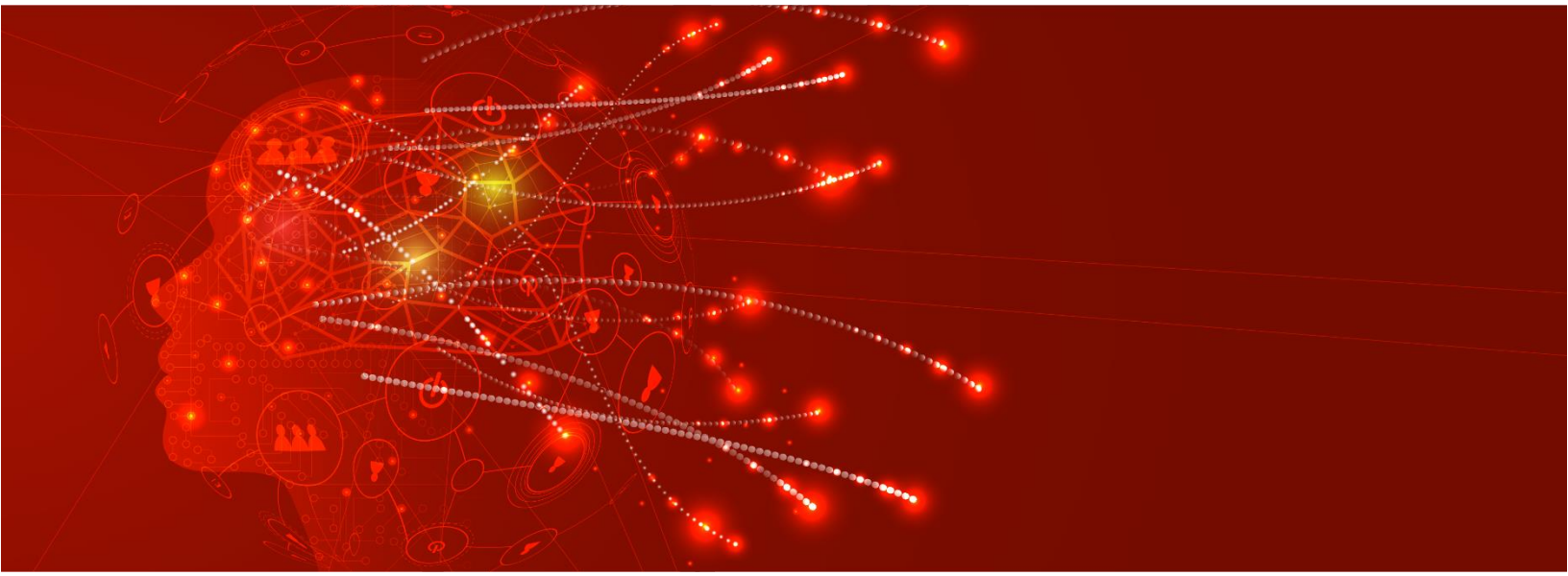
Whitepaper

CyberStack Crisper: Unified Endpoint Security



Challenges in Endpoint Security

In the modern threat landscape, attacks happen at dizzying speed and volume. While AI and machine learning have empowered many organizations to increase efficiency and innovate, they have also empowered attackers to be more effective. This likewise requires incorporating AI, machine learning and automation when preventing, detecting and responding to threats. Traditional approaches centre on indicators of compromise (IOC), signatures for specific threats. IOCs change constantly and an approach centred around behavioural analysis is needed to build on traditional methods.

Endpoint security has often been addressed with a series of standalone tools, each dealing with a particular problem. Often, this approach creates situations where SOC teams would need to stitch together their solutions to ensure that telemetry could be properly correlated. Issues with compatibility prevent teams from realizing a superior security posture.

Even the best endpoint detection and response (EDR) solutions can fail. Attackers can evade prevention, detection and response through techniques that can blend in with system behaviour, subvert the detection logic or even disrupt communications between the endpoint and the EDR server(s).

Moving Forward

A unified approach to endpoint security is required that bundles several key functionalities into one stack. This approach will improve threat prevention, detection and response by consolidating tools, providing more visibility over your systems and improve your security posture.

