The Cybersecurity Problem

- A severe lack of cybersecurity talent is one of an organization’s greatest vulnerabilities.
- Regulated companies face a rapidly growing and changing regulatory environment and the costs to maintain compliance are skyrocketing.
- Vendor consolidation could reduce costs, increase efficiency and enhance ease of use.
- Legacy systems are a security weak link because the software has reached end-of-life and is no longer supported.
- Data requiring analysis never shrinks making SIEMs a necessity but the increasing cost of SIEMs is a challenge for large and small organizations alike.

What is Atomic Workload Protection?

Atomic Workload Protection (AWP) is a multi-platform endpoint protection / endpoint detection solution that eliminates the complexity and burden of cybersecurity and compliance across on-premise, cloud and hybrid infrastructures. Harnessing the power of Open Source Security (OSSEC) and proprietary machine learning, AWP aggregates and correlates data across the enterprise to automatically provide high fidelity active response, threat detection and recovery.
Automatic Compliance, Auditing and Alerting

AWP automates compliance tasks associated with all major regulatory requirements including PCI-DSS, HIPAA, GDPR, NIST, SOX, ISO, CIS, FISMA and JSIG.

There are numerous compliance solutions available today but they are costly and often meet only a portion of regulatory requirements. AWP, for example, meets every PCI-DSS control that can be automated by software, eliminating the need for multiple solutions. AWP is quickly installed with minimal staff, highly effective in determining compliance issues, cost effective and offers a flexible licensing model.

Lowering Escalating SIEM Costs

Many SIEM vendors charge based on log or data volume, and their customers experience rapid, large cost increases as a result. The amount of data never shrinks. Small to mid-size organizations, particularly those in regulated industries, can’t afford the cost of a SIEM and yet they still have to adhere to the same security requirements as larger companies.

Logging data and alert avalanche, in addition to continually growing SIEM charges, is a challenge. AWP significantly reduces the amount of information to just what is relevant and quickly determines the cause of an issue. AWP provides a high-fidelity filter between data sources and the SIEM. Customers have experienced up to an 80% reduction in SIEM costs by running their SIEM data feeds through AWP without the loss of key information. AWP automatically integrates out-of-the-box with all major SIEMs in their proprietary formats.

Maximizing Cybersecurity Talent

Never before has there been such a need for cybersecurity talent. It is difficult to find and retain. Because of that, it is also expensive. AWP provides automated intelligent detection and response for a multitude of platforms, clouds, and legacy systems. Many solutions collect large amounts of data that require numerous cybersecurity analysts to assimilate the sources and determine if an issue exists; let alone determine a correct path to quickly mitigate risk. AWP provides automated assessment, intelligent learning, real-time active response and machine generated updates to respond to and prevent malicious activity across platforms; long before a human analyst could have detected, diagnosed and mitigated a problem. AWP users experience faster and more efficient response without the need for more cybersecurity staff.

Securing Legacy Systems

AWP was designed for a multitude of platforms, including legacy systems and has a very small footprint. The endpoint agents run on almost every operating system including Linux, Windows, Solaris, AIX, HP-UX, OSX, MacOS, and BSD. They also run on every platform: Intel, AMD, ARM, RISC, and SPARC; and in any environment, providing automated security for legacy systems that are no longer supported.
One Enterprise Solution Saves Money and Enhances Efficiency

AWP includes a central role-based Management Interface for log and event visualization, event detail analysis and investigation and system configuration and maintenance, enterprise-wide. It is easy to use and platform agnostic allowing you to control all assets from one console, across every environment and cloud provider eliminating the need for multiple vendor solutions.

Summary

Whether you are challenged by regulatory requirements, escalating security costs, finding and retaining security talent, or securing legacy systems that have reached end-of-life, AWP is a solution that you should not overlook. Developed to extend the power of OSSEC, AWP is multi-platform and supports every infrastructure implementation, aggregating and correlating data to provide threat detection, active response and remediation at a very affordable price.

About Atomicorp

Atomicorp eliminates the complexity and burden of cybersecurity and compliancy across cloud infrastructures through its comprehensive, multi-layered cloud and server protection platform. Harnessing the power of Open Source Security (OSSEC) and proprietary machine learning, Atomicorp aggregates and correlates data across the enterprise to automatically provide high fidelity active response and recovery. And, Atomicorp enables organizations to maximize their cybersecurity resources to better address today’s rapidly evolving threat environment. From end-of-support to cutting edge systems, Atomicorp has the flexibility to provide security and compliancy to any organization. Atomicorp protects thousands of customers within retail, media, healthcare, insurance, and government institutions worldwide.