SIEM or other)
	• Data Localization – Query multiple ElasticSearch in different regions/countries to keep GDPR-protected data local.
	• Integration of a complex correlation engine
	• TIP's integration (Threat Intelligence Platforms)
	• Agents
	  • CloudStrike
	  • McAfee
	  • Norton

Visualization	
implemented	planned

• Data flow diagrams
• Kibana dashboard templates
• Customized dashboards
• Data transformation/classification
	• Machine Learning
	  • Anomaly Detection
	  • CarbonBlack

Distribution	
implemented	planned
• Fully Automated Deployment (infrastructure-as-code) • Deploys to AWS and VMware vCenter (on-prem) • Capacity analysis / requirements • Bursting solutions (automatic up/down scaling) (*except for data nodes)	• Deploys to Azure, Google, GCP • Aggregator and agent conf management, registration and update API