HAKWARE

PRODUCT OVERVIEW

HAKWARE

Hakware is a next-generation Security Management solution offering a comprehensive OneView of your entire IT and security environment.

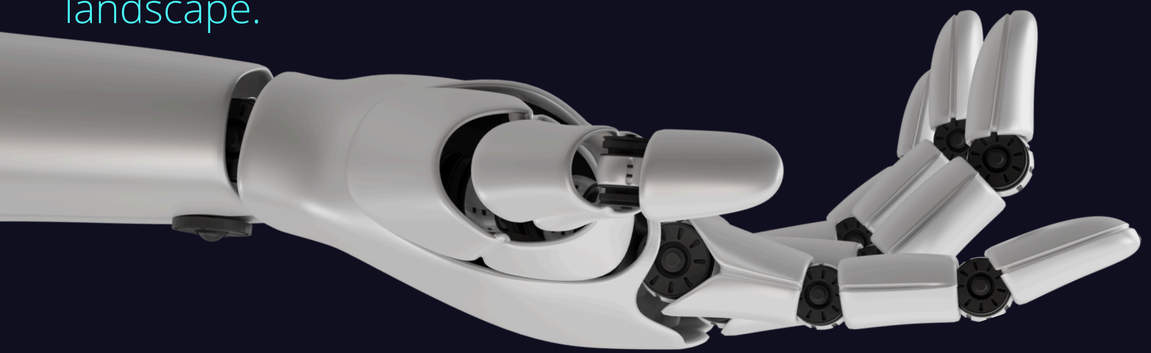
At the heart of Hakware are custom-trained models that consolidate and analyse data from multiple sources, including firewalls, endpoints, zero-day threats, and cloud environments, enabling a unified and proactive approach to managing your security posture.

Our solution includes Hakware Archangel, a powerful Vulnerability Assessment and Management tool that leverages purpose-built models to perform rigorous offensive testing on external environments. By blending intelligent data integration with advanced testing capabilities, Hakware empowers organizations to stay ahead of potential threats with heightened insight, preparedness, and control.

