trapp TECHNOLOGY SM

ArmorPoint Product Details

ArmorPoint's intrusion detection, behavioral monitoring, SIEM correlation, and log management capabilities.

ArmorPoint Level of Security

Feature	Details	
24x7x365 Live Network Monitoring	24x7x365 live monitoring tool that logs various points across the customers' network, depending on their desired level of security.	✔
Cloud and On-Premise Resource Monitoring	Supports monitoring for AWS, Azure, etc. as well as physical devices within the network.	✔
NOC and SOC Analytics	The analytics traditionally monitored in separate silos — SOC and NOC — brought	✔

	together through one pane of glass for a more holistic view of the security and availability of the business.	
Performance Monitoring	Establish metrics and detect significant deviations. Gives the ability to monitor performance at the system, application, virtualization, and database level.	Available
Availability Monitoring	Ability to monitor various systems' up/down/availability.	Available
Distributed Real-Time Event Correlation	Complex event patterns can be detected in real time, allowing ArmorPoint to handle a large number of rules at high event rates for accelerated detection timeframes.	✔
Real-Time Automated Network Topology Discovery	Intelligent infrastructure and application discovery engine that is able to discover and map the topology of both physical and virtual infrastructure as well as on-premises and in public/private clouds, simply using credentials without any prior knowledge of what the devices or applications are.	✔
Real-Time Application Discovery Engine (CMDB)	An up-to-date CMDB (Centralized Management Database) enables sophisticated context-aware event analytics using CMDB Objects in search conditions.	✔
Real-Time Configuration Change Monitoring	Automated detection of changes in network configuration, installed software, file/folders, and windows registries.	Available
Dynamic User Identity Mapping	Users and their roles are discovered from on-premises or Cloud SSO repositories. Network identity is identified from important network events. Then geo-identity is added to form a dynamic user identity audit trail. This makes it possible to create policies or perform	✔

	investigations based on user identity instead of IP addresses — allowing for rapid problem resolution.	
Custom Log Parsing Framework	XML-based event parsing language that is functional like high level programming languages and easy to modify yet can be compiled during run-time to be highly efficient, parsing beyond 10K EPS per node.	✔
Default Dashboards		✔
Rich Customizable Dashboards	Configurable real-time dashboards, with “Slide-Show” scrolling for showcasing KPIs. Ability to layer dashboards for business services, virtualized infrastructure, and specialized apps. Enables association of individual components with the end-user experience that they deliver together providing a powerful view into the true availability of the business.	Available
User and Entity Behavior Analysis	Predefined correlation rules as well as more advanced machine learning help identify insider and incoming threats that pass traditional defenses. High fidelity alerts raise the profile of high priority actions identified within the organization.	✔
External Threat Intelligence Integrations	Threat intelligence analysts track and share trends in global cybercriminal operations to discover and study emerging threats, then automatically implement protections against those threats.	✔
Out-of-the-Box Compliance Reports	Access to pre-defined reports supporting a wide range of compliance auditing and management needs including PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13,	Available

	SANS Critical Controls	
Powerful and Scalable Analytics	Robust search capabilities to schedule reports and deliver relevant results via email to key stakeholders	✔
Baselining and Statistical Anomaly Detection	Baseline endpoint/server/user behavior — hour of day and weekday/weekend granularity, with any set of keys and metrics able to be "baselined." Built-in and customizable triggers on statistical anomalies.	✔
External Technology Integrations	Extensive API-based integrations to streamline multiple tools or platforms	Available
Simple and Flexible Administration	Web-based GUI with role-based controls to deliver powerful platform management.	✔
Scale Out Architecture	ArmorPoint flexible/scalable infrastructure scales with your growing company.	✔
Two-Factor Authentication		Available
Advanced Agent Monitoring	High-performance and expanded data collection. Agentless technology combined with high performance agents for Windows and Linux to significantly bolster its data collection	Available

Choose the level of service that fits your company's needs for managed incident response. **Items in red** indicate managed

services that would occur in the event of an active incident.

ArmorPoint Level of Service

Feature	Details	ArmorPoint Report	ArmorPoint Edge	ArmorPoint 360˚
Basic Reporting	Access to robust search capabilities to schedule reports and deliver relevant results via email to key stakeholders	✔	✔	✔
Customized Reporting	ArmorPoint Security Analysts interface with key stakeholders to determine most relevant reports to deliver on a scheduled basis.	✔	✔	✔
Human Analysis of Events	GIAC-certified Security Operations Center analysts provide 24x7x365 security monitoring, carefully vetting alert notifications	✔	✔	✔
Incident Notification Within 15 Minutes	Once identified as a valid threat, ArmorPoint Security Analysts issue a notification within 15 minute SLA	✔	✔	✔
Remediation Planning	Expert recommendations to isolate, remediate, and restore environment from an incident	✔	✔	✔

Active Threat Containment	Identify and block active threats at the network edge		✔	✔
> Automated Incident Management	When an incident is triggered, an automated script runs to mitigate or eliminate the threat.		✔	✔
> Block Malicious IP Traffic	Prevent the flow of traffic from the IP address of known threats		✔	✔
> Block Malware Domain	Proactive defense against malware domains named on industry-leading blocklists		✔	✔
> Block Compromised Device Network Activity	Identify and block network activity by quarantining and isolating the compromised device.			✔
> Incident History	View ticket history of threats detected, analyzed, and mitigated by ArmorPoint Security Analysts	✔	✔	✔
> Remote Incident Response Services	Available hours to utilize ArmorPoint Security Analysts resources for incident response.		10 hours per month	20 hours per month
Active Threat Mitigation	Identify, block, and remediate active threats within the network down to the endpoint.			✔
> Software Updates and Patching	Apply software updates as necessary to approved Microsoft and Linux products and services. Third party software patches applied on a case-by-case basis.			✔
> Virus and	Remove malicious software			✔

Malware Detection and Removal	when detected.	
> Firewall Management	Optimize firewall for highest level of protection possible through rule-based parameters gathered from current threat intelligence data	✔
> Threat Isolation at the Endpoint	Identify, isolate, and remediate active threats down to the endpoint, preventing the further spread of a virus or malicious process.	✔
> User Account Lockdown	Disable or de-authenticate compromised user accounts to prevent the spread of active threats	✔
> Network Access Control Integration	Integration of policies for controlling devices and user access to the network.	✔
> Disable Switch Ports	Secure switch ports to prevent compromise and prevent malicious actors from entering your network	✔
> Environment Hardening	Provide recommendations for industry best practices to network to improve overall security posture	✔
> Root Cause Analysis	Provide an in-depth report detailing the root cause analysis of an incident.	✔