# MAGENTO WEBSITE SECURITY REPORT

30th April 2021

FOREGENIX

Making Cyberspace Safer for Everyone

# ABOUT FOREGENIX

We are a global cybersecurity firm founded in 2009 by renowned industry experts to help make the cyberspace safe for everyone. With over a decade of experience in the market, we provide critical cybersecurity services to the payment industry, banking, manufacturing, travel, aerospace and government sectors.

Our Elite Team of cybersecurity experts include backgrounds such as IT, law enforcement, counter-terrorism, military, development and scientists from different fields. We combine their knowledge and experience to create services and solutions that, coupled with our in-house technology, protect businesses like yours from cybercriminals and keep your digital assets under control.

From first contact to final delivery, we commit to providing a **strong cybersecurity** posture well beyond compliance

COMPLIANCE & CONSULTING

OFFENSIVE OPERATIONS

DIGITAL FORENSICS & INCIDENT RESPONSE

CYBERSECURITY SOLUTIONS

# WHAT IS WEBSCAN?

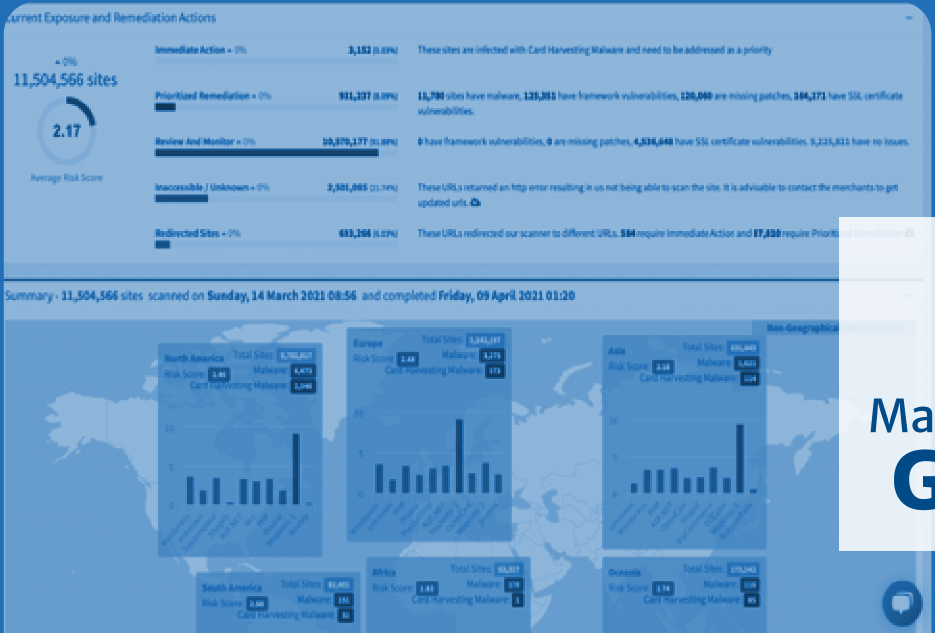
WebScan is our comprehensive non-intrusive website scanning solution. It analyses websites for specific security vulnerabilities to produce a risk score.

The scans are not intrusive, WebScan looks for publicly available information (just like criminals do), and at no point does it try to exploit vulnerabilities.

WebScan detects:

- **MALWARE** (Including card skimmers)
- **PLATFORMS AND PATCHING ISSUES**
- **TLS/SSL VULNERABILITIES**

We like to say that WebScan is **the most up-to-date website scanning solution in the market,** as it is constantly updated by both our **Forensic Team and Threat Intelligence Group.**



Current Exposure and Remediation Actions

▴ 0%
11,504,566 sites
2.17
Average Risk Score

Immediate Action ▴ 0% **3,152** (0.03%) These sites are infected with Card Harvesting Malware and need to be addressed as a priority

Prioritized Remediation ▴ 0% **931,237** (8.09%) **11,780** sites have malware, **125,201** have framework vulnerabilities, **120,060** are missing patches, **184,171** have SSL certificate vulnerabilities.

