stealthentry

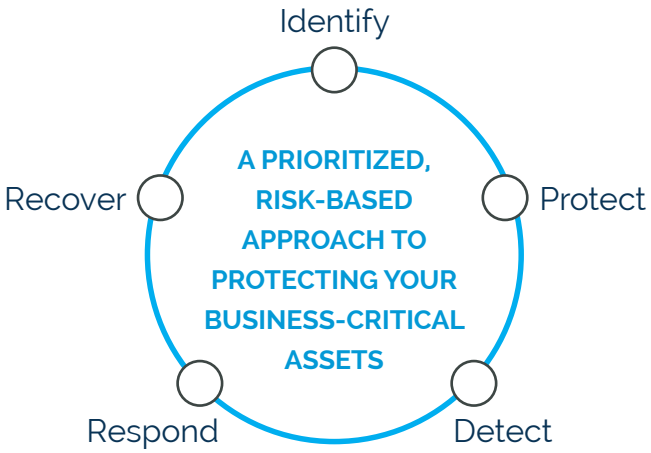
DATASHEET

Cyber Security as a Service (CSaaS) powered by ArmorPoint

ArmorPoint Manged SIEM

Cyber Security as a Service (CSaaS) powered by **ArmorPoint** enables you to leverage new technologies that automatically and proactively identify, monitor, alert, and guide responses to resolve systems and security issues, freeing up staff time for higher-value activities related to investigating, planning, and delivering new revenue-generating and even business-changing services built on new technologies.

A SIEM solution is powerful – it enables companies to gain the visibility, correlation, and automated response needed to safeguard their business-critical assets and protect themselves from exposure to malicious actors. But with great capabilities comes a significant financial investment and an equally difficult path to implementation. To heighten the barrier to entry, many organizations either don't have the in-house IT staff needed to monitor, maintain, and analyze the data collected, or they lack the skills or time needed to get the most value from the SIEM. This leaves organizations in need of an affordable solution without compromise when it comes to service and security.



ArmorPoint

Solve Multiple Business Challenges with One Solution

Stealth Entry combines the intrusion detection, behavioral monitoring, SIEM correlation, and log management capabilities of a SIEM with the intelligence and 24/7 availability of our team of security experts. This unique pairing of monitoring and hands-on managed services provides the analytics and expert intervention needed to improve incident response and stop breaches before they occur.

- Asset Self-Discovery
- Real-time Data Collection and Storage
- Compliance Management
- Threat Detection, Analysis, and Response
- NOC and SOC Analytics
- Performance Availability Monitoring
- Platform Administration and Management
- Active Threat Remediation

Highlights

UNIFIED NOC AND SOC ANALYTICS

ArmorPoint utilizes an architecture that enables unified data collection and analytics from diverse information sources including logs, performance metrics, SNMP Traps, security alerts and configuration changes. ArmorPoint essentially takes the analytics traditionally monitored in separate silos from — SOC and NOC — and brings that data together for a more holistic view of the security and availability of the business. Every piece of information is converted into an event which is first parsed and then fed into an event- based analytics engine for monitoring real-time searches, rules, dashboards and ad-hoc queries.

DISTRIBUTED REAL-TIME EVENT CORRELATION

Distributed event correlation is a difficult problem, as multiple nodes have to share their partial states

in real time to trigger a rule. While many SIEM vendors have distributed data collection and distributed search capabilities, ArmorPoint boasts a distributed real-time event correlation engine, meaning complex event patterns can be detected in real time. This patented algorithm enables ArmorPoint to handle a large number of rules in real time at high event rates for accelerated detection timeframes.

DYNAMIC USER IDENTITY MAPPING

Crucial context for log analysis is connecting network identity (IP address, MAC Address) to user identity (log name, full name, organization role). This information is constantly changing as users obtain new addresses via DHCP or VPN. ArmorPoint's dynamic user identity mapping methodology enables the discovery of users and their roles 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

Effective log parsing requires custom scripts but those can be slow to execute, especially for high volume logs like Active Directory, firewall logs, etc. Compiled code on the other hand, is fast to execute but is not flexible since it needs new software releases. ArmorPoint's XML-based event parsing language functions like high level programming languages and easy to modify, yet can be compiled during run-time to be highly efficient. All ArmorPoint parsers go beyond most competitor's offerings using this patented solution and can be parsed at beyond 10K EPS per node.

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.

