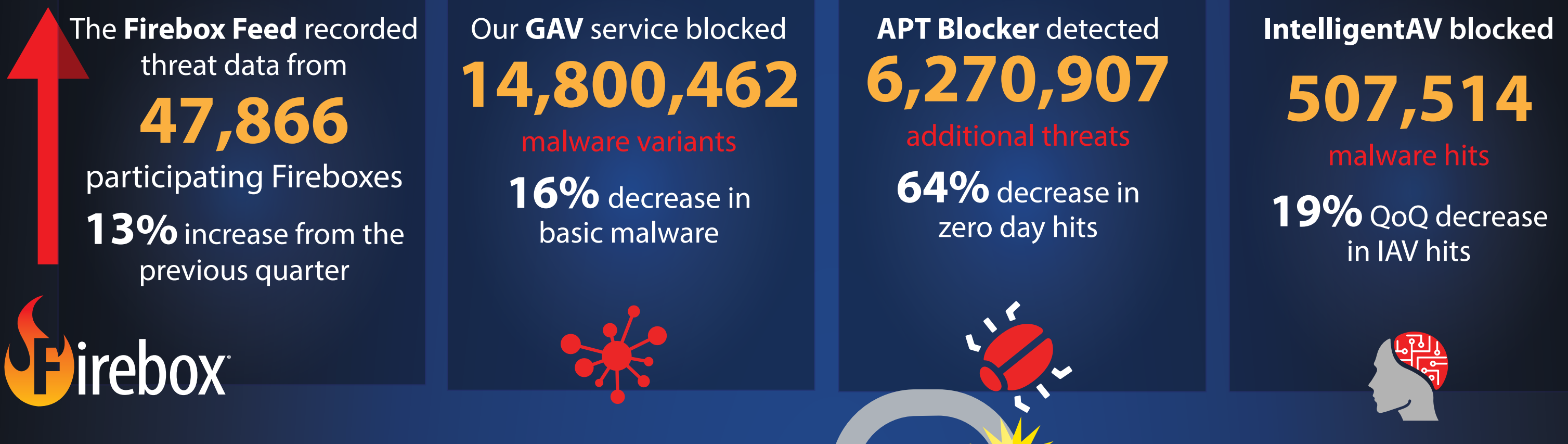# Q3 2020 Internet Security Insights
WatchGuard Threat Lab

The WatchGuard Threat Lab team is a group of analytical, science-based threat experts who want to help you truly quantify the cyber threats your business faces. By statistically measuring the most relevant risks, we help you validate your security strategy with practical defense tips and mitigations. Our quarterly Internet Security Report (ISR) contains measurable threat intelligence on the most prevalent and far-reaching malware, the top network attacks seen in the wild, and the common malicious domains victimizing your employees and users.

Malware Trends

The **Firebox Feed** recorded threat data from
47,866
participating Fireboxes
13% increase from the previous quarter

Firebox

Our **GAV** service blocked
14,800,462
malware variants
16% decrease in basic malware

APT Blocker detected
6,270,907
additional threats
64% decrease in zero day hits

IntelligentAV blocked
507,514
malware hits
19% QoQ decrease in IAV hits

50.6%
OF MALWARE WAS
ZERO DAY

49.4%
OF MALWARE WAS
Known Malware

High-Level Threat Trends for Q3 of 2020

Attackers probed **nearly half of the Fireboxes** in the United States for weaknesses in a popular SCADA-related industrial control system solution.

Overall perimeter-detected malware is down 26% quarter-over-quarter (QoQ), which we have started to expect due to COVID-19 and many employees working from home.

New and Notable Threats
Let's take a look at a few of the top threats from this quarter's report.

SCADA Systems
This quarter saw a large number of network attack detections targeting a popular supervisory control and data acquisition (SCADA) system. Attackers probed nearly 50% of U.S. networks looking for systems vulnerable to this attack.

Happy Clickers
The average organization had 499 connections blocked by WatchGuard's DNS firewalling service DNSWatch. Of those average connections, 262 were destined for domains hosting malware and 52 were a part of active phishing campaigns.

LokiBot Look-Alikes
There was a surge in banking trojans resembling the popular LokiBot in the top malware detections for Q3 2020. Threat actors create these trojans to steal credentials, disable endpoint protections, and deploy additional malware payloads.

