End Point Monitoring/Control Activities	Used cases covered by inDefend Solution	Window	Linux	MAC
Browser Activity	Monitoring browser activities i.e. access to Social Networking sites, Jobs & Career, Shopping portals, personal emails etc.	Yes	Yes	Yes
	Monitor usage or time spent on different websites/URL like Social Networking sites, Jobs & Career, Shopping portals, personal emails etc.	Yes	No	No
	Blocking browser activities i.e. access to Social Networking sites, Jobs & Career, Shopping portals, personal emails etc.	Yes	No	Yes
Application Network Activity	Monitoring of applications and network activities i.e. download accelerators, torrents, Gaming applications, FTP, P2P applications etc.	Yes	Yes	Yes
	Selectively allow or block any kind of internet applications	Yes	No	Yes
	Bypass network applications	Yes	No	No
	Monitor usage or time spent on different applications like proxy & tunnelling applications, download accelerators, torrents, Gaming applications, FTP, P2P applications etc.	Yes	No	No
SMTP Email Activity	Monitor all SMTP based emails that are sent through email clients like Outlook, Thunderbird, Outlook express, etc.	Yes	Yes (SEG)	Yes (SEG)
	Shadow logging of the entire content of the SMTP email along with attachments.	Yes	Yes (SEG)	Yes (SEG)
	Control all SMTP based emails that are sent through email clients like Outlook, Thunderbird, Outlook express, etc.	Yes	No	No
	Monitor all Gmail webmail activity along with complete shadow log of the outbound and draft emails.	Yes	Yes (SEG)	Yes (SEG)
	Control all the outbound Gmail webmail-based email activity.	Yes	No	No
File Upload Activity	Monitor file uploads to any domain through browser i.e. file uploads to Dropbox, personal emails like yahoo etc.	Yes	No	No
	Shadow log of files uploaded to any domain through browser i.e. file uploads to Dropbox, personal emails like yahoo etc.	Yes	No	No
	Control file uploads completely by limiting them on the basis of the file types or the destination where they are being uploaded etc.	Yes	No	No
	Control file transfer over Skype and Windows Live Messenger	Yes	No	No
	Track the destination server to which the files have been uploaded through browser.	Yes	No	No
Device Activity	Control removable storage device media usage	Yes	Yes	Yes
	Access-based policies on each Registered USB device for different endpoints	Yes	Yes	Yes
	Set specific policies on CD/DVD access	Yes	No	No
	Blocking ofMTP/Local and Network Printers	Yes	Yes	Yes
	Blocking Bluetooth activity	Yes	No	Yes
	Monitoring of all files being copied from computer to USB drive	Yes	Yes	Yes
	Shadow log of files transferred from endpoint to external USB storage device using enforced encryption.	Yes	Yes	Yes
	Internal access restriction on USB storage devices	Yes	Yes	Yes
Search Engine Activity	Monitoring and logging of the web search engine activity	Yes	No	No
Content Filtering	Content filter-based alerts for email on the basis of defined sensitive keywords, phrases, patterns (visa card, Pan card, contact numbers, etc) and file type	Yes	Yes (SEG)	Yes (SEG)
	Content filter-based alerts for file upload on the basis of defined sensitive keywords, phrases, patterns (visa card, Pan card, contact	Yes	No	No

	numbers, etc) and file type			
	Content filter-based blocking for email and file upload on the basis of defined sensitive keywords, phrases, patterns (visa card, Pan card, contact numbers, etc) and file type	Yes	No	No
Google Chat Activity	Google hangout chat monitoring for outbound chat messages sent from endpoint.	Yes	No	No
Strong Analytics & Incident Reporting	Graphical representation of activities via Ranking graphs and pie charts.	Yes	Yes	Yes
	Augmentation of analytics section to show incident counts	Yes	Yes	Yes
	Advanced Reporting and Analytics Framework for all kinds of device and network activities	Yes	Yes	Yes
	Graphical representation of productivity of the users.	Yes	Yes	Yes
	Analytics for top trending applications and websites being accessed in the organization	Yes	Yes	Yes
	Real-time incident alert notification on dashboard	Yes	Yes	Yes
	Detailed incident forensics report	Yes	Yes	Yes
Other Valued Added Features	Periodic screenshot to monitor detailed employee activity.	Yes	Yes	Yes
	Print activity monitoring	Yes	Yes	Yes
	Event-triggered screenshot for sensitive application activity and sensitive window title-based activity.	Yes	No	No
	Work schedule-based incident monitoring	Yes	No	No
	Audit Logs for admin activity	Yes	Yes	Yes
	User first and last activity monitoring	Yes	No	No
	Stealth mode to silently monitor activities	Yes	Yes	Yes
	Offline monitoring & Controlling of end user activities	Yes	Yes	Yes
	Temporary Policies for uplifting the user privileges for a defined duration	Yes	No	No
	Customized reports download as per admin requirement	Yes	No	No
	Password-protected uninstallation	Yes	Yes	Yes
	Tamper Proof	Yes	No	No
	Bulk installation on end user computers using Remote Deployment	Yes	No	No
	Easy extraction of analytics and logs via PDF Reports feature	Yes	Yes	Yes
	Admin activity Monitoring and Group Based Administration	Yes	Yes	Yes
	Central management of agent version upgrades via server dashboard	Yes	Yes	Yes
	Capability to detect sensitive content in images using OCR	Yes	Yes	Yes
	Data at rest scanning for files stored on endpoint will act as audit tool in identifying sensitive documents	Yes	Yes	Yes

	Used cases covered by SEG Solution	Window	Linux	MAC
SEG(Secure E-mail Gateway)	Agent-less, cross-platform monitoring of outbound email activities, performed via corporate email	Yes	Yes	Yes
	Graphical summary of outbound email activities of the organization - Total Emails Sent - Emails sent with BCC - Emails sent with attachment	Yes	Yes	Yes
	Blocking of emails based on presence of sensitive content in the email body and attachments	Yes	Yes	Yes
	Incident alerts in case of sensitive content found in the email body or attachments	Yes	Yes	Yes
	Flexibility in creation and assignment of email security policies, can be applied at user level or at user group level	Yes	Yes	Yes
	Granular activity reports for each email activity report, with capability to export the details in CSV format	Yes	Yes	Yes
	Parameters shown are: from, to, cc, bcc, subject, sent time, attachment name(s) and size(s)	Yes	Yes	Yes
	Shadow logging of email body and attachments, for performing incident forensics analysis.	Yes	Yes	Yes
	Capability to trigger incident alerts in case of sensitive content found in the email body or attachments	Yes	Yes	Yes
	Graphical summary of sensitive incidents detected by the Email Gateway	Yes	Yes	Yes
	Capability to detect sensitive content in images using OCR, when sent as email attachments	Yes	Yes	Yes
	Role based access management, to allow multiple administrators to access the administration console, with granular control of privileges	Yes	Yes	Yes
	Admin Activity Logs to track the various activities and changes performed on the dashboard	Yes	Yes	Yes