Integrated Security: Combine Extended detection and response (XDR), which includes Endpoint Detection and Response (EDR), Network Detection and Response (NDR), and Security Information and Event Management (SIEM) to ingest logs from numerous sources, then analyze, aggregate, and correlate logs to detect suspicious activity. This unified approach provides a comprehensive view of your security landscape, eliminating blind spots and enabling you to identify potential threats that might otherwise remain undetected. Furthermore, by correlating data from various

sources, a Unified Endpoint Security solution (UES) can prioritize high-risk events and provide valuable context for security analysts, allowing for faster and more effective incident response.

Machine Learning: UES solution can integrate with existing machine learning and artificial intelligence (AI) tools to facilitate advanced anomaly and behavior detection. This enhances mean time to respond (MTTR) and enables the detection of threats that might otherwise go unnoticed. Machine learning algorithms continuously adapt to evolving threat landscapes, detecting subtle behavioral anomalies that could signal a potential attack. Additionally, UES can leverage machine learning for automated threat analysis, allowing security professionals to prioritize investigations, strategic responses, and security optimization.

Automation: Ensure that simple responses, such as disabling an account or blocking an IP address on an Endpoint can be carried out automatically in response to IOCs or suspicious behaviour. This reduces alert fatigue for your security team by automating repetitive tasks and ensures a swift response to identified threats. Furthermore, automation within a UES solution can streamline incident containment, automatically isolating compromised endpoints to prevent lateral movement and minimize the potential impact of an attack.

Crisper Unified Endpoint Security

Empower your security strategy with Casper Unified Endpoint Security, the next generation of endpoint protection. Casper UES seamlessly integrates the functionality of EDR, NDR, and SIEM into a single stack, providing comprehensive protection for endpoints and your overall network. This unified approach eliminates data silos and streamlines security operations, enhancing threat detection, response efficiency, and simplifying your security infrastructure. Casper UES secures organizations with endpoint protection for your devices, coupled with network device log ingestion, analysis, and correlation in the built-in SIEM. Centralized management of all security controls simplifies security posture maintenance and reduces the Total Cost of Ownership (TCO).

Gain a deep understanding of your security posture with vulnerability scanning, security configuration assessments (SCA), and compliance reporting. Casper's vulnerability scanning module provides an up-to-date view of vulnerabilities on your endpoints, powered by the NIST Vulnerability database, common vendor repositories, and custom vulnerability feeds. The SCA module uses CIS benchmarks to score and track endpoint configurations, highlighting potential security weaknesses. Compliance reporting for frameworks such as GDPR or NIST 800-53 helps identify non-compliant areas, ensuring a strong security posture and avoiding regulatory penalties.

Casper UES leverages comprehensive log collection for threat detection, alongside endpoint agents that can automatically trigger actions like malicious file deletion and suspicious connection blocking. Advanced detections for rootkits and ransomware protect against elevated access and compromised data. Casper UES also provides EDR (Endpoint Detection and Response) capabilities for in-depth investigation, compromised device isolation, and rapid threat containment. This layered approach ensures that even if a threat bypasses initial defenses, the UES solution can still mitigate the damage and minimize the attack impact.

Featured Highlights

- **Integrated SIEM, EDR and NDR:** Casper UES incudes the functionality of EDR, NDR and SIEM to ingest, analyze, aggregate and correlate logs for malicious signatures and behaviours. Casper responds to suspicious events to protect your assets.
- **File Integrity Monitoring:** Casper scans endpoints to track users, permissions and files (through hashes) to detect suspicious file changes.
- **Vulnerability Assessment:** Regular scans on your endpoints detect vulnerabilities with data sourced from the NIST Vulnerability Database, Microsoft and Canonical. Vulnerabilities are assigned scores and severity (Critical, High, Medium, etc.) so your team can prioritize remediation.
- **Malware and Malicious Behaviour Detection:** Rulesets are constantly updated to detect attacks, malware, policy violations and malicious activity with advanced detection capabilities to prevent ransomware execution on your endpoints. Threats are mapped to relevant MITRE ATT&CK TTPs to better understand and mitigate them.
- **Security Configuration Assessment:** The UES provides a report for each endpoint based on CIS benchmarks assessing their overall security configuration with a score as well as listing vulnerabilities and misconfigurations as well as their severity.

