ITQSOFT CYBER SECURITY SOLUTIONS OVERVIEW

Data Sheet

INTRODUCTION

Cyber security has become one of the keys to keeping your business not just healthy, but also competitive in the modern business environment. As a top-notch IT services provider for more than a decade, we've seen the security landscape evolve and have designed a set of solutions specifically to meet the needs of small and mid-sized businesses (SMB).

Unlike most security providers, we work with SMB clients every day and understand your environment, risks, and budgets. We've created a set of affordable solutions that together create a comprehensive cybersecurity program to safeguard your data, help meet your compliance requirements and give you a significant competitive advantage.

This overview provides a summary of ITqsoft's Managed Security Services including:

- Multi-Factor Authentication

- Phishing Prevention Training

- Virtual CISO

- Intrusion Detection and Response

- Vulnerability Scanning and Remediation

- Endpoint Detection and Response

MULTI-FACTOR AUTHENTICATION

Once an attacker steals an employee or customer password, it's game over - unless you have multi-factor authentication (MFA) in place. MFA ensures that only verified users can access your important business data, by requiring more than just a password before access is granted.

MFA adds an extra layer of protection by requesting an extra authentication token - usually in the form of a random one-time password delivered either via text, phone call, or mobile app. In a world full of phishing and social engineering, attackers WILL gain access to your accounts and networks unless you've locked down remote access with MFA.

ITqsoft's MFA solution is incredibly easy to use. When an employee enters in their credentials to access the MFA protected application or service, they will immediately be sent a mobile push notification which will pop up on their registered device. All the user has to do is tap a green button to accept and they will be immediately granted access.

Using ITqsoft MFA, you can easily protect as many applications as you want, from your VPN to Salesforce, Microsoft Office 365, G-Suite and many more.

PHISHING PREVENTION TRAINING

According to the 2018 Verizon Data Breach Investigation Report, 93% of data breaches start with phishing attacks or social engineering. These attacks usually involve a fake email that purports to be from a trusted source, and which lures its target into giving up account information or clicking on a viral payload. It's vital that your workforce be able to screen out phishing attacks.

Our phishing prevention training services go above and beyond most programs, which simply remind employees about phishing attacks once a year. By contrast, ITqsoft offers in-depth campaigns designed by our experts, that help you understand which of your users are phishing experts and which need additional training.

With the right training, your users can evolve from security liabilities to network defenders, reducing the risk of malware, stolen accounts, leaked information, and unauthorized funds transfers.

VCISO (VIRTUAL CHIEF INFORMATION SECURITY OFFICER)

Many small businesses can't afford a full-time strategic director of information security who reports to the board - a Chief Information Security Officer, or CISO. This position is no longer a luxury just for Fortune 500s, it's accessible to all SMBs that need to budget carefully for technology and security. A vCISO can help you chart a course that emphasizes value and optimizes the return on your security investment.

ITqsoft's virtual CISOs are born and bred in the world of SMBs and non-profits. For a certain number of hours per month, you can tap into the knowledge, experience, and creativity of one of our senior security staff. They'll help you develop and implement policies that will help ensure security that's effective not just from day-to-day, but from year-to-year.

By helping to direct your investments and advising one your security posture, you'll be able to avoid major breaches and cope with massive regulatory upheavals such as GDPR and NIST 800-171, and stay well ahead of your competition when it comes to providing the type of secure environment your customers expect.

ADVANCED INTRUSION DETECTION AND RESPONSE (IDR)

As far as data breaches are concerned, time is the enemy. Research from the Ponemon institute shows that on average, it takes organizations almost 200 days to detect a breach. Every day is an added expense.

The ability to detect attacks in real-time and stop them before they can do real damage is the key to keeping your organization safe, costs under control and your reputation intact. Having an advanced Intrusion Detection and Response (IDR) solution in place is now a must for many organizations, especially those who are concerned with rigorous compliance requirements.

In the past, automated security systems with a dedicated incident response team were far too costly, but this has changed. ITqsoft's IDR managed service now makes this type of protection accessible to businesses of all sizes and budgets.

Our comprehensive 24/7 threat monitoring, identification and remediation solution recognizes attackers within seconds, and is backed by a team of security experts who quickly decide on the right course of action without disrupting your business workflow.

VULNERABILITY SCANNING AND REMEDIATION

Usually when attackers gain access to a network, they are limited to a low-level account on one computer. The hackers then seek to "move laterally," or shift to more important systems. At the same time, they try to elevate their level of access from that of an ordinary user to an administrator.

