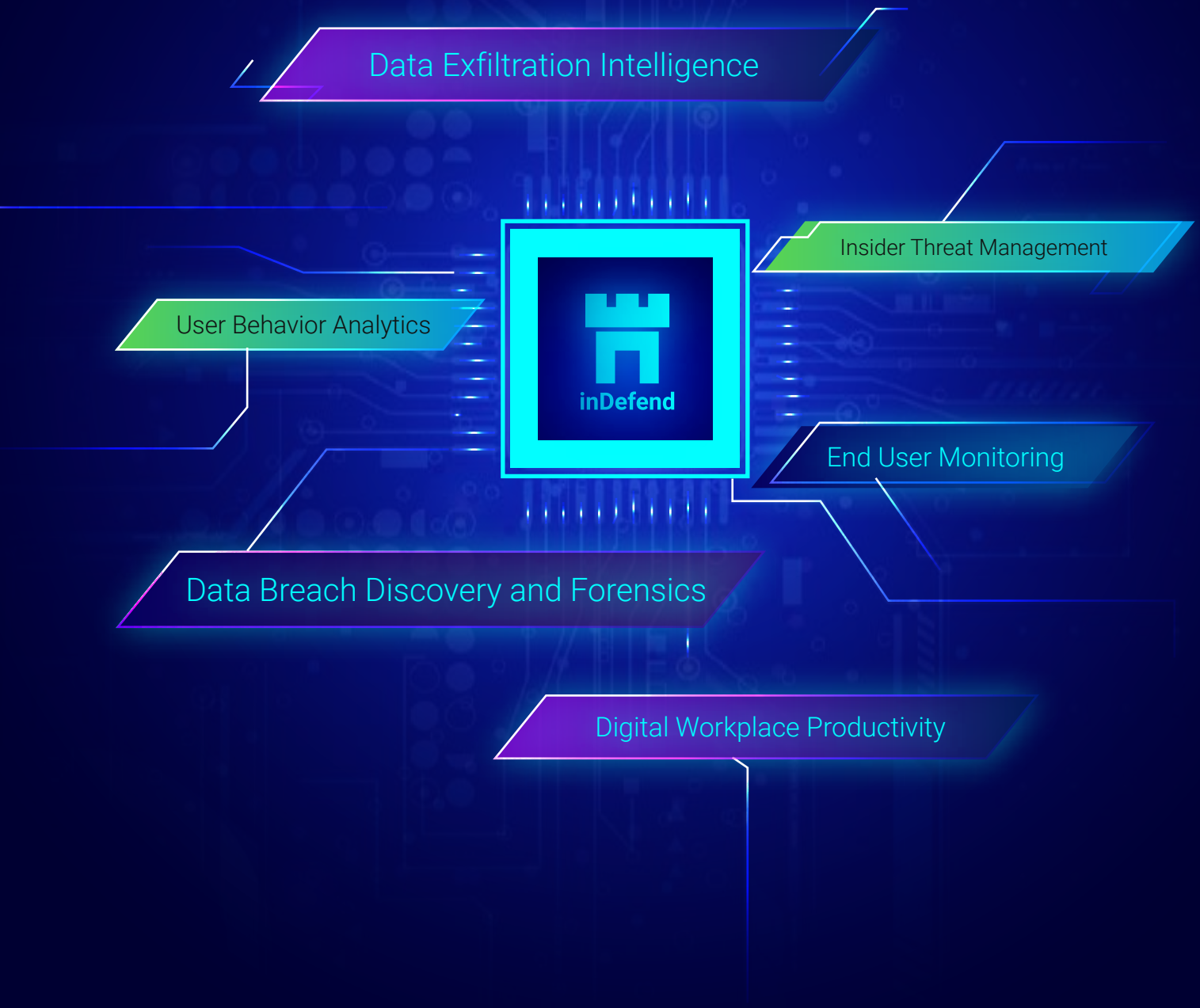
Data Resolve

inDefend Advanced



End Point Monitoring/Control Activities	Use cases covered by inDefend Solution	Windows	Linux
Browser Activity	Monitoring browser activities i.e. access to Social Networking sites, Jobs & Career, Shopping portals, personal emails etc.	Yes	Yes
	Monitor usage or time spent on different websites/URL like Social Networking sites, Jobs & Career, Shopping portals, personal emails	Yes	No
	Blocking browser activities i.e. access to Social Networking sites, Jobs & Career, Shopping portals, personal emails etc.	Yes	No
Application Network Activity	Monitoring of applications and network activities i.e. download accelerators, torrents, Gaming applications, FTP, P2P applications etc.	Yes	Yes
	Selectively allow or block any kind of internet applications	Yes	No
	Bypass network applications	Yes	No
	Monitor usage or time spent on different applications like proxy & tunnelling applications, download accelerators, torrents, Gaming	Yes	No
SMTP Email Activity	Monitor all SMTP based emails that are sent through email clients like Outlook, Thunderbird, Outlook express, etc.	Yes	Yes (SEG)
	Shadow logging of the entire content of the SMTP email along with	Yes	Yes (SEG)
	Control all SMTP based emails that are sent through email clients like Outlook, Thunderbird, Outlook express, etc.	Yes	No
	Monitor all Gmail webmail activity along with complete shadow log of the outbound and draft emails.	Yes	Yes (SEG)
	Control all the outbound Gmail webmail-based email activity.	Yes	No
File Access Monitoring	Monitor file access logs by file extension type i.e. doc., docx.,	Yes	No
	File access monitoring report in csv format- agent wise & user	Yes	No
	Monitor file upload activity, file sharing activity & file transfer	Yes	No
	Shadow logging of file access activity.	Yes	No
	capability to monitor any file transfer activity performed	Yes	No
	Capability to add or modify list of applications for which fileaccess activity needs to be monitored.	Yes	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
	Shadow log of files uploaded to any domain through browser i.e. file uploads to Dropbox, personal emails like yahoo etc.	Yes	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
	Control file transfer over Skype and Windows Live Messenger	Yes	No
	Track the destination server to which the files have been uploaded	Yes	No

Device Activity	Control removable storage device media usage	Yes	Yes
	Access-based policies on each Registered USB device for different	Yes	Yes
	Set specific policies on CD/DVD access	Yes	No
	Blocking of MTP/Local and Network Printers	Yes	Yes
	Blocking Bluetooth activity	Yes	No