- **Automated Incident Response:** Casper will automatically respond to security incidents upon detection by deleting malicious files, blocking suspicious connections, isolating compromised endpoints and more.
- **Real Time Alerting:** Receive real-time alerts and notifications from the UES when security incidents occur so that your security team can take on more complex security events. The platform offers integrations for ticketing platforms and threat intelligence to enhance incident response.
- **Cloud Container Security:** Casper has integrations for AWS, Google and Azure as well as other cloud services to ensure you gain visibility over and protect your cloud containers and workloads.
- **Compliance Reports:** Casper UES comes preloaded with regulatory frameworks such as GDPR and NIST 800-53 to assess regulatory compliance. You can also create custom compliance frameworks to ensure your environment complies with internal policies.

Why Casper UES?

Unified Endpoint Security consolidates your endpoint security stack by combining the capabilities of endpoint protection platform (EPP), endpoint detection and response (EDR), network detection and response (NDR), and security information and event management (SIEM) into a single, unified platform. This consolidation eliminates the need to manage a disjointed collection of tools from various vendors, streamlining security operations and reducing overall complexity. Traditional security solutions often require complex integrations between disparate tools, introducing potential vulnerabilities and hindering effective threat management. The Casper UES approach offers a single point of control, simplifying security administration and fostering a more holistic view of your security posture. This unified approach empowers your security team to investigate and respond to threats more efficiently, improving your overall incident response time and effectiveness.

Integrated Security Tools

Casper UES takes a comprehensive approach to data collection, ingesting data from a wide range of sources including endpoint devices (Windows, Linux, or macOS) and network devices (routers, switches, firewalls, etc.). This ensures that no potential security indicators are missed. The data collected is then fed into the integrated SIEM for advanced analysis and correlation. By correlating events from various sources, Casper UES can identify subtle patterns and connections that might otherwise be overlooked. This advanced threat detection capability allows security teams to detect suspicious events and behaviors with greater accuracy, enabling them to proactively identify and address potential security incidents before they escalate into major breaches.

Understand your Security Posture

The vulnerability detector and security configuration scans within Casper UES proactively detect vulnerabilities, weaknesses, misconfigurations, and other threats on your endpoints. These scans go beyond a one-time assessment, offering continuous monitoring of your endpoint configurations to identify any potential drifts or security posture degradation over time. Additionally, Casper UES regularly scans your endpoints for compliance with industry-standard frameworks such as HIPAA, NIST, and CIS. These comprehensive scans not only identify gaps but also provide valuable context. Detailed reports and analysis are generated, highlighting vulnerabilities, compliance shortcomings, and offering prioritized recommendations for hardening your systems. By following these recommendations, you can effectively reduce your attack surface and significantly improve your overall security posture.