Review And Monitor ▴ 0% **10,570,177** (91.88%) **0** have framework vulnerabilities, **0** are missing patches, **4,536,648** have SSL certificate vulnerabilities. 5,225,821 have no issues.

Inaccessible / Unknown ▴ 0% **2,501,085** (21.74%) These URLs returned an http error resulting in us not being able to scan the site. It is advisable to contact the merchants to get updated urls.

Redirected Sites ▴ 0% **453,266** (4.13%) These URLs redirected our scanner to different URLs. **584** require Immediate Action and **87,158** require Prioritized Remediation

Summary - **11,504,566** sites scanned on **Sunday, 14 March 2021 08:56** and completed **Friday, 09 April 2021 01:20**

We monitor over
**240,000**
Magento Merchants
**GLOBALLY**

# RISK CATEGORIES

## CRITICAL – Compromised

Confirmed as compromised and actively running different types of malware. Cardholder data must be assumed fully compromised.

## HIGH – At serious risk of being easily hacked

Presents serious vulnerabilities and may be already compromised or at risk of being breached by an opportunistic attacker

## MEDIUM – Risk of breach

Vulnerabilities have been found that need attention, the site is at risk of being breached by a seriously organised threat actor.

## LOW – Hacking unlikely

Vulnerabilities have not been detected, active monitoring is still highly recommended.

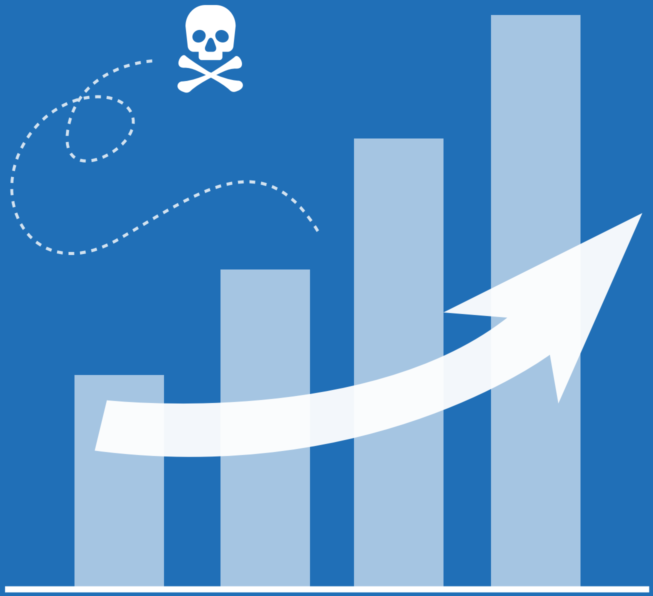
# REPORT SUMMARY

Nearly **140,000** websites still remain on the **Magento 1** platform.

The number of Magento websites in our dataset is over **240,000**

Critical **Magento 2** websites **INCREASED BY 33%** in the last 2 weeks

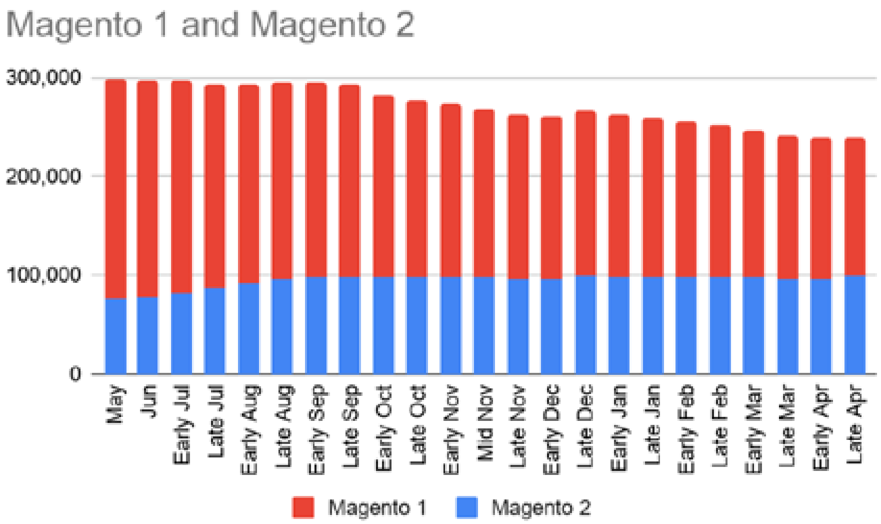
**25% of Magento 2** websites are either Critical (compromised) or High risk.



