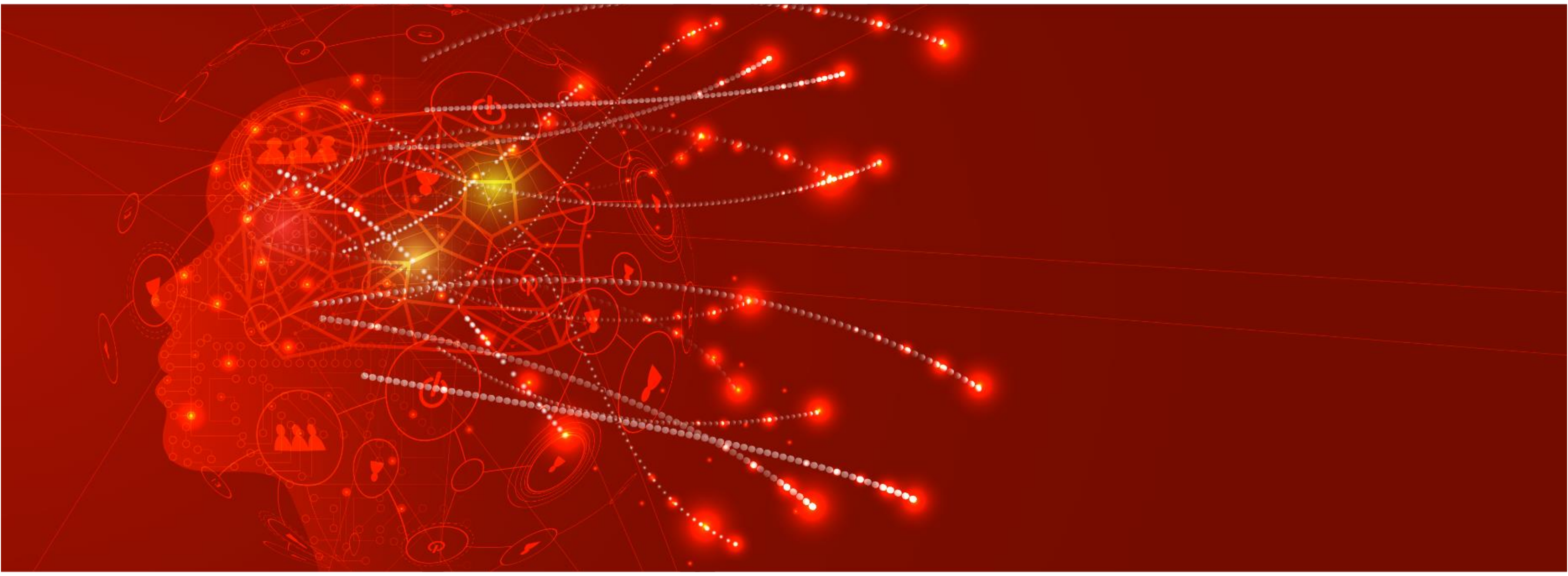
Datasheet

CyberStack Crisper: Unified Endpoint Security



CyberStack Crisper: Unified Endpoint Security

Empower your security strategy with CyberStack Crisper Unified Endpoint Security (UES), ushering in the next generation of endpoint protection. In contrast to traditional approaches that segregate endpoint security, threat intelligence, security operations, and cloud security, Crisper seamlessly integrates these functionalities into a unified platform.

In the ever-evolving threat landscape, organizations face the complexities of managing disparate security tools, however, modern security challenges demand a holistic approach. Unlike siloed solutions that necessitate stitching together multiple tools, CyberStack Crisper offers a unified platform, eliminating the need for an array of disconnected solutions. The UES streamlines your security stack by combining the capabilities of XDR, NDR and SIEM into a single, integrated solution. This not only enhances the efficiency of threat detection and response but also simplifies the overall security infrastructure. Elevate your security posture with CyberStack Crisper, where the power of unified endpoint security meets the intelligence required to navigate the evolving cybersecurity landscape.