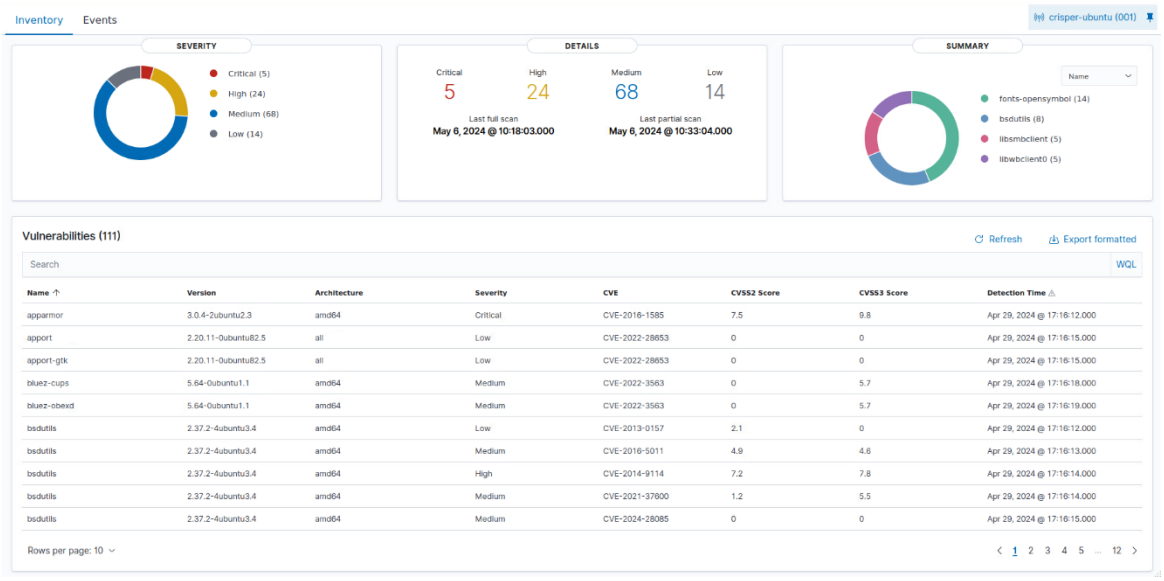


Figure 1: Vulnerability Scanning Module

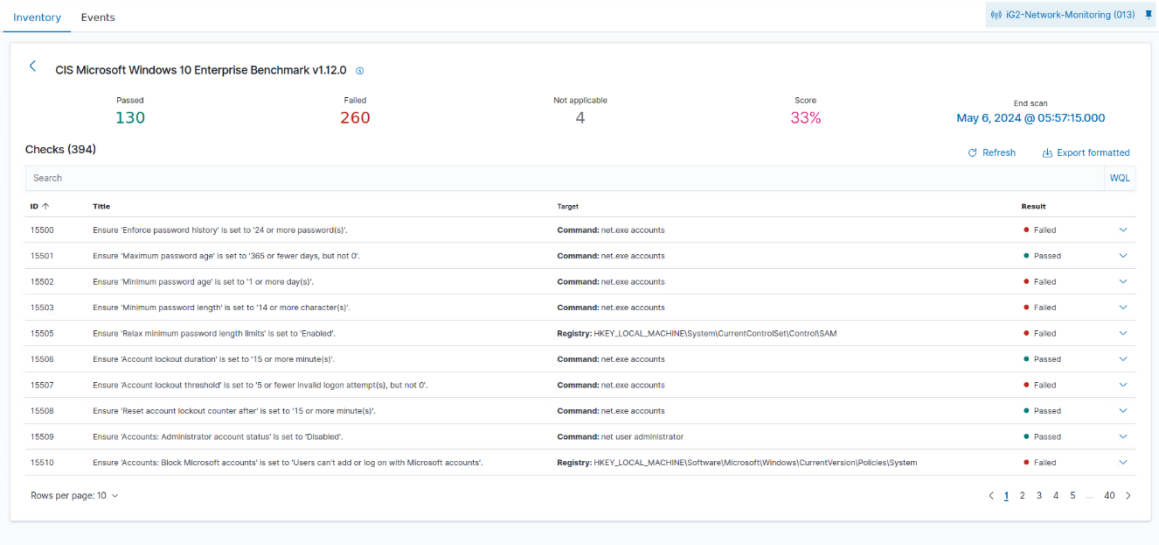


Figure 2: Security Configuration Assessment

Threat Detection and Response

Casper UES rulesets are regularly updated to detect malicious attacks, malware, policy violations and anomalous activity with the option to set custom rules for malware signatures and malicious behaviour. Combine this built in capability with a threat intelligence feed and extensions for tools such as Windows Defender, YARA and VirusTotal to increase your ability to detect malware. The UES uses rootcheck and file integrity monitoring to monitor endpoints for covert processes, unusual permissions, anomalous files and other inconsistencies. The solution also uses advanced detection for ransomware attacks to prevent them from being carried out on endpoints. Events from multiple log sources are correlated to detect malware and malicious behaviour with a centralized dashboard for visualization and analysis of events.

