



Stopping the bad guys in their tracks.

Cybersecurity is big business.

43% of cyberattacks target small businesses. Why? Because they tend to not have the latest and greatest tools to protect themselves. They're an easy target.

Cybersecurity crime is now one of the largest industries worldwide, costing companies a combined \$100 billion or more each year. Small and mid-sized businesses are preferred targets because these attacks are automated, allowing criminals to easily infiltrate them every day with viruses and ransomware. Often, SMBs are just an entry point into a larger, more lucrative target, like a vendor or client. Traditional security standards like Firewalls and Antivirus are simply not enough to protect your business from vulnerabilities like data theft, lost laptops, viruses and malware.

INVICTAVPS
BY RESULTS TECHNOLOGY

Cybersecurity by the numbers



43% of cyberattacks target small businesses.



70% of customers say they'll stop doing business with a company after a single data breach.



200 days – that's the median number of days that attackers stay dormant within a network before detection.



28,765 records are stolen on average per data breach for businesses with <100 employees.



86% of phishing attacks target the United States.



83% of financial services organizations experience more than 50 network attacks per month and take an average of 98 days to identify an attack.

RESULTS announces a cybersecurity tool specifically for small businesses that rivals what the big guys have. Invicta (Latin for invincible) VPS (stands for Vulnerability Protection System) is one of the most advanced cybersecurity tools available to small businesses today. When used in conjunction with firewalls, backup and antivirus tools, Invicta VPS provides security at a level that is compatible with most regulatory compliance requirements (HIPAA, FFIEC, PCI, NIST, etc.).

Invicta VPS is designed to prevent and detect Advanced Persistent Threats (APTs). These threats sit quietly, harvesting your company's sensitive information, or even worse, your client's information for weeks or even months. APTs can also move around within your network, gain administrative rights, and even access secure areas of your network. APTs are truly one of the worst things that can happen to a company.

But don't worry ... we've got your back. Here's how:

1. Once installed on your network, Invicta VPS gets right to work, enforcing policies on workstations and servers to ensure that only legitimate changes and activities are permitted.
2. The network is scanned daily for failed login attempts, changes to permissions and administrative accounts, changes to network configurations, and malware or "hidden" applications.
3. Invicta VPS detects keyloggers, trojans, spyware, unauthorized registry changes, or other malicious activity.
4. A weekly network scan detects security vulnerabilities on all network-attached devices. External vulnerability scans are run quarterly against public firewall IP addresses.
5. An enhanced Ransomware detection system identifies malignant activity and immediately isolates the infected device and initiates corrective action.
6. Lost or stolen devices can be locked down and data destroyed on first connection to the internet.
7. All detected anomalies and alerts are forwarded to the RESULTS help desk for rapid remediation.
8. All reportable events are captured and analyzed by the RESULTS help desk and actions are logged in the Invicta VPS portals.
9. RESULTS technical staff work to remediate persistent issues to keep them from happening again.

10333 W. 84th Terrace,
Lenexa, Kansas 66214

913.928.8300

info@resultstechnology.com
www.resultstechnology.com