Crisper UES Process

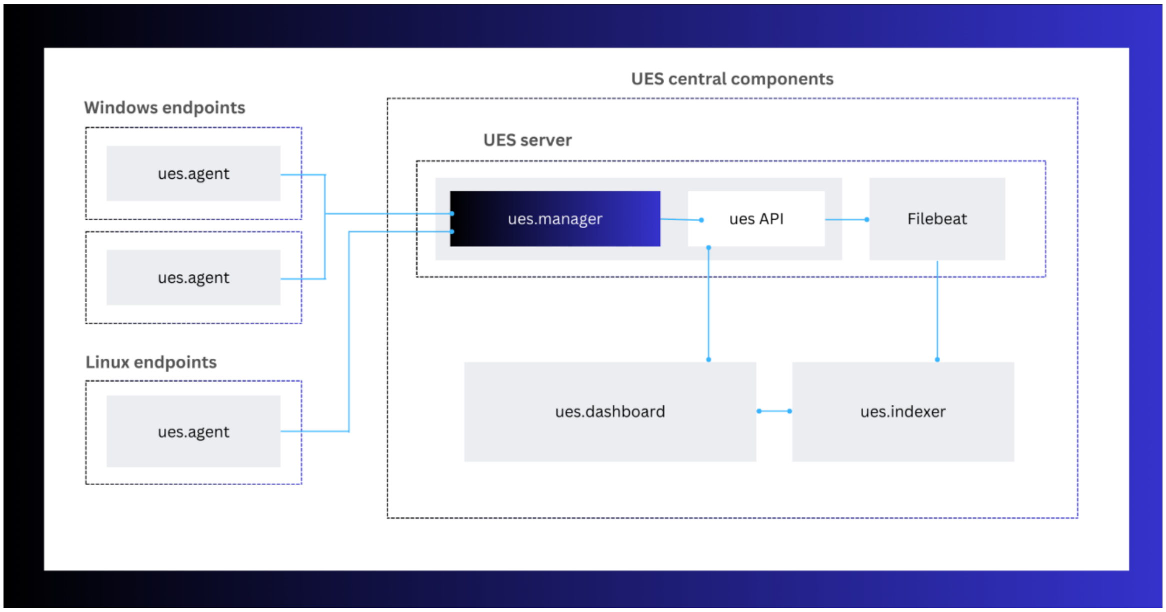


Figure 1: UES Architecture

The Crisper solution (see Figure 1 above) uses unified endpoint security (UES) agents installed on endpoint devices to protect them with threat prevention, detection and response capabilities. These agents also facilitate log collection from endpoint devices like workstations and servers. Agentless network devices such as firewalls, switches and routers can still transmit log data using Syslog, SSH or their API. The data from agents and agentless devices passes on to the central UES server to be indexed and stored.

The UES server analyzes the collected and indexed data and triggers alerts when suspicious events are detected. UES servers also enrich alerts by using the MITRE ATT&CK framework, threat intelligence and selected regulatory frameworks such as GDPR, CIS and NIST 800-53. Moreover, the server can be integrated with ticketing systems such as Jira or ServiceNow in addition to messaging platforms like Slack to help streamline security team operations.

Why Unified Endpoint Security?

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). Organizations often use a series of tools from different vendors. This introduces complexity and difficulty with integrations. The Unified Endpoint Security (UES) approach of Crisper offers several benefits.

Integrated Security Tools

Ingest data from endpoint devices (Windows, Linux or macOS) and network devices (routers, switches, firewalls, etc.) into the integrated SIEM to analyze and correlate events to detect suspicious events and behaviour.

Understand your Security Posture

Built in modules provide vulnerability assessments in addition to compliance reports and security configuration assessments. These work together to provide your team with a comprehensive understanding of your security posture and where you fall short.

Threat Detection and Response

The UES can detect and respond to threats on endpoints or over the network based on signatures or suspicious behaviour. Organizations can set custom rules for detection and response to automate incident response.

Cloud Container and Workflow Security

Ensure that you have visibility over your cloud containers and workflows. CyberStack Crisper ensures that these cloud environments are protected in addition to your on-premises infrastructure.

Customization

Crisper UES supports integrations with tools and services such as Virus Total, YARA, Windows Defender, Slack and more. This ensures that our platform can be tailored to the specific needs of your organization or environment.

Crisper Features

Integrated SIEM and XDR: Crisper UES includes the functionality of XDR and SIEM to ingest, analyze, aggregate and correlate logs for malicious signatures and behaviours. Crisper then responds to suspicious events to protect your assets.

File Integrity Monitoring: It regularly scans endpoints to track users, permissions and files to detect suspicious file changes.

Vulnerability Assessment: Regular scans detect vulnerabilities on your endpoints with data sourced from the NIST Vulnerability Database, Microsoft and Canonical. Vulnerabilities are assigned scores and severity 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: Crisper provides a report for each endpoint based on CIS benchmarks assessing their overall security configuration, providing an overall score for each endpoint.

Automated Incident Response: CyberStack Crisper 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 Crisper UES when security incidents occur so that your team can take prompt action. There are options to integrate with ticketing platforms and threat intelligence to enhance incident response.

Cloud Container Security: CyberStack Crisper 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: Crisper UES comes preloaded with regulatory frameworks such as GDPR and NIST 800-53 to assess regulatory compliance. You can also create custom frameworks to ensure your environment complies with internal policies.

Benefits of Crisper UES

Cost-Effective Endpoint Protection: iG2 Crisper offers a cost-effective approach to prevent, detect and respond to threats throughout your environment.

Increased Efficiency: The UES integrates several tools into one stack and provides automation capabilities to decrease the mean time to respond (MTTR) to incidents.

Comprehensive Visibility: Between the agents on your endpoints, logs from network devices and integrations with cloud containers and workflows, your team can gain comprehensive visibility over your environment.

Scalability: Additional UES servers and UES indexers can be added to your Crisper deployment as needed to accommodate an increase in the number of endpoints and network devices.

Customization: Custom rule sets for detection and response as well as integrations for threat intelligence, incident response and team communications allow Crisper to be customized according to your team’s needs.