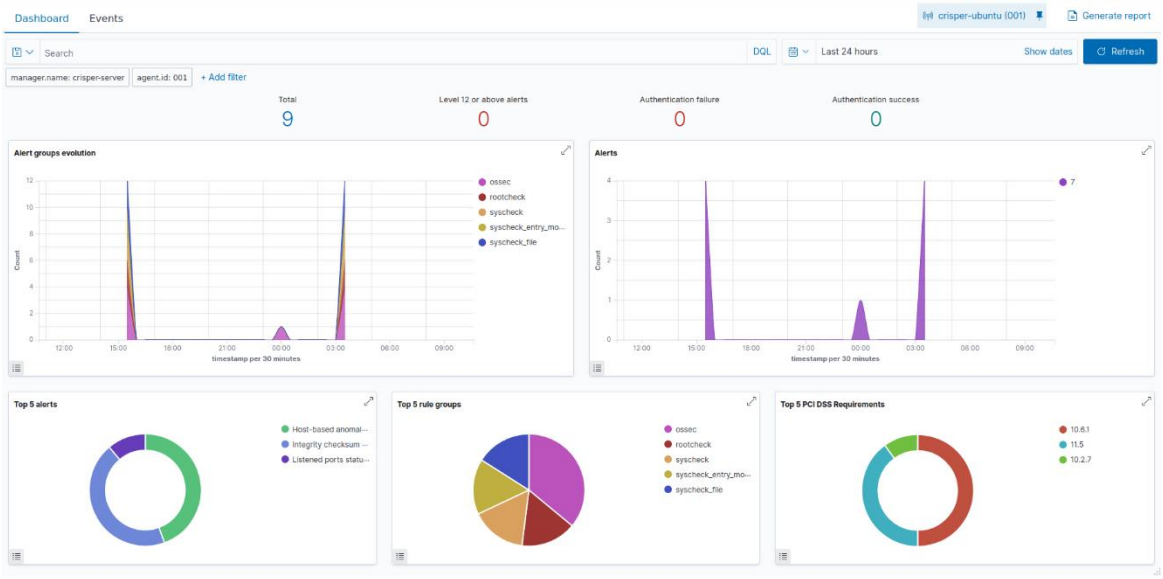


Figure 3: Security Alert Dashboard

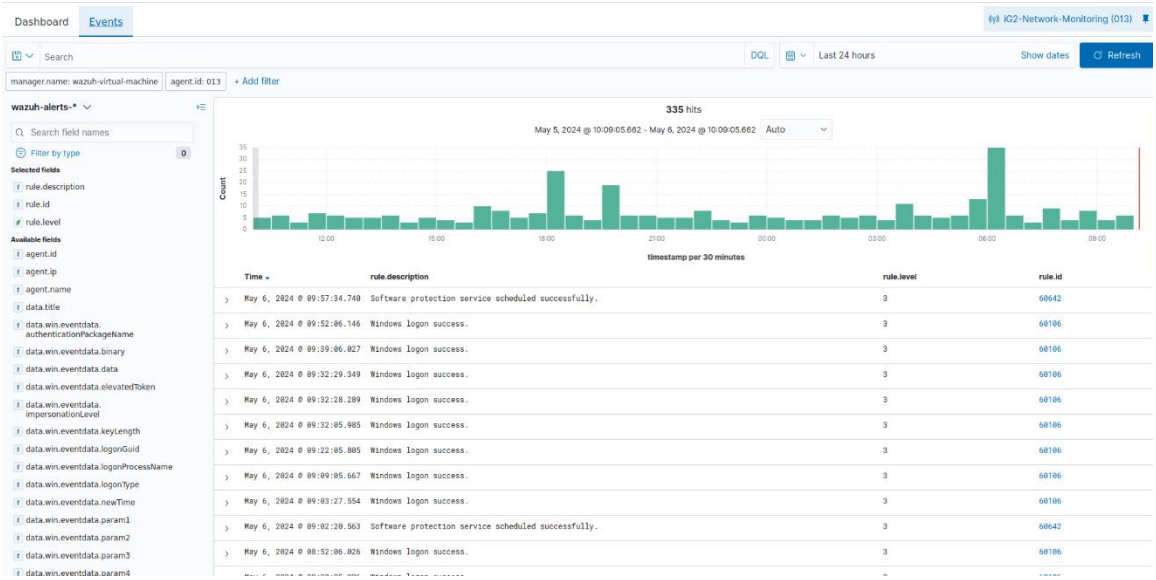


Figure 4: Casper UES Events

Casper UES provides real-time alerts on suspicious activity, enabling swift action by your security team. These alerts offer critical context, helping analysts prioritize and understand the nature of potential threats. The platform allows for the customization of alert thresholds and severity levels, ensuring that you receive the most relevant and actionable notifications. All this protection is offered in real time across various operating systems including Windows, Linux, macOS, and more.