	Monitoring of all files being copied from computer to USB drive	Yes	Yes
	Shadow log of files transferred from endpoint to external USB storage device using enforced encryption.	Yes	Yes
	USB control and ristriction based on file content	Yes	Yes
	Internal access restriction on USB storage devices	Yes	Yes
Search Engine Activity	Monitoring and logging of the web search engine activity	Yes	No
Content Filtering	Content filter-based alerts for email based on defined sensitive keywords, phrases, patterns (visa card, Pan card, contact numbers,	Yes	Yes (SEG)
	Content filter-based alerts for file upload based on defined sensitive keywords, phrases, patterns (visa card, Pan card, contact numbers,	Yes	No
	Content filter-based blocking for email and file upload based on defined sensitive keywords, phrases, patterns (visa card, Pan card,	Yes	No
Google Chat Activity	Google hangout chat monitoring for outbound chat messages sent	Yes	No
Strong Analytics & Incident Reporting	Graphical representation of activities via Ranking graphs and pie	Yes	Yes
	Augmentation of analytics section to show incident counts	Yes	Yes
	Advanced Reporting and Analytics Framework for all kinds of device	Yes	Yes
	Graphical representation of productivity of the users.	Yes	Yes
	Analytics for top trending applications and websites being accessed in	Yes	Yes
	Real-time incident alert notification on dashboard	Yes	Yes
	Detailed incident forensics report	Yes	Yes
Other Valued Added Features	Periodic screenshot to monitor detailed employee activity.	Yes	Yes
	Print activity monitoring	Yes	Yes
	Event-triggered screenshot for sensitive application activity and sensitive window title-based activity.	Yes	No
	Audit Logs for admin activity	Yes	Yes
	User first and last activity monitoring	Yes	No
	Stealth mode to silently monitor activities	Yes	Yes
	Offline monitoring & Controlling of end user activities	Yes	Yes
	Temporary Policies for uplifting the user privileges for a defined	Yes	Yes
	Customized reports download as per admin requirement	Yes	Yes
	Password-protected uninstallation	Yes	Yes
	Tamper Proof	Yes	No

Other Valued Added Features	Bulk installation on end user computers using Remote Deployment	Yes	No
	Easy extraction of analytics and logs via PDF Reports feature	Yes	Yes
	Admin activity Monitoring and Group Based Administration	Yes	Yes
	Central management of agent version upgrades via server dashboard	Yes	Yes
	Capability to detect sensitive content in images using OCR	Yes	Yes
	Data at rest scanning for files stored on endpoint will act as audit tool in identifying sensitive documents	Yes	Yes
API integration	API integration supported for productivity analytics	Yes	No
	API integration supported for incident reporting	Yes	Yes