ONEVIEW

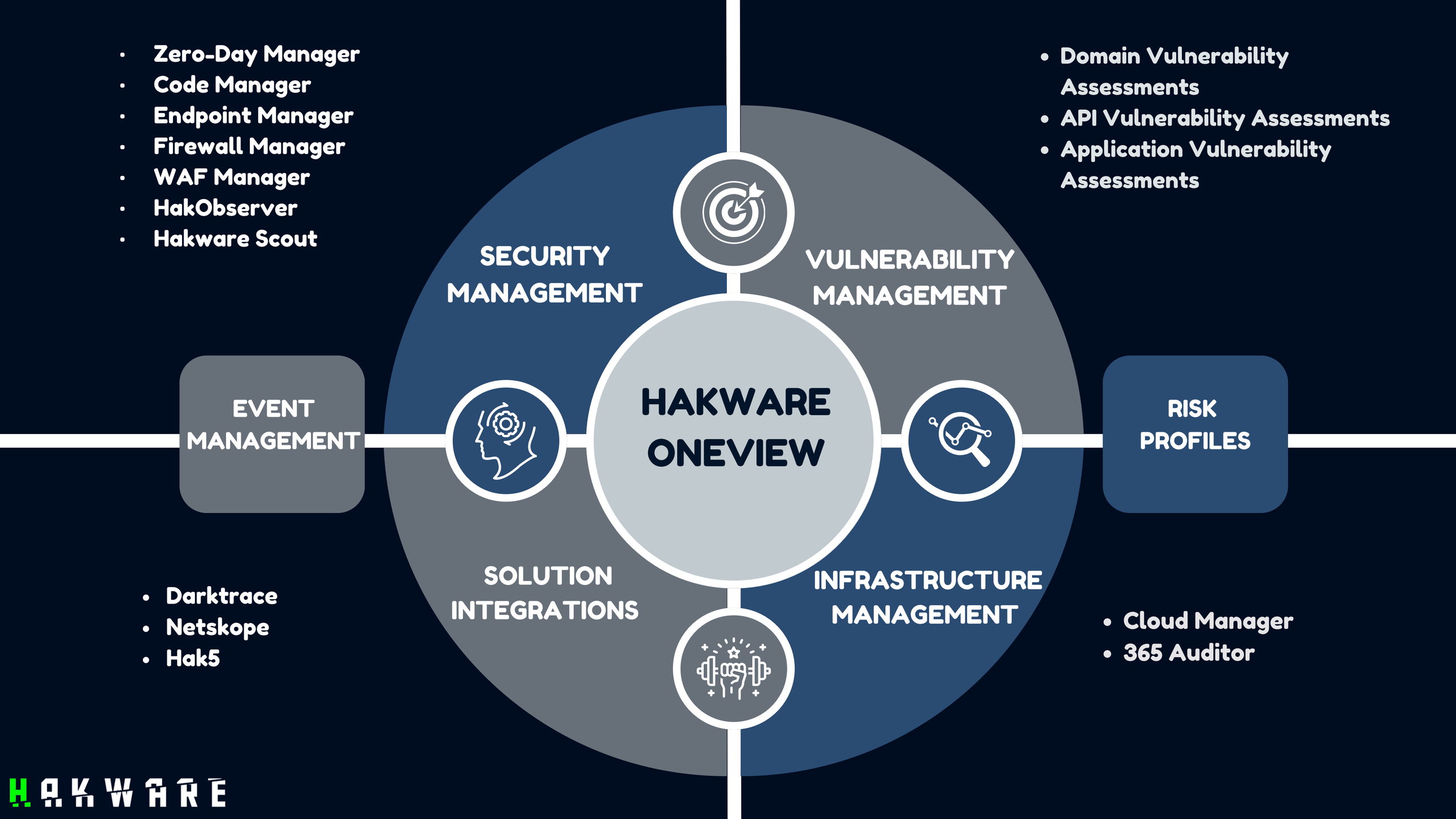
Hakware OneView is a comprehensive Security Management platform designed to streamline and unify all aspects of your IT and security infrastructure into a single, actionable interface. With a focus on delivering real-time insights, Hakware OneView consolidates critical data from diverse sources such as firewalls, endpoints, zero-day threat intelligence, cloud assets, and more.

This extensive integration enables a centralized view of potential vulnerabilities, threat activities, and compliance statuses across your organization's entire digital ecosystem. By bringing together fragmented data into one cohesive dashboard, Hakware OneView empowers security teams to make faster, data-driven decisions, significantly enhancing visibility and control over their security landscape.



At the core of Hakware OneView's effectiveness is its deployment of advanced, custom-trained models. These models analyze vast data sets with precision, enabling the identification of nuanced patterns and anomalies that would be difficult to detect otherwise.

The platform's proactive approach is further strengthened by Hakware Archangel, which conducts in-depth vulnerability assessments and management using purpose-built models that simulate offensive security tests on external assets. Together, Hakware OneView and Archangel provide an unparalleled level of insight, allowing organizations to move from reactive to proactive security management, improving their security posture and resilience against emerging threats.


Zero-Day Manager
Code Manager
Endpoint Manager
Firewall Manager
WAF Manager
HakObserver
Hakware Scout
SECURITY MANAGEMENT
Domain Vulnerability Assessments
API Vulnerability Assessments
Application Vulnerability Assessments
VULNERABILITY MANAGEMENT
EVENT MANAGEMENT
HAKWARE ONEVIEW
RISK PROFILES
Darktrace
Netskope
Hak5
SOLUTION INTEGRATIONS
INFRASTRUCTURE MANAGEMENT
Cloud Manager
365 Auditor
HAKWARE

HAKWARE

HAKWARE AI

MODELS

Each scan is not just a script, it's a unique model trained for a specific purpose. If our models aren't able to exploit your environment it will attempt different ways and in different combinations.

