

ESSENTIALS BUNDLE

IBM i DATA SECURITY SERVICES

IBM i IS SECURABLE - BUT HOW PROTECTED IS YOUR ENVIRONMENT?

Running on IBM Power, your IBM i environment may be connected to your Intel, Linux, or Opensource platforms, which could be on-premises, hosted, SaaS or outsourced. You may also share data with external business partners.

Connectivity across your network provides many pathways into your IBM i servers holding your key applications and data. On a good day all of the layers of security in your environment will be configured and patched correctly and in a timely manner to protect your IBM i server. If your environment is targeted, it only takes a single misconfiguration through human error, or lack of knowledge, to grant access to bad actors. They can steal or encrypt your IBM i data or even damage the OS to a point where it has to be restored.

As a minimum protection for your IBM i LPARs and data you should only allow authorized users and services to access the IBM i LPARs and ensure they remain protected from malware and ransomware. This line of defence is a basic requirement of compliance frameworks - a software firewall for the IBM i server and LPARs.

TRUSTED TECHNOLOGY PARTNERS



IBM i DATA SECURITY OVERVIEW

Discover the benefits, outcomes, and responsibilities behind our IBM i data security starter bundle.

BENEFITS

- IBM i Server protected from bad-actors or accidental breach
- Data and applications protected from theft/ encryption/deletion by malware
- Operations teams and/or security/compliance team notified of breach attempts and existence of malware on the server

OUTCOMES

- IBM i foundations to provide perimeter software firewall and virus protection
- Address minimum compliance requirements
- Ability to integrate events to SIEM/SOC service to provide event data for incident response and cyber resilience

WHAT YOU DO

- Identify users and services that are authorized to access the IBM i LPAR
- Confirm process for notification of invalid access attempts, virus found and ransomware blocked
- Incorporate IBM i security events in your SIEM or SOC service
- Include IBM i in your Cyber Incident Response Plan

WHAT WE DO

- Install and configure end-point protection
- Configure rules to block any unauthorized users or services from the IBM i
- Set-up monitoring solution to send security alerts to your named security/compliance owners
- Provide monthly access reports to the security/compliance owners.



GROW



SAVE



INNOVATE



PROTECT

SECURITY 'STARTER BUNDLE'

Here's what to expect from our cutting-edge starter bundle for IBM i security.

AV SOLUTION

Keep your environment safe from viruses, worms, Trojans, and other malware using the *only* antivirus solution native to IBM Power Systems.

Our solution gives you:

- Enterprise scanning technology
- Heuristic Analysis
- Automatic Updating & Scanning

INSIDE THIS BUNDLE:

- Protection
- Regular Updates & Upgrades
- Real-time scanning
- Scheduled scanning
- Reporting & Alerts
- Incident Management
- Compliance
- Integration
- Customer Support



ARE YOU SECURE?

While IBM Power Systems are generally less susceptible to viruses due to their unique architecture and proprietary operating system (IBM i), they are not entirely immune. Thus, our robust antivirus protection remains an essential part of your system's defense.

EXIT POINT MANAGER

As your dedicated Managed Service Provider, Tectrade offers a comprehensive **Exit Point Manager Service** for IBM Power Systems, ensuring you remain protected from costly security breaches by tracking and monitoring data access.

Get a free, non-disruptive security scan today.



Tectrade Computers Corporation

8480 Honeycutt Road
Suite 200
Raleigh, NC 27615

CONTACT INFO

info@tectrade.com
www.tectrade.com