ivanti

DATA SHEET

Ivanti Endpoint Security for Endpoint Manager

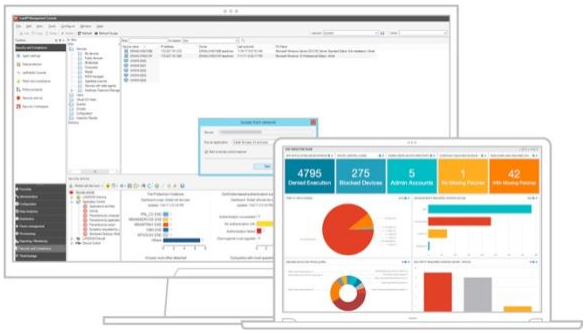
Ivanti® Endpoint Security for Endpoint Manager, powered by Landesk, prevents, detects, and remediates even the most sophisticated threats, including ransomware. Powerful, multi-layered protections automate discovery, inventory, and patch management, and prevent malware from running or spreading. When combined with Ivanti Unified Endpoint Manager, the solution uniquely enables you to isolate a device, remote control while it's isolated, and remediate or re-image the infected system. This integration with Ivanti Unified Endpoint Manager increases efficiency and control over your IT environment.

Protect Your Environment from Ransomware and Other Modern Threats

With Ivanti Endpoint Security for Endpoint Manager, you can see everything necessary to find and remediate malware, diagnose problems, and identify faulty or non-approved processes. If ransomware invades your network, Endpoint Security will catch it, kill it, notify other connected machines, and block the malware from running on them. Powerful remote capabilities allow you to isolate, investigate, and remediate or re-image endpoints across the network. Additionally, device blocking and connection control let you monitor and restrict I/O device access. Application control guards against zero-day exploits, stealth attacks, and other sophisticated threats. And data protection features prevent malicious software from encrypting your files.

Discover and Inventory All Your Networked Devices and Software

Active and passive discovery technologies identify and inventory all IP-enabled devices in real time—even so-called "rogue" devices like wireless hubs as well as those



devices behind firewalls. Automatic discovery also helps you find all the software on those devices, including usage details. And when used with the Ivanti Cloud Services Appliance, Ivanti Endpoint Security for Endpoint Manager can inventory, scan, isolate, and patch remote devices without the need for virtual private network (VPN) connections.

Automatically Patch to Ensure a Stable and Secure Environment

Ivanti Endpoint Security for Endpoint Manager simplifies patch management, with no impact on users, through best practices, automated processes, and fast deployment. It patches multiple operating systems and third-party software across your network reliably—even those devices that are on the road, at a remote site, or asleep.

Harden Endpoints with Device and Connection Blocking

Device control and application firewall capabilities limit the types of external devices or connections that endpoints can access. You can also block devices that may be employed to introduce malware or steal data. Application firewall helps block malware from "calling home," rendering most of it useless. The solution logs which files are copied to external devices, so rest assured you'll pass your security audit.

Configure and Patch		Detect and Prevent		Remediation and Visibility	
What's Included	**Capabilities**	**What's Included**	**Capabilities**	**What's Included**	**Capabilities**
Device Discovery	Active, passive, and agentless discovery and inventory—to know what devices to patch and secure. Also detect and locate wireless access points.	**Ransomware Detection**	Detect malicious encryption, kill it, and inform IT and other machines.	**Network Isolation**	Isolate devices on the network to prevent transferring malware, but leave the device accessible to remote control.
Patch	Automate patching for multiple operating systems and third-party applications.	**Ransomware Prevention**	Prevent files from being encrypted and prevent them from running elsewhere.	**Malware Containment**	Quarantine malware when detected.
	Schedule and roll out patches methodically through pilot groups and increasingly larger deployment rings.	**Malware Detection**	Signature, network, and behavioral-based detection.	**Remote Remediation**	Remote control; kill processes remotely; remote file management; remote re-imaging; deploy other forensic tools and scripts remotely.
	Prevent patches from interfering with users' productivity through reboot management and maintenance windows.	**Malicious Website Detection**	Prevent users from visiting suspicious sites.	**Dashboards and Reporting**	Ivanti Xtraction dashboards—powerful insight without a spreadsheet expert. Vulnerability, patching, and security-activity dashboards, plus alerts and detailed security reports.
Patch Intelligence	Gather feedback from end users about patch performance to better correlate incidents created by patches that impact users.	**Fileless Prevention**	Block fileless attacks initiated from Microsoft macros.	**SIEM Integration**	Send event logs to SIEM tools for further intelligence and forensics.
				Top Unified IT Solutions	**Capabilities**
Secure Config. Management	Out-of-the-box compliance content for PCI.	**Application Control**	Dynamic whitelisting learns what is in your environment and prevents unauthorized code execution.	**Windows 10 Migration and Windows as a Service (Updates)**	Automate how you deliver Windows 10 machines that are personalized and ready for users—then maintain all the updates and channels Microsoft throws at you.
	Ability to script additional compliance content.	**Device Control**	Prevent use of removable storage and ports to introduce malware or to copy sensitive data and log all data copying activities.	**Onboarding & Offboarding**	Provide the right access, apps, and resources when a user starts or moves positions—then remove their rights and licenses when they leave.
Firewall	Block malicious apps from calling home and transferring data.			**Self-service IT**	Create a service catalog that ties everything together in the background—services, deployment, asset management—while the user just pushes a button.

Protect Against Zero-Day Threats with Advanced Application Control

Application control features protect against file-based and fileless attacks by preventing malicious software and scripts from executing, and by using memory protection techniques. Learning capabilities minimize false positives and allow legitimate apps to run uninterrupted. A cloud-based reputation database provides further insights about which apps should be allowed to run in your environment.

See, Act, and Show Results

Ivanti Endpoint Security for Endpoint Manager also provides an array of reports and dashboards to help you monitor the effectiveness of your security efforts. The dashboards let you take actions from within the visual data. This visibility includes detailed reports on policy enforcement, compliance levels, user behavior, patch status, real-time security outbreak alerts, and much more.

Strengthen Security Through Unified IT

As its name implies, this solution integrates with Ivanti Endpoint Manager to unify endpoint security and management. This enables fast automation of both security and IT management policies, optimizing IT resources. Gain unequaled visibility across IT security and management activities to reduce risk and improve decision-making.

As an add-on, use Ivanti Antivirus to protect against known malware as well as malware detected through behavioral analysis. However, if you have another antivirus solution, Ivanti Endpoint Security for Endpoint Manager lets you manage third-party antivirus solutions of your choice.