ThePurpleGuys
Stress-Free IT Support

Security Services

24 x 7 SECURITY SERVICES

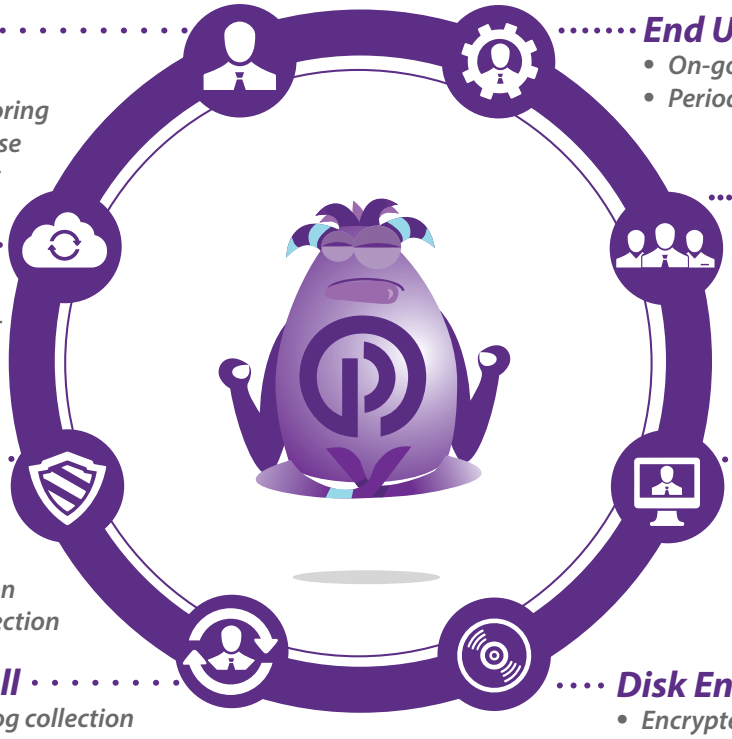
Gone are the days of a simple antivirus software and password protecting your organization. Without a cybersecurity program, your organization cannot defend itself against data breach campaigns, making it an irresistible target for cybercriminals.

Microsoft 365 Security
- 365 setting monitoring
- Account compromise
- Policy enforcement

Password & Patch Management
- Password policy enforcement
- Security and system updates

Endpoint Protection
- Anti virus/Anti ransomware
- Detection and response
- DNS filtering
- Advanced endpoint protection
- Endpoint detection and protection

Firewall
- Audit log collection and monitoring
- Centralized management



End User Training
- On-going training
- Periodic testing

Anti-Spam & Anti-Phishing
- URL & Attachment Sandboxing
- Email continuity

Security Operations Center (SOC)
- 24x7 Monitoring and Response
- Managed Detection and Response (MDR)
- Centralized data analysis

Disk Encryption
- Encrypted disks
- Centralized management

Percentage of cyber attacks that target small business... **43%**

60% of small businesses that are victims of a cyber attack go out of business within six months.

Ready To Learn More?

855.PPL.GUYS PurpleGuys.com
info@purpleguys.com

Managed Detection and Response (MDR) Services

Our MDR Services are split into two categories. Fundamental (F) and Comprehensive (C). Fundamental is intended for non-regulated businesses where security is a business function and not dictated by industry specific regulations. Comprehensive is intended for regulated businesses (Healthcare, Financial, etc…) where industry regulations dictate more stringent requirements. The components of each are outlined below.

Managed Security Component	F	C
Advanced Endpoint Protection The Purple Guys will deploy, maintain, and report on an agent-based, Advanced Endpoint Protection solution for our clients. This solution is designed to prevent execution of malicious software on client computers, as well as provide alerting for any conditions that the endpoint protection tool deems suspicious.	X	X
Managed Detection & Response The Purple Guys will deploy, maintain, and report on an agent-based solution for our clients. This solution is designed to alert on suspicious activities observed by the agent-based solution and allow for further investigation of suspicious activity on hosts with the agent installed. The Purple Guys will leverage this agent where it is necessary to have a closer look at suspicious activity that may indicate an intrusion.	X	X
Active Directory Monitoring & Detection The Purple Guys will deploy, maintain, and report on Active Directory for our clients who use Active Directory. Additionally, the Active Directory solution will provide reporting on areas of risk for our client Active Directory installations.	X	X
Security Alert Response and Reporting The Purple Guys will review security events, and during network security monitoring, evaluate alerts for escalation to IT support staff for action, to include remediation of vulnerabilities, exploits by attackers, and other events that represent realized risk within the client's environment.	X	X
Security Operations Center (SOC) Alert Monitoring and Analysis The Purple Guys will leverage a suite of detective tools to collect data and alerts based on the observed activity in Clients' networks, evaluate the output of these tools, and classify security alerts based on a combination of custom, predefined alert rules, anomalous activity detection, machine learning, and curated threat intelligence to enhance security event detection, discover malicious automation, detect vulnerability exploits, and track attacker activity and/or data exfiltration.	X	X
Vulnerability Assessments The Purple Guys will perform vulnerability assessments of Clients' network-connected devices from The Purple Guys' network sensor device at regular intervals. Current vulnerability data will be pulled daily from national databases to evaluate the security of devices on our clients' network. Each month, a comprehensive vulnerability report will be generated. Vulnerabilities will be ranked according to their CVSS score and potential impact.		X
Log Aggregation & Storage The Purple Guys will deploy and maintain a log forwarding agent for all our clients' servers that exist within the monitored network and for which services are ordered. Server Operating System, application, security, and other logs will be forwarded to an aggregation and storage solution provided by The Purple Guys, where they will be available for search by Security Operations Center (SOC) staff. Logs will be maintained for up to 31 days in indexed, ready search capability, and 3 months of cold storage availability.		X
Network Intrusion Detection The Purple Guys will deploy, maintain, and report on a Network, appliance-based Intrusion Detection System (IDS or NIDS). This system will be updated with the latest available threat intelligence rulesets produced by commercial and other vendors and information sharing organizations on a regular basis. Alerts will be reviewed by the Security Operations Center analysts based on automated sorting using Security Orchestration and Automated Response (SOAR) processing of alert data.		X