LEARNING

Our models continuously train and improve. The more domains we scan the more advanced our models become.

NON INTRUSIVE

Our scans simulate a real world attack, and in the real world you won't know the attacker is there. Using our advanced technology you won't even notice us.

HAKWARE
COMPLIANCE

GDPR
& POPI

Vulnerability scanning is not explicitly required by the GDPR (General Data Protection Regulation) or POPI (Protection Of Personal Information Act).

Although the Regulation does require organisations that process personal data to ensure that they have implemented appropriate technical and organisational security measures – which includes identifying vulnerabilities.

ISO 27001

- Timely identification of vulnerabilities.
- Assessment of your organization's exposure to a vulnerability.
- Proper measures considering the associated risks.

HAKWARE MONITORING

Hakware's monitoring is broken down into three main monitoring elements.

- Deepweb Monitoring.
- Passwords & account monitoring.
- Brand Impersonation monitoring.

Deepweb Monitoring
Our monitoring solution will review your brand on our indexed Deep/Dark web forums and marketplaces for any mentions of your brand.

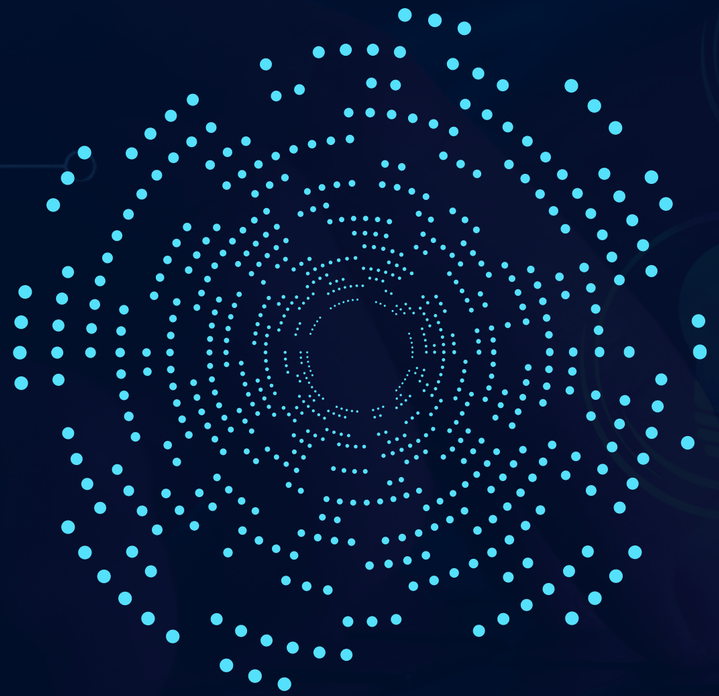
Passwords & account monitoring

We currently own 17.5 Billion records of leaked data. We will notify you of any new passwords or accounts leaked as they are sold on the web.

Brand Impersonation monitoring

We monitor the surface web for any sites impersonating your organisation.

ARCHANGEL ASSESSMENTS



At the core of our solutions is the Hakware Archangel scanner.

Covering 34+ attack vectors including OWASP top 10, there truly is no other solution as comprehensive.

The Archangel scanner will run daily to provide you with a proactive overview of your environment, identifying vulnerabilities as they arrise.

HAKWARE

WHAT IS ARCHANGEL

Hakware Archangel is an Artificial Intelligence based vulnerability assessment and pentesting tool.

Archangel enables organizations to monitor their networks, systems, and applications for security vulnerabilities with advanced Artificial intelligence continuously testing your environment.

Identify vulnerabilities before cyber criminals do. Stay on top of vulnerabilities and avoid human error. Mitigate the risks of a data breach, which will come with a range of costs including remediation, the loss of customers due to reputational damage and fines.