AUTOMATED INCIDENT MITIGATION

When an Incident is triggered, an automated script can be run to mitigate or eliminate the threat. Built- in scripts support a variety of devices including Fortinet, Cisco, Palo Alto and Window/Linux servers. Built-in scripts can execute a wide range of actions including disabling a user's Active Directory account, disabling a switch port, blocking an IP address on a Firewall, deauthenticating a user on a WLAN Access Point, and more. Scripts leverage the credentials that have already been generated in the ArmorPoint CMDB. Administrators can easily extend the actions available by creating their own scripts.

INFUSION OF SECURITY INTELLIGENCE

Threat Intelligence and Indicators of Compromise (IOC) and Threat Intelligence (TI) feeds from commercial, open source and custom data sources integrate easily into the security TI framework. This grand unification of diverse sources of data enables organizations to rapidly identify root causes of threats, and take the steps necessary to remediate and prevent them in the future.

Features

REAL-TIME OPERATIONAL CONTEXT FOR RAPID SECURITY ANALYTICS

- Continually updated and accurate device context — configuration, installed software and patches, running services
- System and application performance analytics along with contextual inter-relationship data for rapid triaging of security issues
- User context, in real-time, with audit trails of IP addresses, user identity changes, physical and geo-mapped location
- Detect unauthorized network devices, applications, and configuration changes

AVAILABILITY MONITORING

- System up/down monitoring — via Ping, SNMP, WMI, Uptime Analysis, Critical Interface, Critical Process and Service, BGP/OSPF/EIGRP status change, Storage port up/down
- Service availability modeling via Synthetic Transaction Monitoring — Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP,
- FTP, JDBC, ICMP, trace route and for generic TCP/UDP ports
- Maintenance calendar for scheduling maintenance windows
- SLA calculation — "normal" business hours and after-hours considerations

REAL-TIME CONFIGURATION

- Change Monitoring Collect network configuration files, stored in a versioned repository
- Collect installed software versions, stored in a versioned repository
- Automated detection of changes in network configuration and installed software Automated detection of file/folder changes — Windows and Linux — who and what details Automated detection of changes from an approved configuration file
- Automated detection of windows registry changes via Advanced Agent Monitoring.

NOTIFICATION AND INCIDENT MANAGEMENT

- Policy-based incident notification framework Ability to trigger a remediation script when a specified incident occurs
- API-based integration to external ticketing systems — ServiceNow, ConnectWise, and Remedy
- Built-in ticketing system
- Incident reports can be structured to provide the highest priority to critical business services and applications
- Trigger on complex event patterns in real time

RICH CUSTOMIZABLE DASHBOARDS

- Configurable real-time dashboards, with "Slide-Show" scrolling for showcasing KPIs
- Sharable reports and analytics across organizations and users
- Specialized layered dashboards for business services, virtualized infrastructure, and specialized apps

Features

EXTERNAL THREAT INTELLIGENCE INTEGRATIONS

- API's for integrating external threat feed intelligence — Malware domains, IPs, URLs, hashes, Tor nodes
- Built-in integration for popular threat intelligence sources — ThreatStream, CyberArk, SANS, Zeus
- Technology for handling large threat feeds — incremental download and sharing within cluster, real-time pattern matching with network traffic. All STIX & TAXII feeds are supported

POWERFUL AND SCALABLE ANALYTICS

- Search events in real time — without the need for indexing
- Keyword and event-based searches
- Search historical events — SQL-like queries with Boolean filter conditions, group by relevant aggregations, time-of-day filters, regular expression matches, calculated expressions — GUI & API
- Use discovered CMDB objects, user/identity and location data in searches and rules
- Schedule reports and deliver results via email to key stakeholders
- Search events across the entire organization, or down to a physical or logical reporting domain
- Dynamic watch lists for keeping track of critical violators — with the ability to use watch lists in any reporting rule
- Scale analytics feeds by adding Worker nodes without downtime

CONFIDENCE IN INCIDENT RESPONSE

- Remote incident response performed by ArmorPoint Security Analysts
- Malware Detection and Removal
- Automated incident management and threat elimination
- Block malicious IP traffic stemming from known threats
- Isolation of a compromised device
- Active threat remediation down to the endpoint Expert-led root cause analysis

SIMPLE AND FLEXIBLE ADMINISTRATION

- Web-based GUI
- Rich Role-based Access Control for restricting access to GUI and data at various levels
- All inter-module communication protected by HTTPS
- Full audit trail of user activity
- Rapid updates to knowledge base (parsers, rules, reports)
- Policy-based archiving
- Hashing of logs in real time for non-repudiation & integrity verification
- Flexible user authentication — local, external via Microsoft AD and OpenLDAP, Cloud SSO/SAML via Okta
- Ability to log into remote server behind a collector from GUI via remote SSH tunnel

