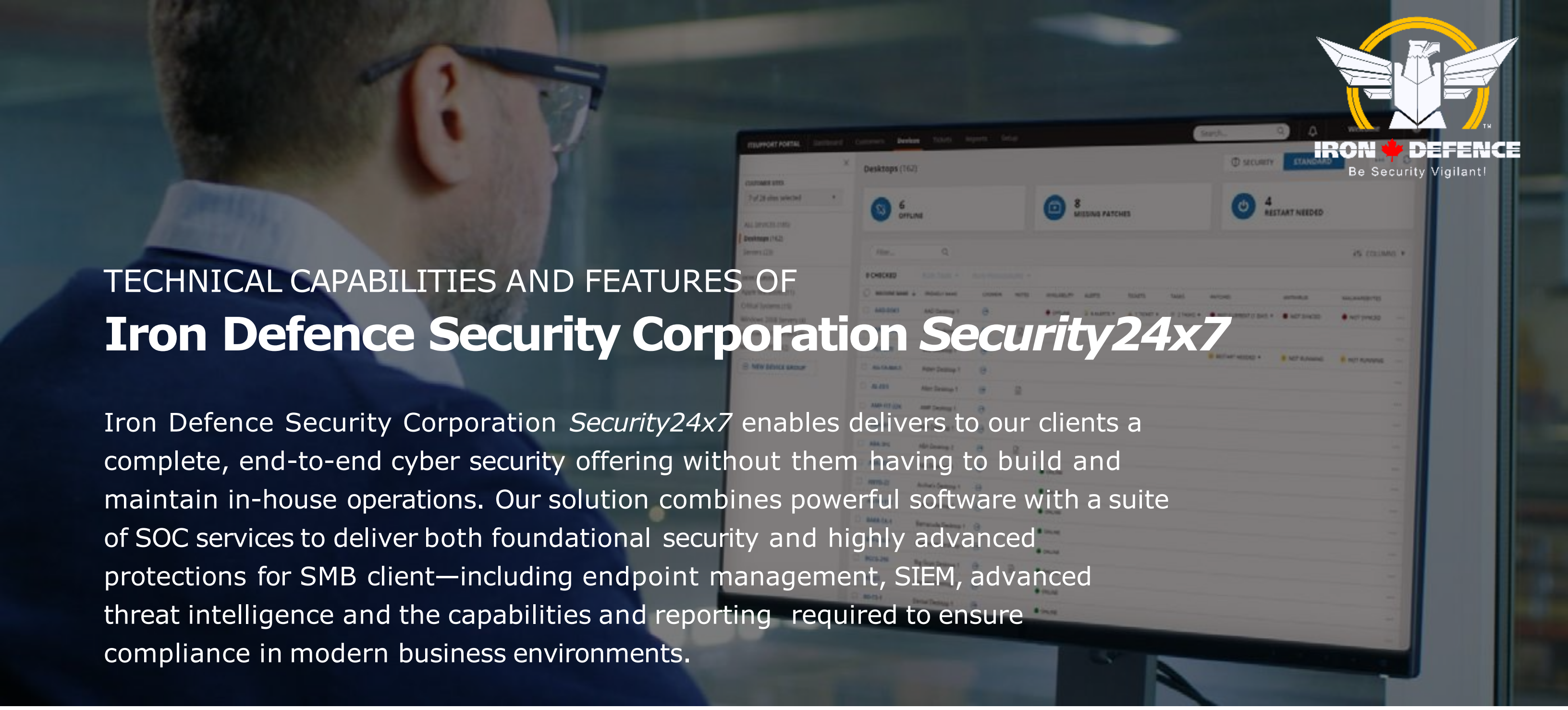

TECHNICAL CAPABILITIES AND FEATURES OF

Iron Defence Security Corporation *Security24x7*

Iron Defence Security Corporation *Security24x7* enables delivers to our clients a complete, end-to-end cyber security offering without them having to build and maintain in-house operations. Our solution combines powerful software with a suite of SOC services to deliver both foundational security and highly advanced protections for SMB client—including endpoint management, SIEM, advanced threat intelligence and the capabilities and reporting required to ensure compliance in modern business environments.

Iron Defence Security Corporation *Security24x7* empowers our clients and their technical teams to better-support their organisations in the following ways:

1. The ability to accurately define and address security services by leveraging pre-built or custom “profiles” that map to specific attack vectors and protection needs, with real-time alerting when a system or site reaches risk levels that are above security-controlled thresholds.

2. Advanced detection and response capabilities to identify and isolate any active threats or suspicious activity, with included documentation and recommended remediation steps to help avoid future issues.

3. Access to our fully-staffed SOC facility which provides 24x7 threat detection, mitigation and remediation, and possesses the advanced cyber security knowledge and expertise needed to help us deliver security services to our SMB clients.

Iron Defence Security Corporation *Security24x7* delivers these benefits through three distinct products: *Profile & Protect, Detect & Respond – Iron Endpoint* and *Detect & Respond – Iron Network*.