File Integrity Monitoring

Leverage real time monitoring to detect changes to entire directories as well as individual files and trigger alerts for your team to act with support for Windows, Linux and macOS. The UES file integrity monitoring (FIM) tracks permissions, ownership, attributes and file content while using hash values to detect file changes. The solution effectively scales by distributing the workload across multiple nodes to handle monitoring many directories and files. Use FIM to demonstrate regulatory compliance on privacy and data security. Finally, configure and manage FIM policies and alerts from the central UES dashboard with detailed analysis on file changes.

Cloud Container and Workflow Security

Casper UES can track the metadata of your containers to produce an inventory and track network connections, deployment, transition status, process executions as well as triggering alerts when container images are created or deleted. The health of your containers is continuously monitored to proactively identify points of failure and remediate them. Running containers are consistently scanned for configuration changes, unauthorized command executions and other suspicious activity with alerts triggered to notify your team of potentially malicious activity. Take this a step further by monitoring the audit logs of container orchestration platforms such as Kubernetes. By collecting container telemetry, the UES provides real time threat detection in your cloud environment(s) that can be enriched by third party threat intelligence.

Ingest, aggregate, store and analyze logs from CSPs and cloud services to effectively identify security gaps and misconfigurations. Expand your vulnerability detection to the cloud and automatically detect and prioritize vulnerabilities so your team can remediate them. FIM capabilities can detect and monitor changes to your cloud directories and files while checking hash values against threat intelligence databases for malicious files.

Customization

Casper UES supports integrations with tools and services such as Virus Total, YARA, Windows Defender, Slack and more. The configuration can be customized with user-defined rules, detections and active responses. This granular control allows you to tailor Casper UES to the specific needs of your organization or environment. Whether you require advanced threat hunting capabilities or integration with custom security tools, Casper UES provides the flexibility to configure your security posture for optimal effectiveness.

