# AWARENESS
T E C H N O L O G I E S

WE PROTECT YOUR BUSINESS FROM ALL INTERNAL THREATS

InterGuard is a complete insider threat prevention platform that protects companies from the full spectrum of internal threats (threats that originate from inside the organization) such as leakage of confidential data from the organization, loss of employee productivity, inappropriate employee behavior, and the damage caused by a lost or stolen laptop. Deployed at the endpoint and delivered in a SaaS format, InterGuard requires no hardware.

The agent includes 4 modules

① Web Filtering

② Employee Monitoring & Productivity

③ Laptop Recovery

④ Data Loss Prevention

All four modules are available either separately or together through one agent download and viewable through one control console.
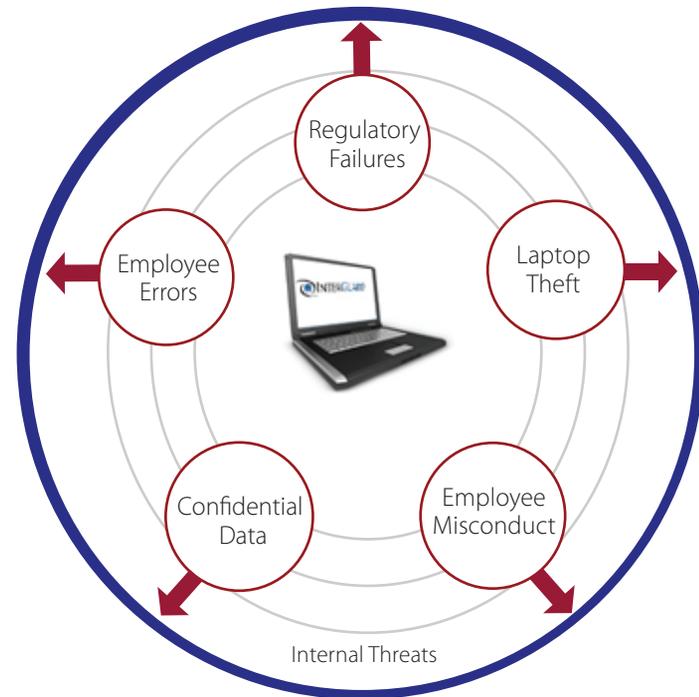
① Web Filtering

By solving the web filtering problem directly at the endpoint, InterGuard removes the need for hardware, eliminates latency, and extends protection beyond the corporate network. In addition InterGuard Web Filtering is designed to extend your visibility beyond a simple list of URLs and give you a true understanding of whether or not your employees are acting in a safe and productive manner. With InterGuard, you'll see everything from everywhere. No exceptions.

② Employee Monitoring & Productivity

Allows you to monitor and control ALL employee computer activity including websurfing, instant messages, all emails sent and received (including webmails such as Gmail, Hotmail, etc.), programs used, keystrokes typed and even take screenshots of computer activity.

③ Laptop Recovery

Laptop theft/loss remains far and away the biggest cause of confidential data loss. In the event of laptop theft or loss, you can geo-locate the laptop in real time as well as remotely delete/retrieve files from the stolen computer. You can also monitor and control the thief's every action. We'll also work with law enforcement to help you recover the physical property.

④ Data Loss Prevention

Identifies the location of sensitive data at rest and provides "push button" compliance, ensuring that no critical or regulated data is stored inappropriately across the organization. Additionally, InterGuard blocks confidential data from leaving the organization via email, email attachments or USB devices such as flash memory. InterGuard actually scans the content before it can leave the organization and determines whether or not a policy violation is being committed. If there is a violation, it blocks the action.

Regulatory Failures
Laptop Theft
Employee Errors
Employee Misconduct
Confidential Data

Internal Threats

Additional Information:

- Supports different settings for each user
- No hardware required
- Can be used in a Terminal Server or Citrix environment
- Ties in with Active Directory
- Quick and easy silent deployment with no user prompts if desired
- Can enforce policy even on laptops that never connect to the corporate network

SIMPLE SaaS SOLUTION

① Download Agents
Easily download and install agents on each workstation with just a few mouse clicks

② Make Settings
Through your online account, make your settings, which get pushed down to the agents over the internet