HAKWARE

HAKWARE

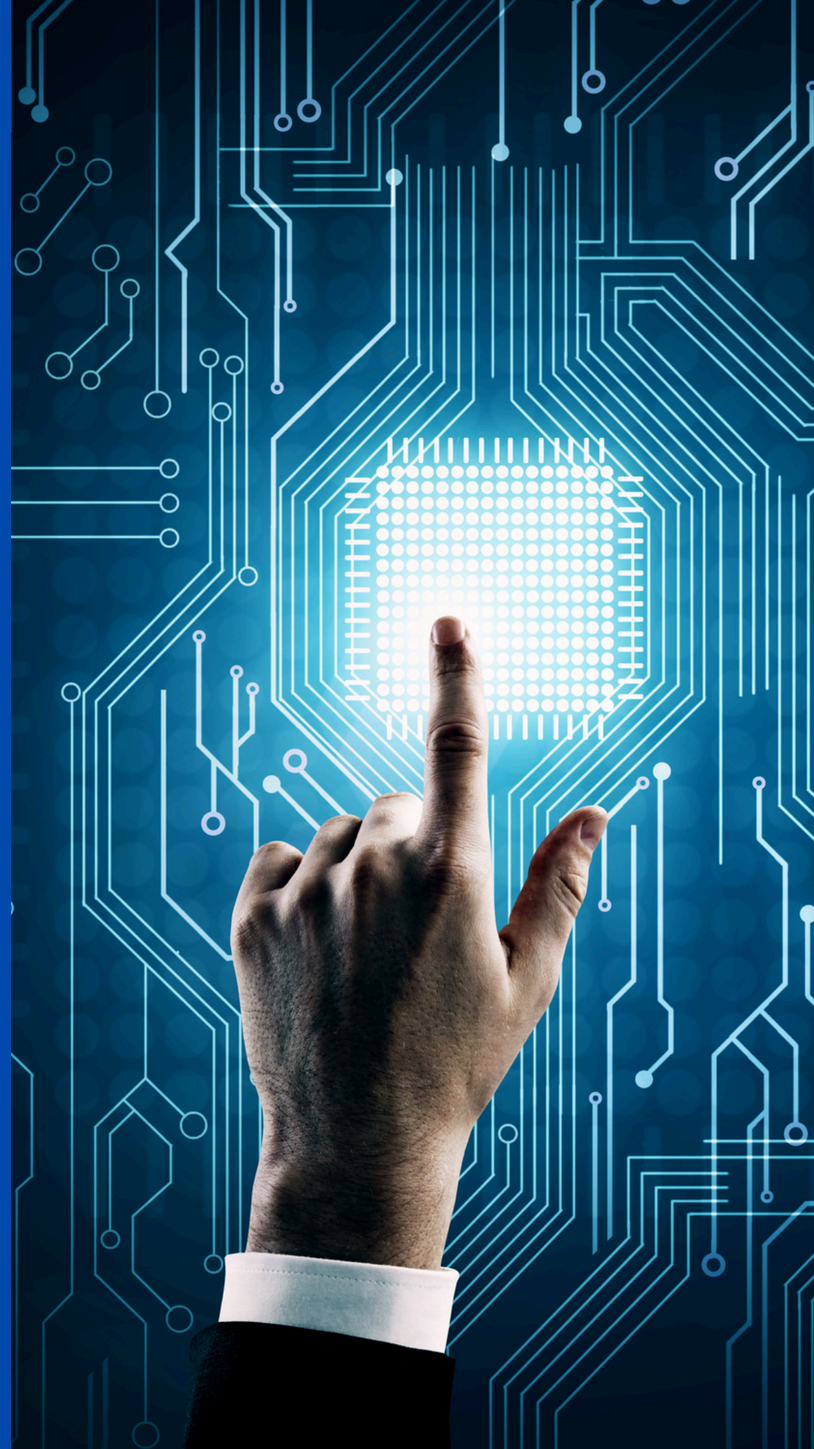
Microsoft 365 AUDITOR

- Make sure your 365 tenant has been set up securely.
- Confirm MFA and password policies have been set up correctly.
- User Sign-in audit logs identifying suspicious activity.
- Creates a Risk profile on each employee.