**Magento 1 and 2 remain the most targeted eCommerce platforms**

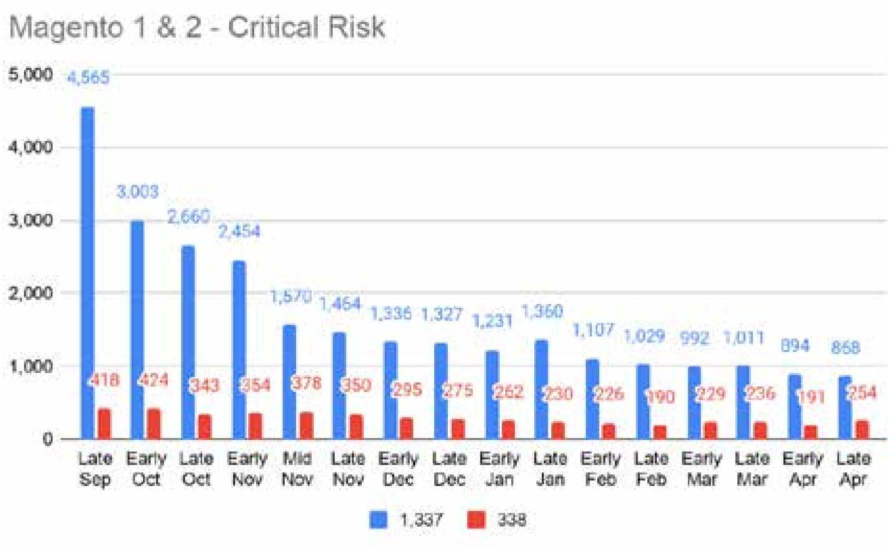
# RESULTS

## Magento sites reviewed


Magento 1 and Magento 2

Current dataset over **240,000** Magento sites

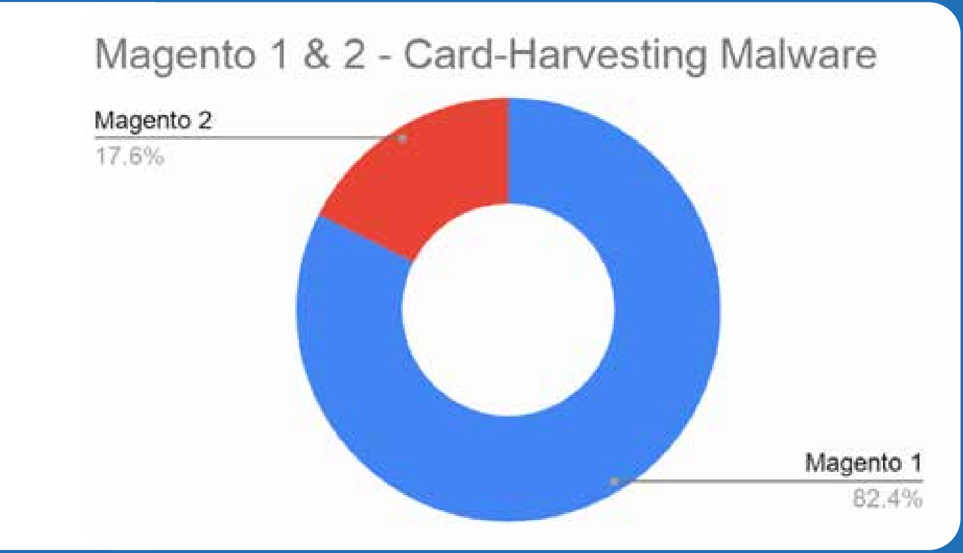
## Magento sites compromised


Magento 1 & 2 - Critical Risk

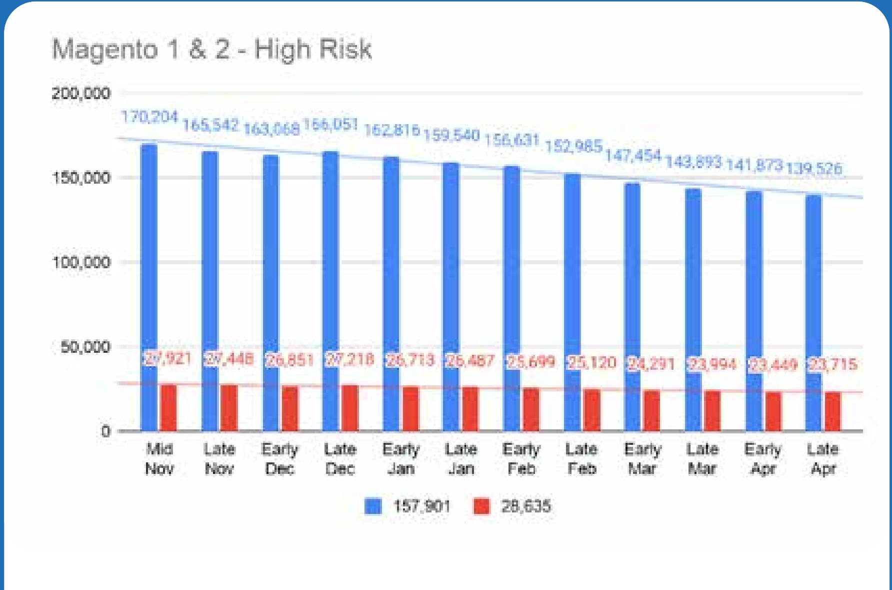
Well over **1,100** Magento sites are compromised

# RESULTS

## Card Harvesting Malware Distribution



## High Risk Websites



Websites identified as High Risk have significant security issues that make them very vulnerable to criminals and require attention.