③ View Reports
View reports over the internet from any computer at anytime
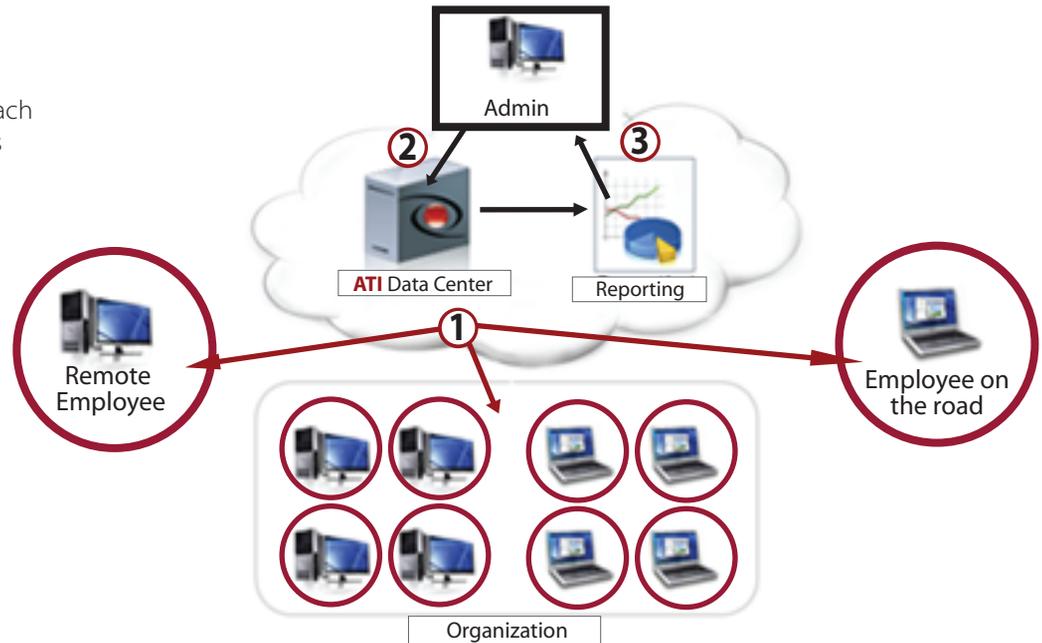
All of these products will work on all computers – desktops and laptops – no matter where they go regardless of whether or not they ever connect to the company network. No hardware is required if you want to keep things simple and host on Awareness Technologies' servers. All you have to do is deploy the software (it only takes minutes) and then log in via the web-based user interface. Alternatively, the entire solution can be hosted behind your firewall if desired.

One Control Console for all Insider Threats
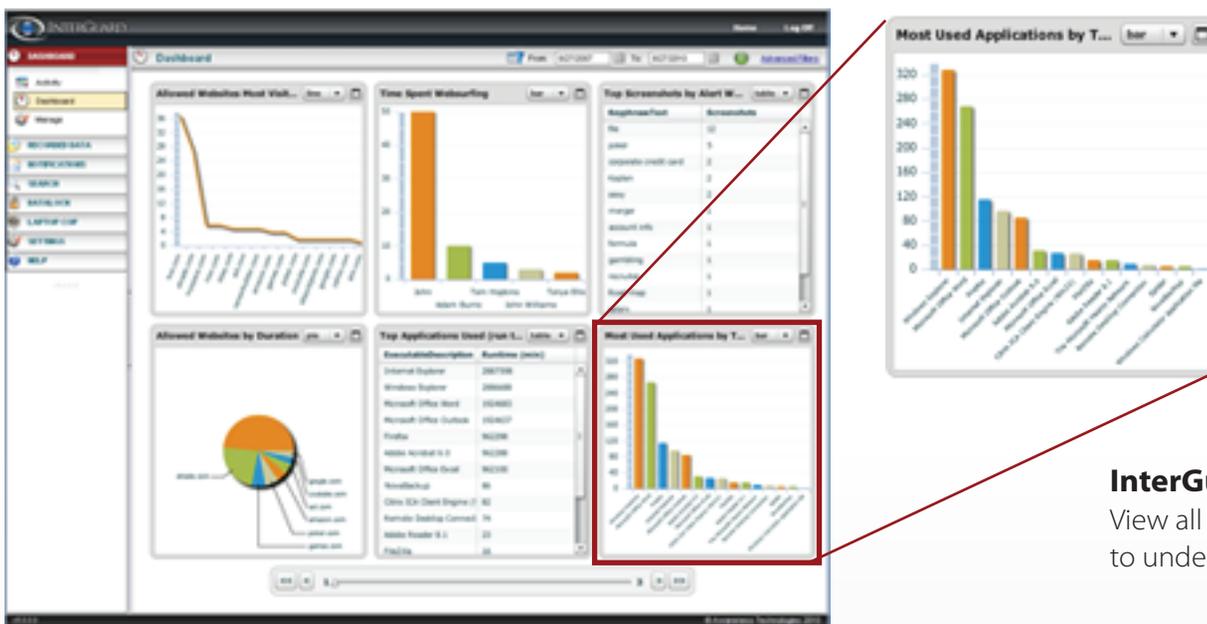
InterGuard's Dashboard
View all your reports in one easy to understand interface.