H.A.K WARE

CLOUD MANAGER

Our Cloud manager integrates directly into your Azure or VMWare environments to monitor vulnerabilities, resources, best practice configuration and vendor recommendations.

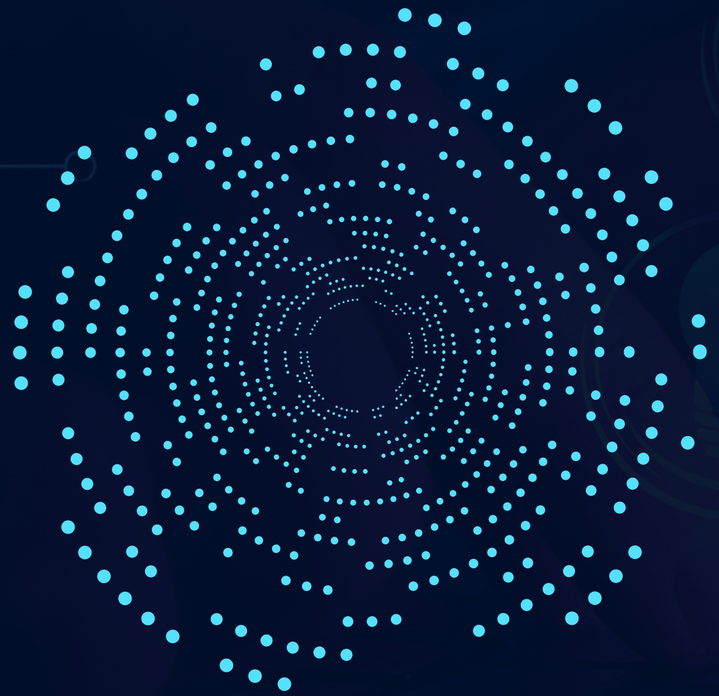


MSX CYBER

Built-in integration to XGRC Software's MSX Cyber solution allows you to manage and assess new vulnerabilities, set up action plans and track incidents.

HAKWARE

ZERO-DAY MANAGER



Don't wait for the next big threat. Be prepared.

Log the technology you use and we will monitor them for any Zero-day vulnerabilities and new CVE's.

HAKWARE

CODE MANAGER

Hakware's Code Manager integrates seamlessly with Azure DevOps and Git repositories to provide a thorough assessment of your code for potential vulnerabilities—all without ever storing or retaining your source code. By connecting directly to your repositories, Code Manager performs real-time analysis to detect security flaws or risky code patterns, helping developers maintain high standards of code integrity and security.

This module enhances your DevSecOps pipeline by allowing security assessments to happen natively within your development environment, making it easier to catch vulnerabilities early in the development cycle and reducing the risk of exposure in production environments.

HAKWARE

ENDPOINT MANAGER

Endpoint Manager connects to leading endpoint security solutions like SentinelOne and Microsoft Defender for Endpoint, gathering comprehensive data on all your devices. This powerful integration enables a unified view of endpoint activity across your organization, complete with dashboards and customizable event management triggers to help you monitor and respond to endpoint-related security events.

Endpoint Manager offers granular insights and allows for tailored alerting, ensuring that your security team can act swiftly in response to unusual activities, malware detection, or policy violations, ultimately enhancing the security and control of your endpoint environment.

HAKWARE

FIREWALL MANAGER

Hakware's Firewall Manager integrates with firewalls from top providers like Fortinet and Palo Alto Networks, pulling in all logs and events to provide a centralized view of firewall activity.

Through dashboards and customizable event management triggers, Firewall Manager enables real-time monitoring and detailed analysis of firewall interactions and traffic patterns.

This capability allows security teams to detect and address unauthorized access attempts, potential threats, and policy violations, ensuring firewall configurations align with organizational security requirements and proactively defend against network-based attacks.