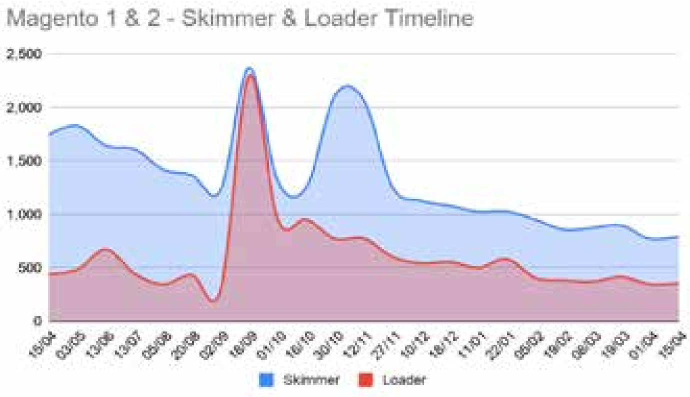
The sites have one or more of the following:

- Missing critical framework security patches
- Have known framework vulnerabilities
- Missing basic hardening or have similar configuration issues
- Non–card harvesting malware

**Note:** Magento 1 has reached its End Of Life and therefore security updates are very unlikely to be released in the future. Staying on this platform pose an immediate threat. For this reason, Magento 1 sites will be classified as High Risk onwards.

