

Information Security Program: Management Policies & Practices



HAVI serves the most complex supply chains in foodservice, retail and convenience and is committed to ensuring the confidentiality, integrity, and availability of customers' critical data sets. The intent of our Information Security Program is to clarify how HAVI protects customer data in the delivery, transfer and ongoing management processes associated with services provided.

HAVI's supply chain management and marketing analytics solutions require customer data management, assessment, analysis and planning and may use customer data such as financial, inventory and product data. Customer data may be hosted by HAVI and/or transferred between HAVI and

the customer through a variety of methods including web portals, reports, and software.

HAVI is integrating the globally accepted, international standard security framework, ISO27001, into our plans and has established it as the basis for our security program. We are integrating the Center for Internet Securities' "Critical Controls;" a security standard developed from threat intelligence and breach investigations, to best protect sensitive customer data.

We also engage with third-party security organizations to enhance and build on our security capabilities.

About HAVI

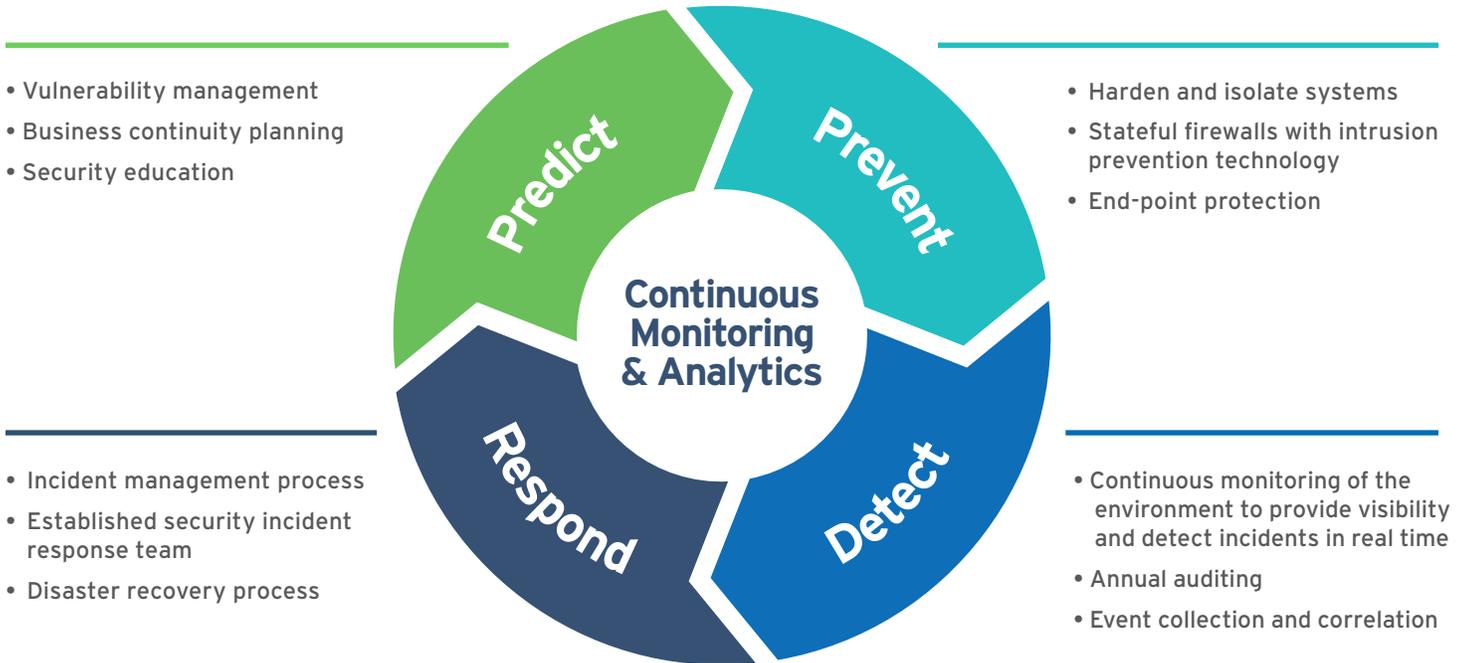
HAVI is a global, privately owned company focused on innovating, optimizing and managing the supply chains of leading brands. Offering services in supply chain management, marketing analytics, packaging, logistics and recycling and waste, HAVI partners with companies to address challenges big and small across the supply

chain, from commodity to customer. Founded in 1974, HAVI employs more than 10,000 people and serves customers in more than 100 countries. HAVI's solutions are complemented by the customer engagement services offered by affiliated company The Marketing Store.



For more information, contact your account representative or visit [HAVI.com](https://www.havi.com).

HAVI Security Framework



Predict

Strategic oversight and ongoing security education serves as key enablers to predicting security issues. HAVI works to stay abreast of emerging threats and areas of vulnerability while keeping in mind customers' information security requirements. We continually monitor the policies, tools and controls that are required and evolve when needed.

Prevent

A continuous focus on security measures and capabilities serves to prevent unauthorized modification, destruction or disclosure whether incidental or intentional. HAVI's security policies, awareness programs and access control procedures are interrelated and ensure customer data confidentiality, integrity and separation from other customer datasets. Also included in our program is proactive risk mitigation and vulnerability management, end-point protection, data retention policies, physical security and entry control, intrusion prevention and end-user education.

Detect

Even with the most robust prevention tools and processes, a system is always at risk of getting compromised. Customers can be assured that HAVI has appropriate measures to monitor and test system activities, ensure corrections are made as they are detected and threats are addressed as quickly as possible. Also included is centralized event monitoring that correlates data from intrusion detection, authentication, and border protection systems.

Respond

Timely response in the event of an information security breach requires an incident response plan that includes threat intelligence and business technologies. If a security breach has been detected, HAVI will engage the right people, processes and technologies to quickly assess, communicate, and execute the appropriate actions. Components include documented incident response and disaster recovery plans, proactive patching, and vulnerability management cycles.