HAKWARE

WAF MANAGER

WAF Manager connects directly to web application firewalls (WAFs) from providers such as Cloudflare, offering visibility into all logs and events through intuitive dashboards and customizable triggers for event management.

By centralizing WAF data, WAF Manager empowers security teams to monitor and manage web application traffic and respond quickly to potential threats, such as SQL injections, cross-site scripting (XSS), and other application-layer attacks.

This tool is invaluable for organizations with a strong online presence, helping to secure web assets against both common and sophisticated threats in real time.

HAKWARE

HOST MANAGER

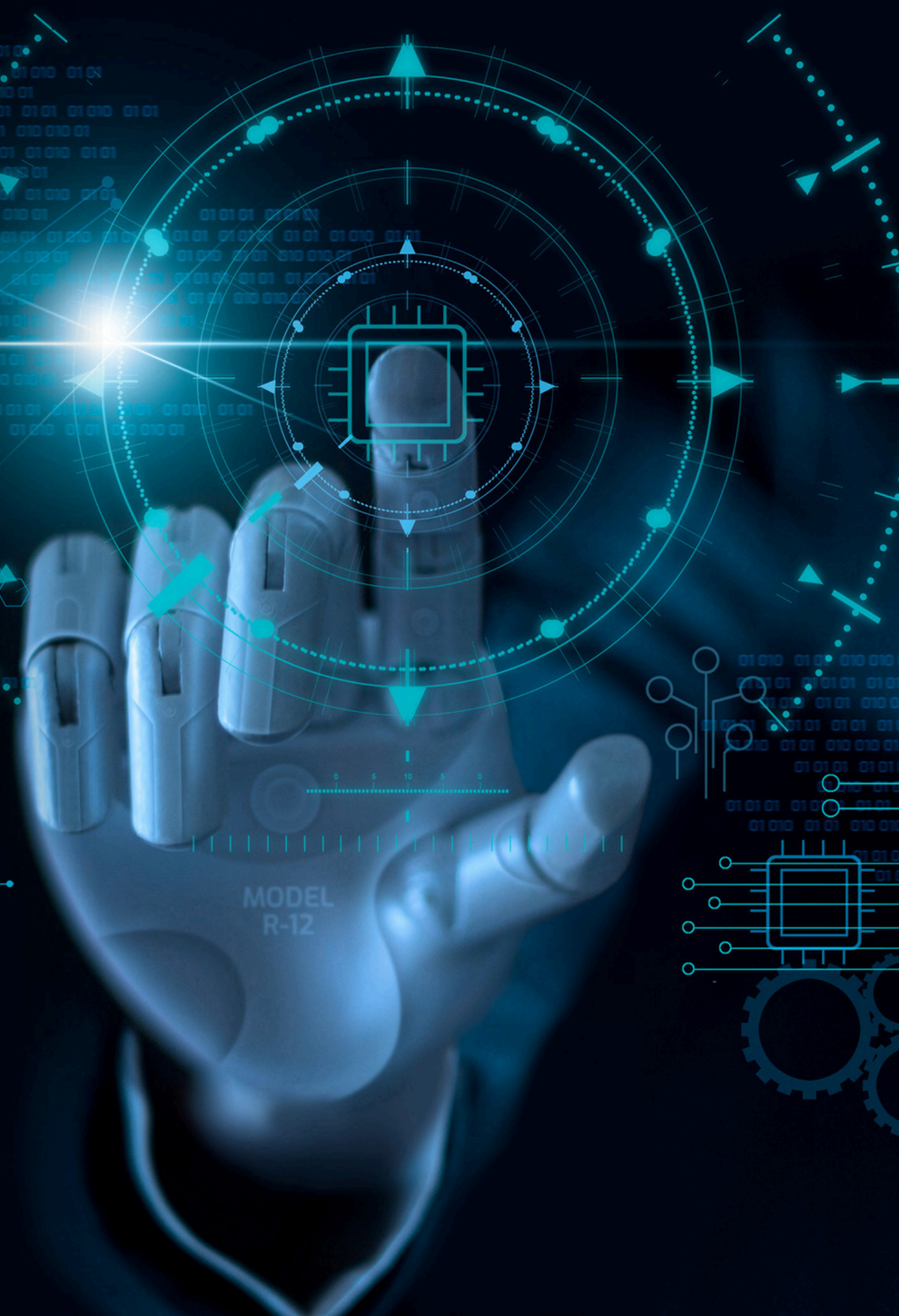
Host Manager provides a centralised view of all hosts available externally —ensuring complete visibility into every Host/Domain or IP. This module integrates seamlessly with Hakware's vulnerability intelligence and attack surface monitoring to prioritise risk across your environment.