Much of the time, attackers look for missing patches and insecure settings to enable them to do just that. Closing off vulnerabilities essentially maroons the hackers on a desert island with nothing to do and nothing to steal. It also provides a security team with valuable time in which to detect and remove them.

ITqsoft Vulnerability Scanning and Remediation services will regularly scan your network for the kinds of vulnerabilities attackers target: missing security patches, insecure settings, unneeded services. We analyze and prioritize the scan findings and then address them, closing the loopholes before an attacker can exploit them and create havoc in your organization.

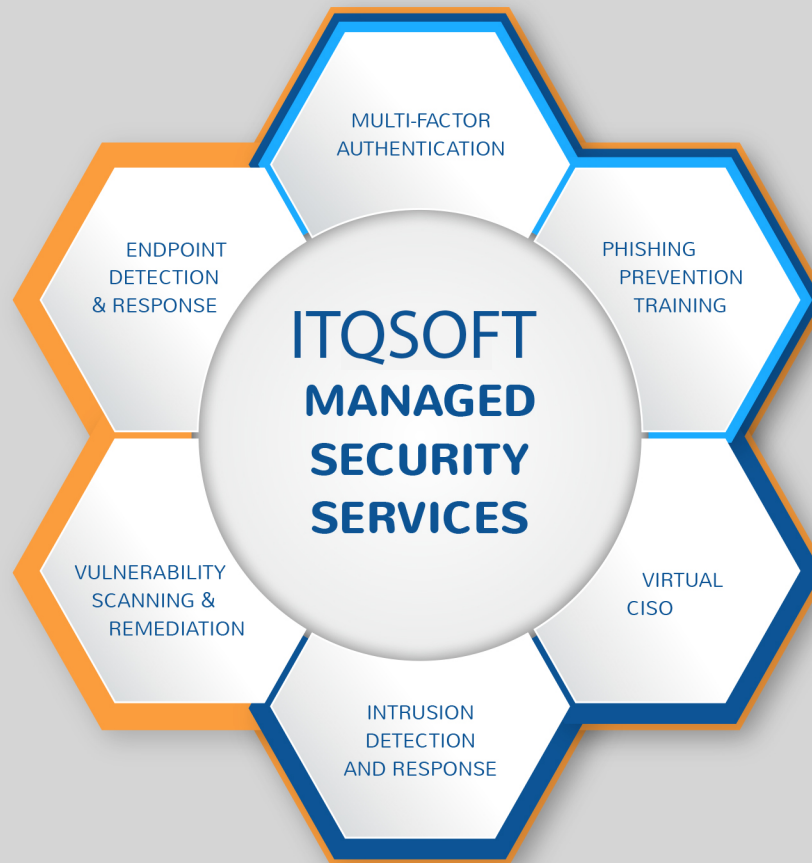# ADVANCED ENDPOINT DETECTION AND RESPONSE (EDR)

Modern antivirus software can protect your computers from simple attacks, but isn't much help protecting you from a determined attacker or modern hacking techniques, where attackers change their tactics in real-time.

The majority of cyberattacks are now mostly concentrated on endpoints - computers and servers - where businesses stores important data. Since businesses may have dozens or hundreds of endpoints which are often remote, it's difficult for administrators to implement continuous monitoring.

ITqsoft's advanced EDR solution uses powerful artificial intelligence (AI) techniques to identify suspicious activity and respond immediately, faster than attackers can change their tactics. Our unique real-time approach is powered by state-of-the-art automated software, backed by a team of expert security resources who operate 24/7 to investigate alerts and determine the right course of action.

ITQSOFT
Quality IT Solutions

While cyber security needs vary based on organizational size and the type of data being protected, every organization needs foundational IT management and security.

ITqsoft offers a comprehensive suite of Managed Security Services that can meet the needs and budgets of almost every organization. Below is a high-level guide, however, there is seldom a one-size-fits-all approach when it comes to cybersecurity. Please consult with us to determine which solutions are the best fit for you!

MULTI-FACTOR AUTHENTICATION

ENDPOINT DETECTION & RESPONSE

PHISHING PREVENTION TRAINING

ITQSOFT **MANAGED SECURITY SERVICES**

VULNERABILITY SCANNING & REMEDIATION

VIRTUAL CISO

INTRUSION DETECTION AND RESPONSE

Small organizations, fewer than 50 people and without large amounts of personally identifiable information or health information.

Organizations with 100-200 employees or that have large amounts of personally identifiable information or health information.

Organizations of 200+ employees, defense and federal contractors.

Contact Us to Consult with an ITqsoft Security Expert