# RESULTS

## Magento 1 & 2 – Loaders & Skimmers

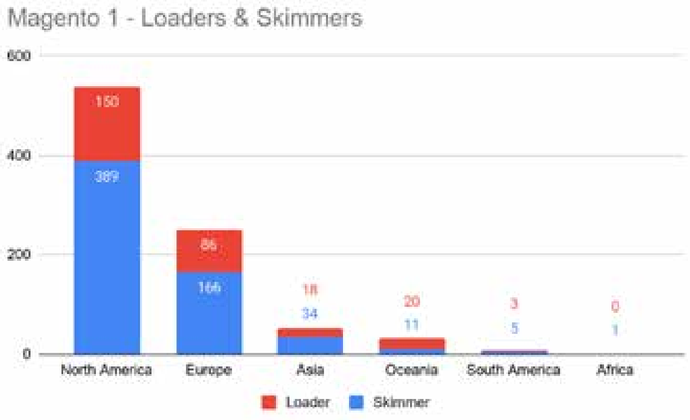


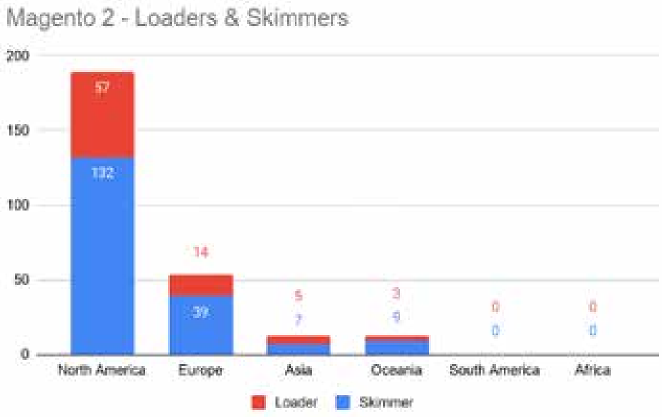
We also track how many websites are infected with loaders and skimmers.

**Loaders** are small pieces of code designed to load in additional malicious code onto a website.

**Skimmers** are malicious scripts designed to scrape card data and customer information from a site's payment page before sending them off to the attacker.

The charts to the right show which regions in the world have the highest infection rate, and below shows change over time.





# RESULTS

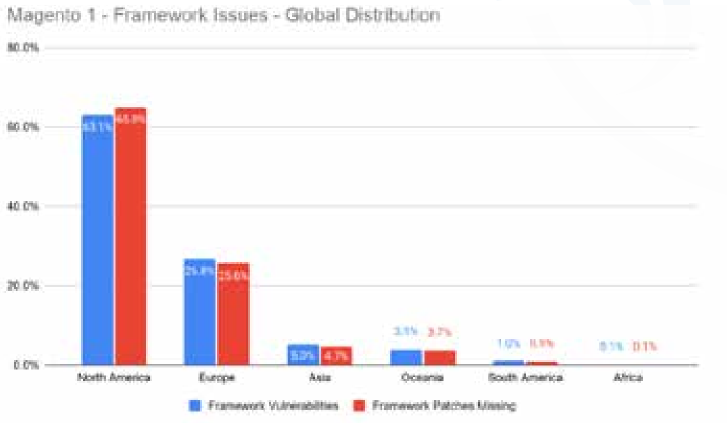
## Framework Issues Distribution

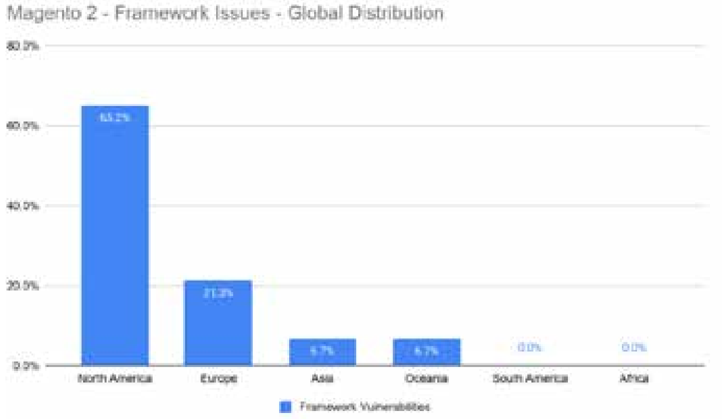
**Framework Vulnerabilities** are usually serious bugs in the software used to run your website. This category also include insecure website set-up, such as leaving default settings in place (e.g. admin panel location, etc.).

