Your Success. Secured.

NTIVA MANAGED SECURITY SERVICES

Stand-Alone Service Package

Solution Sheet

7900 Westpark Drive, Suite A100 | McLean, VA 22102
1-888-996-8482 | www.ntiva.com

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).

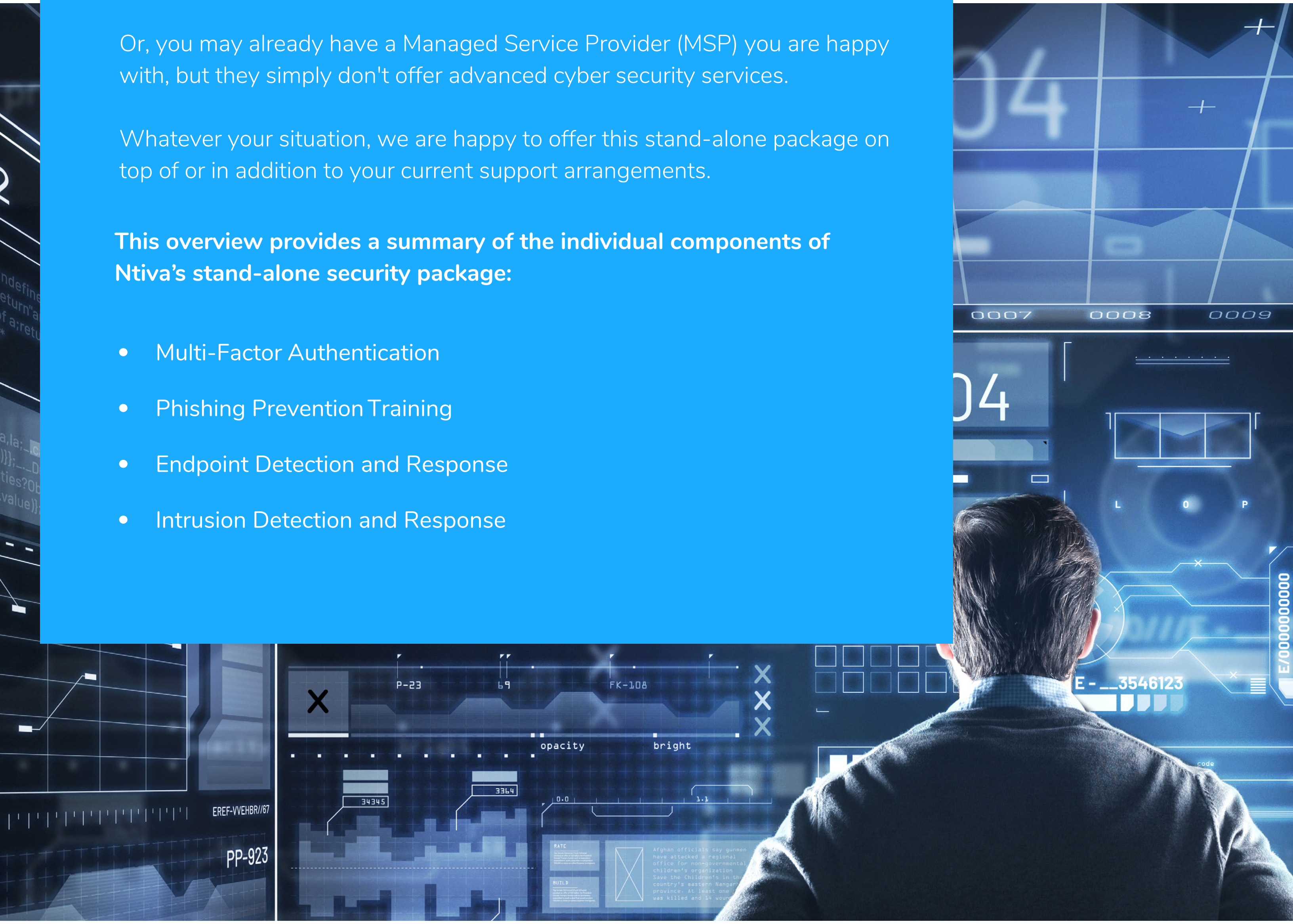
Unlike most security providers, we work with SMB clients every day and understand your environment, risks, and budgets. We've created a stand-alone security package that we're offering to businesses who may already have an in-house IT team, but are looking for expertise and systems they simply don't have access to.