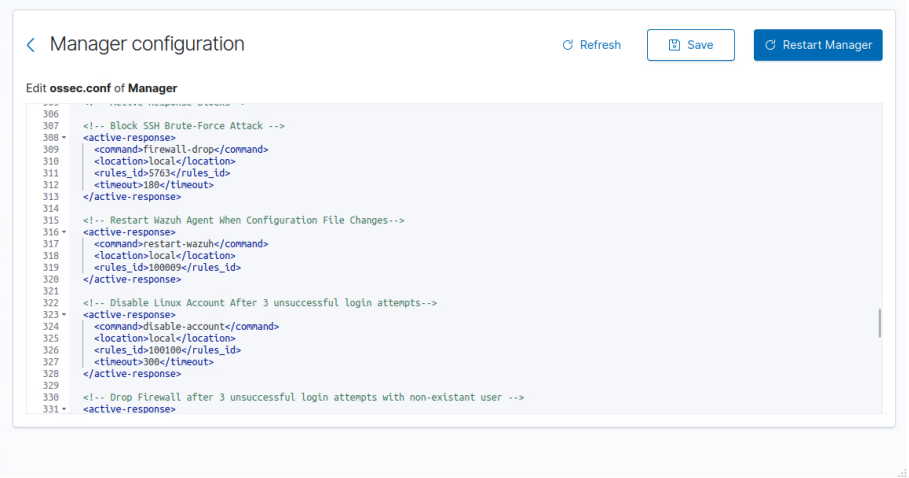


Figure 5: Manager Configuration

Casper UES Architecture

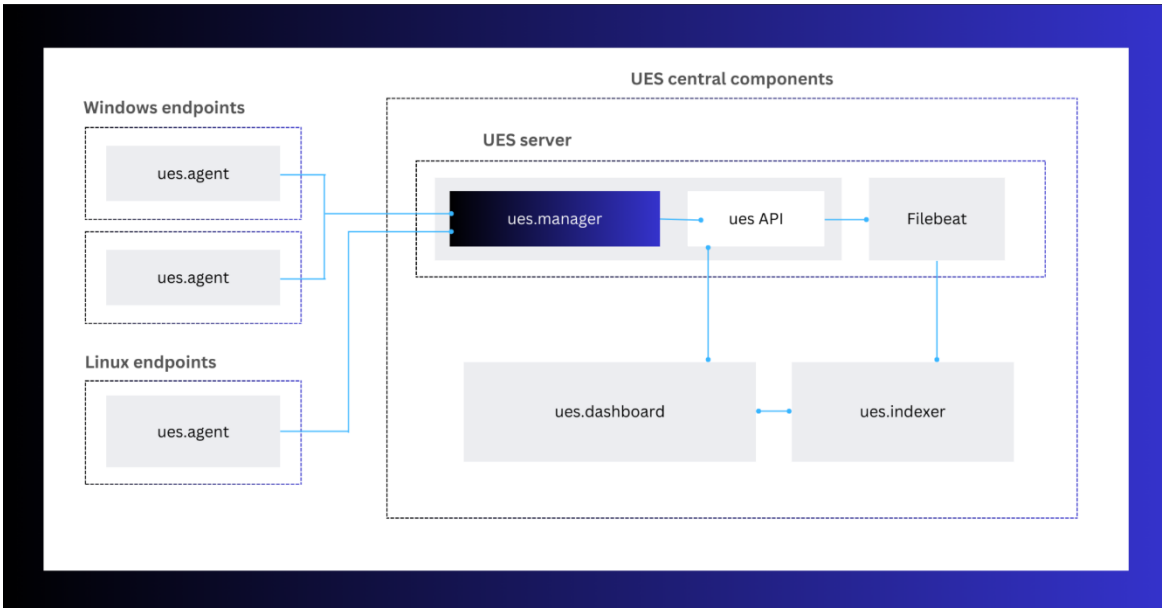


Figure 6: UES Architecture

The Casper UES solution utilizes a multi-layered approach to deliver comprehensive endpoint security. Lightweight UES agents deployed on workstations and servers provide essential threat prevention, detection, and response capabilities. These agents function not only as security shields but also as data collectors, gathering security-relevant logs from the local system. Network devices that lack native agent support, such as firewalls, switches, and routers, can still contribute to the overall security posture. These agentless devices can

seamlessly transmit logs to the central UES server using industry-standard protocols like Syslog, SSH, or their respective APIs. This ensures comprehensive log collection from all relevant endpoints within the network.

The UES server acts as the central hub for log management and analysis. UES agents and agentless devices transmit collected logs to the server, where a robust indexing and storage mechanism facilitates efficient log retrieval and forensic investigations if needed. Security doesn't stop at log collection; the UES server performs real-time analysis of this data. Utilizing advanced security analytics techniques, the server can identify anomalous activity and trigger security alerts for potential threats. To provide richer context for security personnel, UES enriches alerts using the MITRE ATT&CK framework for adversary tactics mapping. Additionally, threat intelligence feeds and selected regulatory compliance frameworks (e.g., GDPR, CIS, NIST 800-53) can be integrated to further enhance alert context and prioritization. This enrichment process empowers security teams to make faster and more informed decisions.

The Casper UES solution goes beyond threat detection by offering seamless integration with popular ticketing systems (e.g., Jira, ServiceNow) to streamline incident management workflows. Furthermore, integration with messaging platforms (e.g., Slack) facilitates real-time communication and collaboration within the security team. This ensures that identified threats are promptly addressed and mitigated, minimizing potential damage.

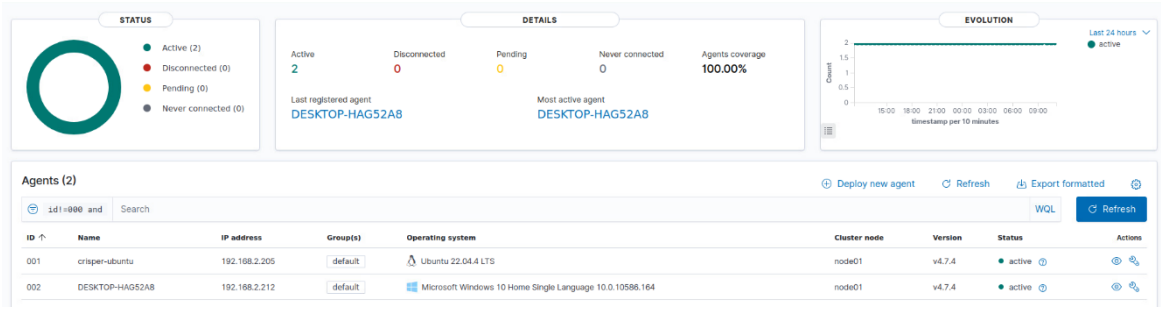


Figure 7: Agent Dashboard