**Framework Patches Missing** means your website is missing security patches/updates that are already available.

It's good to note that patching in Magento 2 works a bit differently than in Magento 1. With Magento 1, standalone security patches used to be released. This meant that websites could install these patches over older versions of Magento 1 selectively, keeping the sites secure against the latest threats without having to update the entire framework.

With Magento 2, Adobe typically offers a single security patch for the previous version, whenever a new version is released. This gives merchants some flexibility when it comes to upgrading their sites, however they will eventually need to perform a full version upgrade to remain secure.

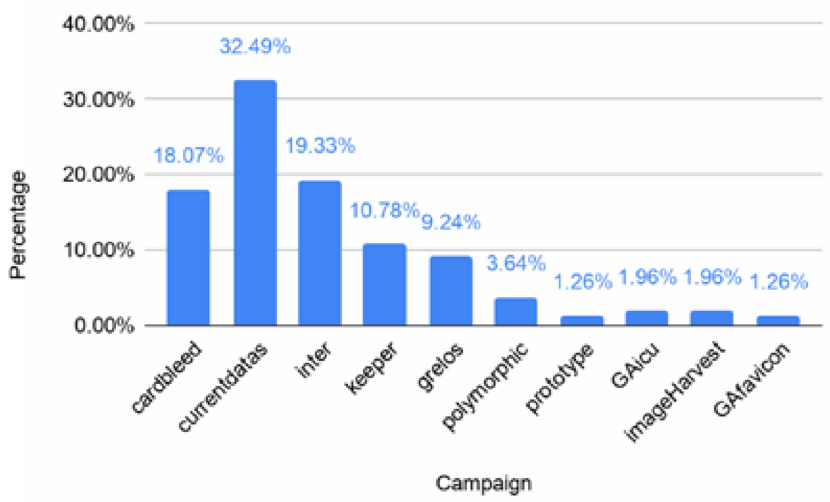




# RESULTS

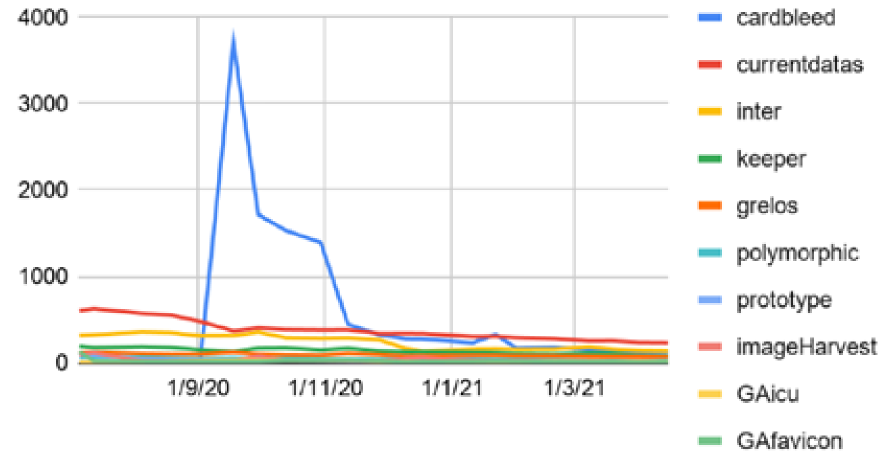
## Malware Campaigns

These are the Top 10 types of malware identified in our most recent Magento scan. *currentdatas* is the malware that we have seen the most, and after a period of stability, *inter* has grown in numbers and now occupies second place.