HAKWARE

TRAINING MANAGER

Training Manager is Hakware's fully integrated cybersecurity awareness platform, designed to reduce human risk by educating users on phishing, social engineering, and safe digital practices. It delivers engaging, micro-learning video content with built-in progress tracking, exam assessments, and automated compliance reporting. Training can be customised per role or region and scheduled on a recurring basis to maintain organisational readiness.

Awarness Training



HAKWARE

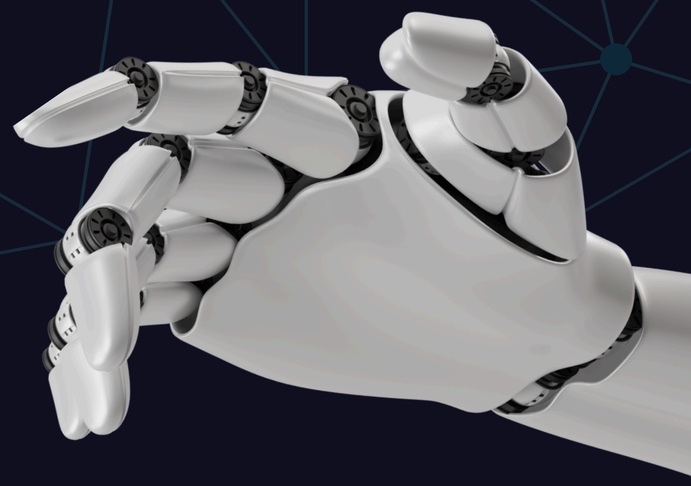
PERMISSION MANAGER

Permission Manager helps organizations maintain least privilege by auditing and controlling access across systems, applications, and cloud environments. It detects over-provisioned accounts, tracks permission changes.

With integrations into Active Directory, Microsoft 365, and cloud IAM platforms, Permission Manager empowers IT and security teams to enforce access governance and reduce insider risk.

HAKWARE

OVERWATCH DASHBOARDS



Overwatch Dashboards give clients full control over how they visualize their security and operational data.

With a powerful drag-and-drop interface, users can build custom dashboards using any data source within Hakware—including endpoint telemetry, firewall logs, vulnerability metrics, cloud security insights, awareness training status, and more. Designed to support both executive reporting and live Security Operations Center (SOC) views,

Overwatch lets each team tailor the dashboards to match their priorities—whether it's tracking threats, compliance, user behavior, or risk trends. Dashboards can be shared, scheduled, and filtered by client, region, or business unit, providing real-time, role-based visibility across the entire environment.