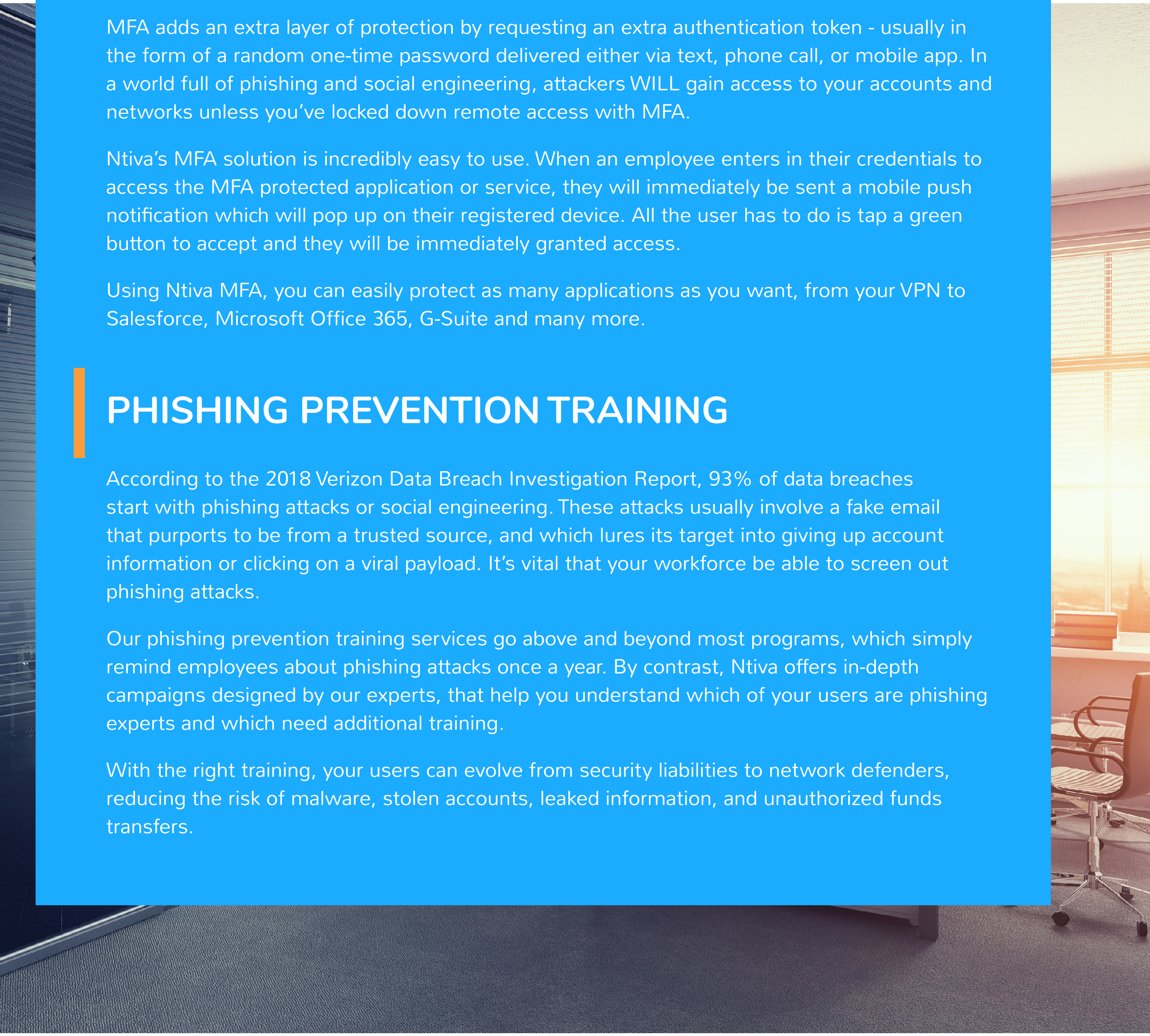
Or, you may already have a Managed Service Provider (MSP) you are happy with, but they simply don't offer advanced cyber security services.

Whatever your situation, we are happy to offer this stand-alone package on top of or in addition to your current support arrangements.

This overview provides a summary of the individual components of Ntiva's stand-alone security package:

- Multi-Factor Authentication
- Phishing Prevention Training
- Endpoint Detection and Response
- Intrusion 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.

Ntiva'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 Ntiva 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, Ntiva 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.

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.

Ntiva'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.

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. Ntiva'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.