# MALWARE TRENDS

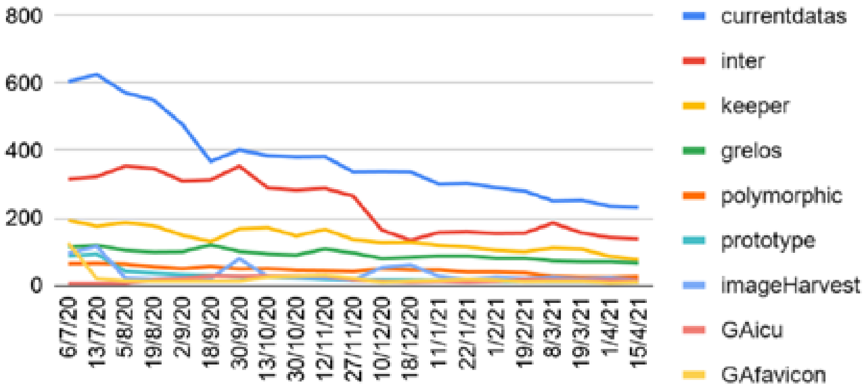
## Distribution of malware types



Foregenix is tracking the malware types that are infecting Magento websites. Due to the **Cardbleed** attack in September 2020, we have broken the data into two graphs.

The first graph shows how all Top 10 malware combined compares with the spike of **Cardbleed**, while the second graph shows the trend over time without it.

## Without Cardbleed



# INSIGHTS

A steady but slow decline in the number of websites using Magento 1 continues to evolve, with **Magento 1 remaining the most targeted eCommerce platform** on the internet. Within the Magento ecosystem, we have seen an uptick in the proportion of compromised Magento 2 sites, which supports the anecdotal evidence received through our forensic and support teams.

Of concern is the regular expectation that Magento 2 sites no longer need a strong focus on security – **we expect the numbers of hacked Magento 2 sites to continue to grow** in proportion to Magento 1 as a result of this misunderstanding in the industry.

For free guidance on how to improve your website security, check out our Magento Security Insights page.

If you are ready to adopt a website security solution or invest in cyber insurance, please get in touch with sales@foregenix.com

# ADDITIONAL RESOURCES

**Magento Security Insights Page**

foregenix.com/magento

**Use our free scanner to understand your website security posture**

foregenix.com/webscan

**Try out our website security solution, FGX-Web**

foregenix.com/fgx-web

# WHY FOREGENIX

## Experience

Cybersecurity experts with extensive hands-on experience. Qualified, recognised and certified professionals.

## Sense of Duty

Real commitment to help simplify complex topics and protect business continuity.

## Research and Development

Passionate about Cybersecurity and its continual challenges. Consistently learning and researching to stay ahead of the curve by developing skills, tools and methodologies.

## Global, but Local

We have active analysts, consultants and investigators in every continent. We source and nurture talent where our customers are.

# GET IN TOUCH

### United Kingdom (HQ)

Foregenix Ltd.
8 9 High Street,
Marlborough
SN8 1AA

+44 845 309 6232

### North America

Foregenix Inc
75 State Street, 1st Floor
Boston, MA, 02109
USA

+1 877 418 4774

### Europe

Foregenix Germany
GMbH.
Betzelsstrabe 27, 55116
Mainz, Germany

+49 6131 2188747

### MEA

Foregenix (Pty) Ltd.
Sec H, Blg E, Coachman's
Crossing Office Park 4 Brian
Street, Lyme Park, Sandton,
South Africa

+27 860 44 4461

### APAC

Foregenix (Pty) Ltd.
1 Market Street, Sydney
NSW 2000
Australia

+61 420 904 914

### LATAM

Foregenix do Brasil
São Paulo
Brazil

+55 (11) 98781-4241

FOREGENIX

sales@foregenix.com