HAKWARE

SECURITY OPERATIONS

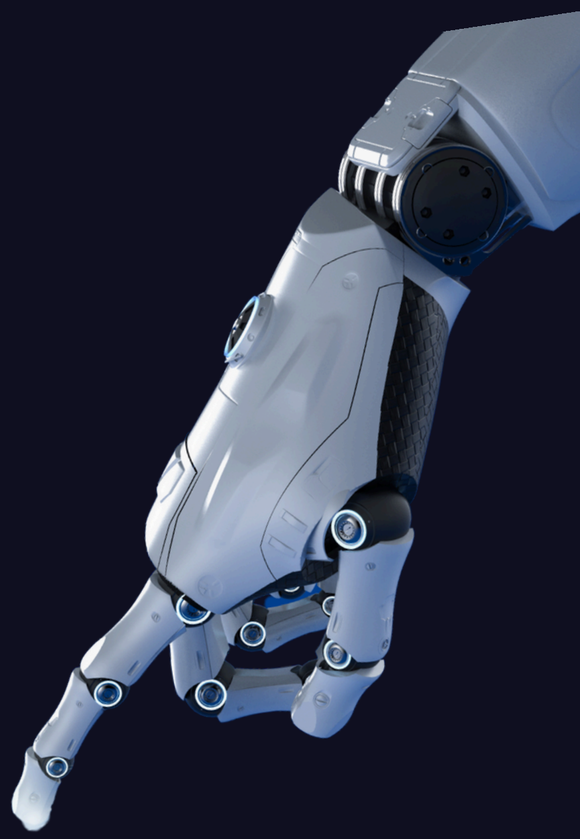
The Security Operations module is the central nervous system of Hakware's threat response ecosystem. It ingests and correlates data from endpoints, firewalls, cloud platforms, and vulnerability scans into a unified, real-time dashboard.

When threats or risks are identified, the platform automatically creates actionable tasks—assigning them to the appropriate teams or users—so nothing falls through the cracks.

Security Operations includes built-in support for executing industry-standard playbooks, enabling guided response, documentation, and remediation tracking. With integrated alerting, threat intelligence enrichment, and continuous visibility, this module empowers teams to proactively manage and reduce cyber risk with speed and confidence.

HAKWARE

HAKOBSERVER



HakObserver is a versatile agent that collects critical data on each VM where it’s installed, including a list of installed applications, user activities, system logs, and memory dumps for forensic analysis.

Designed to offer full visibility into VM environments, HakObserver acts as a continuous monitoring tool that supports proactive management and post-incident investigations.

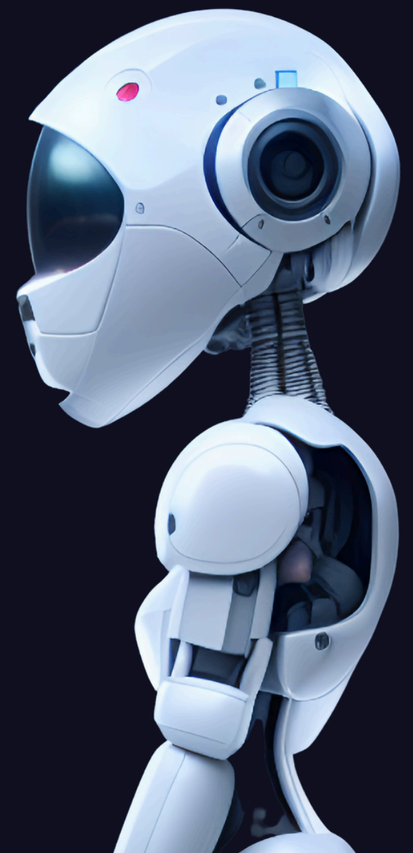
By capturing both real-time and historical data, it aids security teams in understanding the operational state of their VMs, detecting potential anomalies, and supporting root-cause analysis in the event of a security incident.

HAKWARE SCOUT

Hakware Scout is an agent installed on your network to detect and identify all devices within your network’s range.

Acting as an intelligent scout, it scans for and categorizes devices, providing a detailed map of network-connected assets.

This capability is essential for visibility into shadow IT, unauthorized devices, or unmanaged endpoints that could pose a security risk. With Hakware Scout, organizations gain an accurate and comprehensive understanding of their network landscape, enabling more robust asset management and enhancing network security.



HAKWARE

LET'S KEEP IN TOUCH

Nothing works better than a demo with data you recognise. Let us know when you are ready to identify vulnerabilities before cyber criminals do.

www.hakware.com

tamsin@hakware.com

Cell +27 76 403 2826