ActivID® Threat Detection Service

Detection of Malware, Fraud and Data Breaches

The growing number of web-enabled devices, most without updated virus or malware protection, represents low-hanging fruit for cybercriminals looking for financial gain. Online businesses need to support their customers using a variety of devices including mobile devices and smart phones, but must protect the integrity of their interactions to prevent costly attacks, data breaches and fraud.

HID Global’s ActivID® Threat Detection Service gives businesses and consumers a new defense against cybercrime, protecting customer data and defending against fraud, malware and data breaches. Working transparently to the user, it protects online transactions from a wide range of threats, including Trojan and man-in-the-browser (MitB) attacks. It helps businesses detect and prevent fraud from compromised devices or accounts. Importantly, it works with a wide range of devices, including laptops and notebooks, tablets and smartphones.

How It Works

ActivID Threat Detection Service uses a unique combination of web page fingerprinting and tagless device identification technology to protect businesses from malware:

- **Web page fingerprinting**: ActivID Threat Detection Service can identify whether web page elements have been altered by cybercriminals, suggesting a MitB attack or a targeted Trojan. This also works for non-visual elements, such as JavaScript.

- **Device identification**: Tagless device identification creates device ‘fingerprint’ information, without cookies or having to store anything on the device.

All of this happens transparently to the user, without requiring any downloads or cookies. As a completely clientless solution, it works with many web-enabled devices, including tablets and smartphones.

On the back end, the information discovered can be integrated with broader fraud, risk, compliance and other systems. And when integrated with ActivID Appliance, ActivID Threat Detection Service adds another layer of intelligence for comprehensive defenses against malware and data breaches.
Protecting Your Business from Malware, Fraud and Data Breaches

ActivID Threat Detection Service provides clientless technology to protect the transaction between the device and your site. Its unique combination of web fingerprinting and tagless device identification technologies can:

- Instantly detect new Trojans targeting your organization.
- Detect devices compromised by crimeware.
- Spot and defeat MitB attacks.
- Identify accounts being used for money laundering or mule activities.
- Help detect fraudulent online account applications or registrations.

By integrating the information from the ActivID Threat Detection Service into existing fraud prevention and data security measures, organizations can reduce risk exposure from fraud while securing customer data.

An overview of banking trojans

Who Uses ActivID Threat Detection Service?

ActivID Threat Detection Service is an ideal solution for the growing number of organizations that need to protect data and transactions from potential threats from a wide range of client devices, including home computers, notebooks, tablets and smartphones.

This layered cybercrime protection is particularly valuable for financial institutions, online merchants and service providers that are potential targets for cybercriminals and malware.
Part of a Layered Cyber Security Strategy

ActivID Threat Detection Service is part of HID Global’s ActivID Authentication Appliance, which offers multi-faceted authentication to secure transactions, devices and accounts. When used in conjunction with the ActivID Authentication Appliance, ActivID Threat Detection Service adds essential malware and device identification technologies to a layered cyber security solution — protecting the integrity of the entire online transaction.

Availability and Platforms

ActivID Threat Detection Service is completely transparent to the end user and requires no download or user intervention. It works with most web browsers on most computer platforms and mobile devices.