THE NEED
Advanced threats easily bypass signature-based detection solutions such as antivirus software and network-based intrusion prevention systems. To successfully prevent, detect, and contain advanced cyber threats, enterprises need multi-layered defenses at both the network level and the endpoint. This “kill chain” defense collects and correlates attack intelligence, identifies anomalies, and challenges malware at each step of an attack. By integrating network and endpoint defense mechanisms, security organizations can quickly investigate, confirm, and stop advanced threats.

THE DIGITAL GUARDIAN SOLUTION
Digital Guardian is a scalable platform that protects intellectual property and other sensitive data against insider threats and outsider malware attacks. Digital Guardian provides visibility into data movement to detect malware and it provides controls to prevent malware from compromising critical systems and data.

Unlike antivirus software that can only detect known threats, Digital Guardian detects and blocks malware behavior as it unfolds in real time. Digital Guardian even protects host systems when users are off the company network and unprotected by corporate network defenses.

Digital Guardian recognizes and correlates compound process events from system, application, and user activity, including:

- Process activity - including file and network access, and starting and stopping processes
- Data events - including file operation type, destination, and classification of file
- System context - including user, application, time, OS, and network

Digital Guardian also provides a wide range of policy controls to stop malware and protect sensitive information:

- Block code from executing
- Block access to files and networks
- Alert administrators and incident response teams to policy violations and malicious activity
- Prompt users to acknowledge company policies and justify their actions
- Encrypt sensitive data automatically based, based on policy, user permissions, and activity

Digital Guardian uses a broad set of malware detection rules to identify malware threats without using signatures. Unlike application whitelisting, which can only compare process characteristics to a predefined list, Digital Guardian correlates individual system, application, and data events against a proprietary set of rules to establish the risk level of process actions and detect malware activity. Based on the risk level, Digital Guardian can implement control responses ranging from passive alerting, to blocking process actions, to locking down the host.
At Digital Guardian, we believe in data. We know that within your data are your company’s most valuable assets. The sum total of innovations, plans and potential. We protect your company’s sensitive information like it’s our own so you can minimize risk without diminishing returns.

For over 10 years we’ve enabled data-rich organizations to prevent data loss at the endpoint. Our expert security team and proven Digital Guardian platform radically improve your defense against insider and outsider threats.

Hundreds of customers across a wide range of industries rely on Digital Guardian to protect their critical information at the point of risk. Seven of the top ten IP holders and five of the top ten auto companies trust us with the integrity of their most valuable and vulnerable data. We take pride in knowing that, at this very moment, Digital Guardian agents are securing the sensitive data of the world’s most inventive, influential companies.

Companies serious about data protection choose Digital Guardian.