EXTERNAL TECHNOLOGY INTEGRATIONS

- Integration with any external web site for IP address lookup
- API-based integration for external threat feed
- intelligence sources
- API-based 2-way integration with help desk systems — seamless, out-of-the box support for ServiceNow, ConnectWise and Remedy
- API-based 2-way integration with external CMDB Kafka support for integration with enhanced Analytics Reporting — i.e. ELK, Tableau and Hadoop
- API for easy integration with provisioning systems API for adding organizations, creating credentials, triggering discovery, modifying monitoring events

Refocus internal teams while reducing your overall risk.

Organizations know that digitalization has the potential to transform their business. But lack of time, and expertise more often hinder IT teams from planning for such an ambitious future. In fact, in its annual CIO survey, IDG found that 72% of respondents struggle to juggle business innovation and operational excellence requirements. And the number of challenges isn't decreasing: 87% said they are increasing. What's needed is a way to free up time for overburdened IT teams that often handle IT support, security and even compliance in many cases.

INCREASING PRODUCTIVITY THROUGH TOOLS AND MANAGED SERVICES

An effective way to create time to develop new staff skills and tackle strategic projects is to automate time-consuming tasks that take significant human effort. Specifically, introducing strategic managed services partners and tools to monitor IT, security and compliance, proactively identify issues before they become major problems and even streamline resolution can free up individuals to focus on higher value activities.

Finding the Right Plan

ArmorPoint is a two-part security solution, comprised of a level of security and a level of service that reduces your costs while maximizing value.

REPORT

Monitoring and Reporting

FOR ORGANIZATIONS WITH

- Dedicated IT security staff
- Minimal compliance requirements

LEVEL OF SECURITY

- 24/7/365 Monitoring
- NOC and SOC Analytics
- Real-time Asset Discovery
- Distributed Event Correlation
- Dashboards
- User and Entity Behavior Analysis
- Threat Intelligence Integration

LEVEL OF SERVICE

- Basic Reporting
- Human Analysis of Events
- Incident Notification SLA
- Incident History
- Remediation Recommendations

EDGE

Managed Response to Network Edge

FOR ORGANIZATIONS WITH

- Some IT security staff
- Managed services provider

LEVEL OF SECURITY

- 24/7/365 Monitoring
- NOC and SOC Analytics
- Real-time Asset Discovery
- Distributed Event Correlation
- Dashboards
- User and Entity Behavior Analysis
- Threat Intelligence Integration

LEVEL OF SERVICE

- Customized Reporting
- Automated Incident Management
- Human Analysis of Events
- Incident Notification SLA
- Incident History
- Remediation Planning
- Threat Remediation to Network Edge
- 10 Hours of Remote Incident Response Services per Month
- Root Cause Analysis

360°

Managed Response to the Endpoint

FOR ORGANIZATIONS WITH

- Little to no IT staff
- Strict compliance requirements

LEVEL OF SECURITY

- 24/7/365 Monitoring
- NOC and SOC Analytics
- Real-time Asset Discovery
- Distributed Event Correlation
- Dashboards
- User and Entity Behavior Analysis
- Threat Intelligence Integration

LEVEL OF SERVICE

- Customized Reporting
- Automated Incident Management
- Human Analysis of Events
- Incident Notification SLA
- Incident History
- Remediation Planning
- Threat Remediation to the Endpoint
- 20 Hours of Remote Incident Response Services per Month
- Root Cause Analysis

Why STEALTH CSaaS?

SCALABLE

Gain the ability to collect, parse, normalize, index, and store hundreds of thousands of events per second, with a foundation to support future needs from IoT to our cloud.

SECURE

Rapid detection and response to security, performance and compliance threats with ArmorPoint's robust analytics dashboards

AWARE

Accurate detection of devices, systems, hardware, software, running services, applications, storage, users, network configuration, network topology and device relationships

ACTIONABLE

Identify and remediate root causes of threats with ArmorPoint's pre-built and customizable reports for security and compliance

OPEN

Integrate hundreds of devices, common applications, and third party threat feeds data through native and API connectors

AFFORDABLE

Proactive protection your sensitive data without buying expensive hardware and hiring more staff

stealthentry

To build a CSaaS solution that is customized to your business needs, contact Stealth Entry Technology representative at
sales@stealthentry.com • 833.423.2927 • stealthentry.com