Profile & Protect

Profile & Protect features pre-built and customizable profiles that identify specific gaps in protection on client devices, helping us identify potential vulnerabilities and take corrective action where needed.

These “profiles” represent collections of security tools and configuration, and each profile explains exactly which technologies should be in place based on what’s being protecting against, and offers advanced alerting and risk scoring so you can accurately measure risk on a per-site or per-device basis.

Once a profile is applied, the agent continuously monitors the endpoint and will report back any categories or issues that are identified as out of compliance. This information is then used to calculate a risk score. Each profile has a set number of risk points, which is determined by the active categories and levels of importance noted during configuration. Profiles and risk factors can include insights such as:

- **Antivirus software is not installed or not up to date** —This requirement is satisfied when an antivirus software package that is supported by Iron Defence Security Corporation is installed and up to date with the latest definitions.

- **DNS protection is not configured** —Validates that the endpoint is configured for DNS Protection.

- **User not configured for password complexity** —Validates that password complexity rules have been applied to user accounts.

Features & Benefits

Simplified Risk Monitoring

Shift from analyzing risk in a siloed, limited view to determining true risk and vulnerability management through continuous, active monitoring from a unified dashboard.

Automated Prioritization

Reduce the noise associated with responding to security gaps by setting custom alert thresholds. Through risk scores and tickets, you can prioritize work on endpoints that are more susceptible to a potential breach or security incident.

Time Efficiency

Leverage risk-based views of security gaps to remain focused on real risks—and effectively separate false positives from active threats.

Maximum Client Impact

Identify common factors and patterns that are lowering risk scores across multiple systems to quickly drive large-scale improvements in client environments.

Out-of-the-Box Reporting

With visibility into the list of profiles, number of devices assigned to each profile, average risk score and more, you can automatically generate compelling client-facing reports to articulate current risk and the effectiveness of your services. Historical reporting is also included to enable you to clearly communicate and demonstrate actions you've taken to improve your clients' security over time, or to show your response to a particularincident.

Policy Compliance

Create custom profiles that represent your internal policies to continuously monitor and report against compliance with those policies and identify areas for improvement or optimization.

Quick Landscape View

Compare the state of your security environment to expertly crafted security profiles that represent today's top security risks to derive opportunity.

Detect & Respond -Iron Endpoint

Detect & Respond – Iron Endpoint provides fully SOC-supported endpoint monitoring and threat detection to identify active threats and remediate attacks. Iron Defence Security Corporation *Detect & Respond – Iron Endpoint* builds on foundational security to rapidly identify and halt even the most sophisticated attacks, minimizing harm and reducing risk to client endpoints.

Features & Benefits

Simple driven Operation

Automate and easily implement advanced operations without the need for in-house security expertise.

AV/Malware Detection

Rapidly identify thousands of variants of viruses and malware.

Immediate Rollback

Quickly respond to detected ransomware variants by leveraging journaling to roll back to an acceptable riskstate.

Full Rollback Capabilities

In the case of any over written systems, you can leverage robust rollback functions through comprehensive tracking of changes at the endpoint.

Endpoint Attack Forensics

Identify the root causes of malicious behaviors by quickly diagnosing source processes and applications.

Complete SOC Services

Reduce false positives and ensure comprehensive protection through SOC analysis of quarantined applications and files.

Ransomware Warranty

Our insurance will pay up to $1,000 per infected machine towards the cost of paying the ransom if they don’t defend against or can’t rollback and restore data after a ransomware attack (up to $1M) has occurred on a covered machine.

Detect & Respond – Iron Network

Detect & Respond – Iron Network leverages industry-leading SIEM technology to collect, analyze and correlate information from network devices, endpoint logs and threat intelligence feeds. This information is used to identify security incidents, policy violations, fraudulent activity, and other threats — and when such activities are identified, the Iron Defence Security Corporation SOC quickly takes action to mitigate the attack while providing advanced remediation documentation and recommended next steps.

Features & Benefits

No Additional Agent

Provides network coverage without an additional agent on every endpoint.

Endpoint Log Monitoring

Monitor key log files to identify and correlate events that could be malicious, while providing additional security and adherence to common regulatory requirements.

Common Network Device Monitoring

Easily leverage out-of-the-box integrations with networks devices commonly seen in SMB client environments.

Behavioral Analysis

Quickly detect and address changes in systems and user behaviors with real-time processing and advanced correlation rules for intrusions & insider threats.

Threat Intelligence Integration

Enable a quick and accurate detection of threats on a network by integrating with valuable threat data feeds from ecosystem partners and open source providers.

Meet Common Regulatory Requirements

Adheres to log management and threat analysis requirements for 23 regulatory standards.

SOC Analysis and Basic Response

With analysis of events and basic remediation actions by the Iron Defence Security Corporation SOC, you can adhere to compliance regulations without needing additional security-focused resources.