Malware Detection by Region

AMERICAS 30.7%

EMEA 38.5%

APAC 30.7%
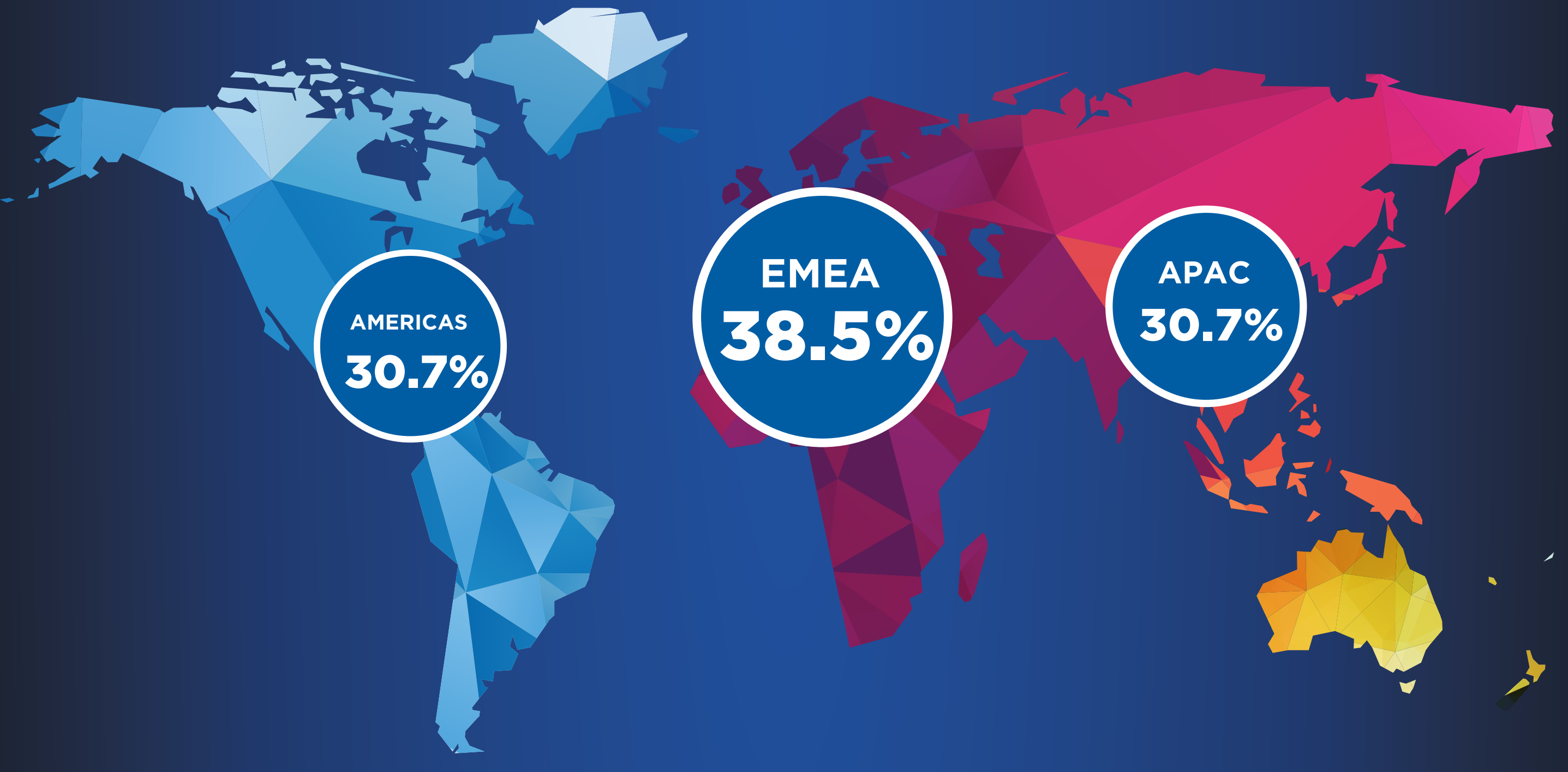
Win32/Heri took the number one spot with **394,253** detections this quarter, which represents **13%** of all the malware we saw.

COUNT	THREAT NAME	CATEGORY	LAST SEEN
394,253	Win32/Heri	Scam Script	Q2 2020

Firebox Feed included threats captured from
47,866 Firebox appliances
deployed across the world

In Q3 2020, WatchGuard Fireboxes blocked over
3.3 million
network attacks

Firebox
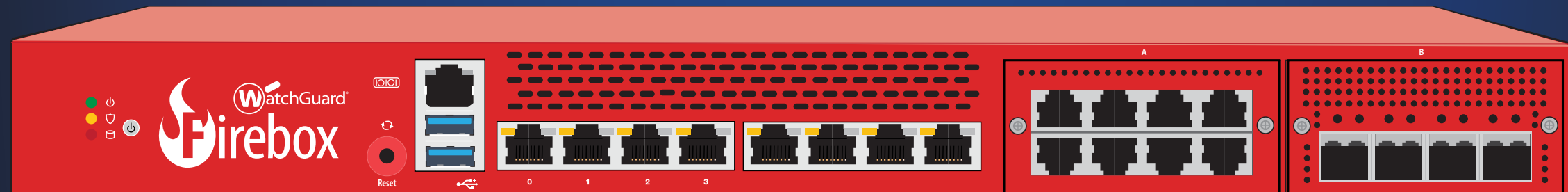
→ **70** attacks per device

14.8 million
malware variants blocked by WatchGuard in Q3 2020

→ **16% decrease** in malware

Read the full Internet Security Report at
www.watchguard.com/security-report

WatchGuard