ivanti

DATA SHEET

Ivanti Endpoint Security, powered by Heat

Today's rapidly changing IT network is more distributed and virtual than ever: more data is being stored on remote endpoints, such as laptops and smart phones, and increasingly accessed through collaborative cloud-based applications. Additionally, targeted threats are on the rise, with the demand for defense-in-depth security frameworks more important than ever. Successfully balancing the need for layered, point-based technologies to disrupt these persistent attacks against budget and resource constraints is the struggle organizations continually face.

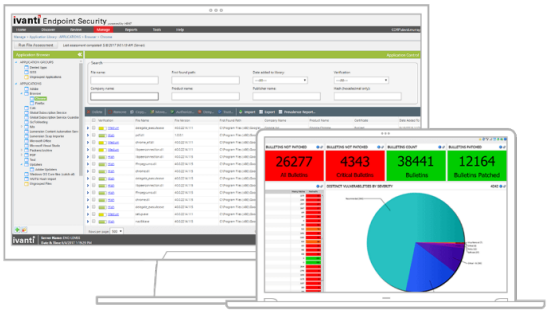
All organizations, no matter the size or industry, are impacted by targeted threats:

- 40% of organizations say their endpoints have been the entry point for an Advanced Persistent Threat (APT) attack.[1]
- Although the median size of targeted organizations is 2,500 employees, the fastest growing segment is those with 250 or fewer employees.[2]

Relying upon multiple, point-based endpoint management and security technologies has added IT environment complexity and cost. In fact, the average number of agents has been growing over the past several years to more than seven per endpoint; similarly, the average number of consoles used to manage basic endpoint security and operational functions has grown to almost seven per organization.[3]

Ivanti Endpoint Security provides:

- Defense-in-depth protection for targeted threats, combining operational and security capabilities to effectively reduce the attackable surface area while layering multiple preventative technologies to disrupt targeted attack progression.



- Greater visibility and control with an end-to-end approach that includes capabilities to meet endpoint operations, security, compliance, and IT risk-management needs.
- Reduced complexity and TCO via a fully integrated single-agent, single-console architecture to eliminate agent bloat and endpoint performance drains while streamlining workflow.

Ivanti Endpoint Security addresses the problem of endpoint protection from both operational- and security-based perspectives, while delivering an integrated platform that reduces complexity and costs.

By reducing the known exploitable surface area on endpoints, defining a trusted application environment, blocking known and unknown malware, and protecting data, Ivanti provides layered protection around multiple aspects of endpoint risk. Complexity can foil the most wellthought-out approaches to security, and that's why Ivanti has designed Ivanti Endpoint Security to operate through a single server, database, and console architecture with a modular agent — making it easier to manage thousands of endpoints, regardless of their location.

Endpoint Operations

Patch Management: Reduces organizational risk and optimizes IT operations by eliminating operating system and application vulnerabilities across all endpoints and servers. Supports multiple OS versions (e.g., Windows, Linux, UNIX, OSX), as well as third-party applications (e.g., Adobe Acrobat Flash and Reader, Google Chrome, Mozilla Firefox, and Oracle Java).

Content Wizard: Delivers customized extensibility through wizard-driven tools for deploying and removing software, remediating configurations, performing systems-management tasks, and delivering custom patches.

Reporting Services: Provides integrated, pre-configured, and centralized business intelligence that can be customized to meet organizational needs.

40% of organizations say their endpoints have been the entry point for an Advanced Persistent Threat (APT) attack. [1]

Endpoint Security

Application Control: Defines and enforces trusted application usage through whitelist policies to ensure only applications explicitly authorized or trusted can execute. Includes Advanced Memory Protection to defend against sophisticated memory injection attacks.

Antivirus: Provides blacklist protection and removal of all malware, including viruses, worms, spyware, Trojans, and adware.

Device Control: Enforces usage policies for devices and ports, while providing data encryption for removable media to prevent data loss / theft.

Key Features

- Modular, Extensible Architecture with a Single, Resilient Agent: An extensible platform that uses a single agent to reduce agent bloat.
- Role-based Access Control: Provides granular control of groups and domains to effectively safeguard sensitive information and prevent user errors caused by unauthorized access.
- Active Directory Integration and Synchronization: Supports domains, user groups, and individual users set up in Active Directory and ensures sync with Active Directory to reduce setup and maintenance.
- Enhanced Asset Discovery and Agent Deployment: Scans the environment for endpoints to ensure visibility of managed and unmanaged systems, and deploys agents to unmanaged systems automatically or via scheduled basis.
- Immediate Policy Updates and Actions: Delivers near real-time policy and events updates without relying on push technology.
- Virtual Infrastructure Aware: Identifies all virtual systems in the environment to enable management of both physical and virtual systems within one solution.
- Reporting: Provides comprehensive visibility into the endpoint environment with a full range of operational and management reports that deliver critical feedback to the business.
- Enhanced Wake-on-LAN: Ensures that offline machines can be awakened to receive critical patches and software updates, and ensures maximum energy efficiency when used with power policies via the Content Wizard.

Learn More

ivanti.com/contact

epg@ivanti.com

[1] Ponemon Institute, 2014 State of Endpoint Risk
[2] Symantec, Internet Security Threat Report vol. 17
[3] Ponemon Institute, 2015 State of Endpoint Risk