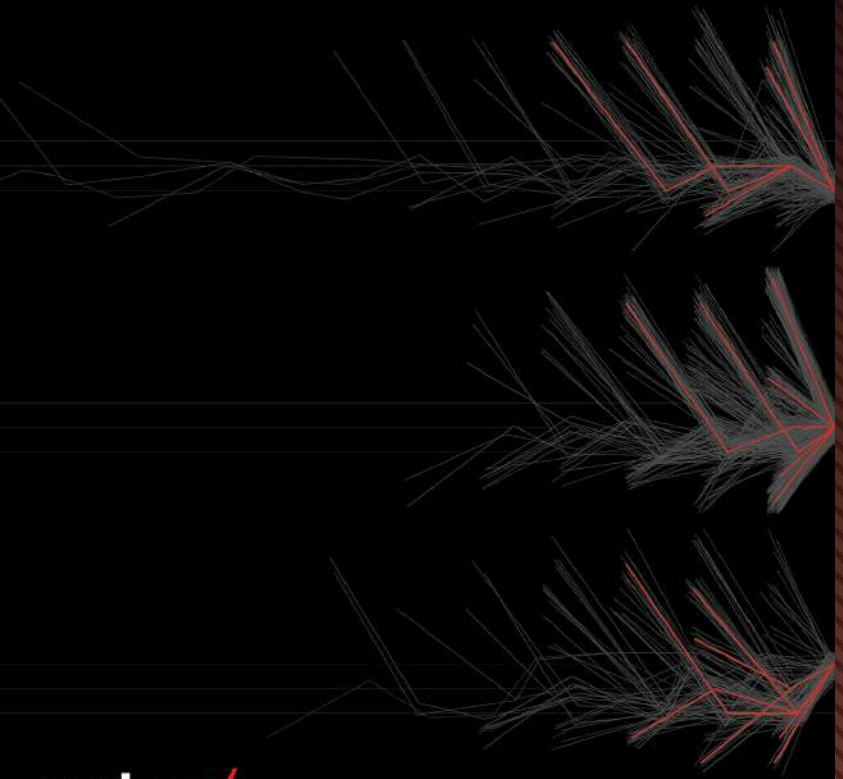
CROWDSTRIKE

SANDEEP RAO
SALES ENGINEER, INDIA & SAARC
PH: + 91 99670 94284

LEO THOMAS
ACCOUNT MANAGER, SOUTH
PH: + 91 97314 45784

BREACHES ARE EVERYWHERE

2019 Data Breach Investigations Report



verizon
business ready

Three key takeaways from the 2019 Verizon Data Breach Investigations Report

1. Understand the attack vendors used by adversaries
   - 60 per cent of breaches involved simple techniques such as phishing and stolen credential, not malware

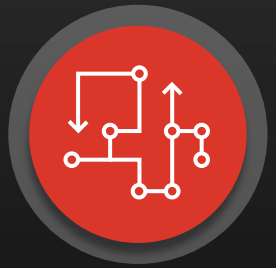
2. Detection of breaches remains very slow
   - 56% of breaches took months or longer to discover

3. Companies still suffer bad hygiene

CROWDSTRIKE

KEY CYBERSECURITY CHALLENGES

ATTACK SOPHISTICATION

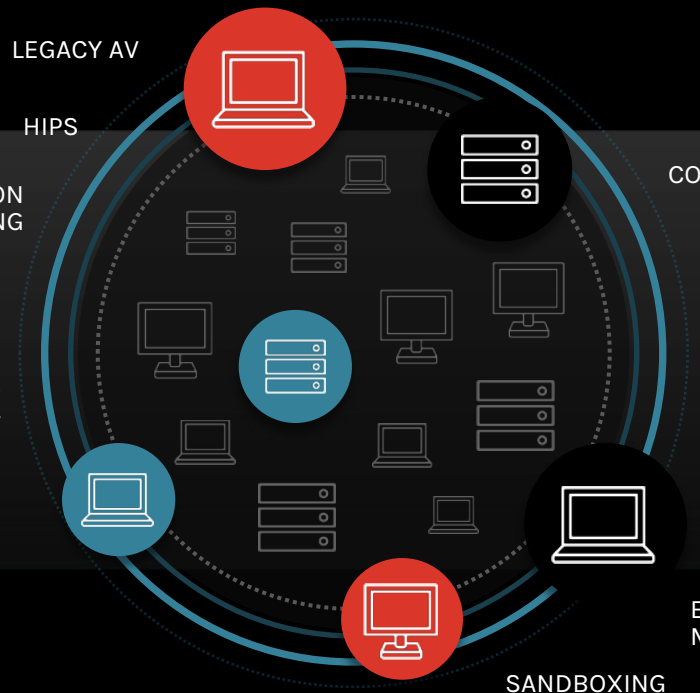


SOLUTION COMPLEXITY

SKILLS SHORTAGE

CROWDSTRIKE

MULTIPLE AGENTS FOR DIFFERENT NEEDS:



COSTLY TO DEPLOY

DIFFICULT TO MAINTAIN

POOR USER PRODUCTIVITY

REDUCED SECURITY EFFECTIVENESS

CROWDSTRIKE

CHALLENGES WITH BUILDING A TEAM

STAFF UP

Hire 3-6
skilled FTE

TOOL UP

Acquire necessary
tools for responders

TRAIN UP

Train responders and
keep their skills sharp

RETAIN

Promote and retain
your responders

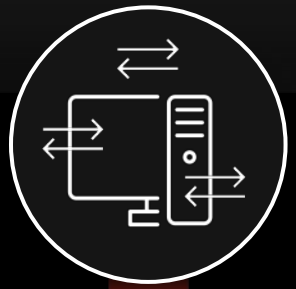
CROWDSTRIKE

WHAT SHOULD WE ADDRESS TO IMPROVE OUR SECURITY:

ON-PREM INFLEXIBLE TO EVOLVING NEEDS

CLOUD

AGENT BLOAT



REDUCE MULTIPLE AGENTS

SIGNATURES DON'T WORK – MISS NEW ATTACK TYPES

SIGNATURELESS SOLUTION

CROWDSTRIKE

KNOW YOUR ADVERSARY

AT THE HEART OF EVERY ATTACK IS A HUMAN ADVERSARY.

FALCON INTELLIGENCE REVEALS THEIR MOTIVATION AND TRADECRAFT TO KEEP YOU ONE STEP AHEAD.

MAZE RANSOMWARE

WHAT?

- RANSOMWARE FAMILY USING CHACHA & RSA-2048 TO ENCRYPT MOST FILES ON A VICTIM'S SYSTEM
- SENDS INFORMATION ABOUT VICTIM MACHINE, USERNAME, HOSTNAME, & DISK CAPACITY TO A SET OF IP ADDRESSES
- CAN BE EXECUTED W/OR W/OUT A COMMAND-LINE ARGUMENT
- ABILITY TO ESCALATE PRIVILEGES BY EXPLOITING VULNERABILITIES FROM CVE-2016-7255 AND CVE-2018-8453
- ALTHOUGH PRIMARILY BIG GAME HUNTING FOCUSED, HAS BEEN DISTRIBUTED BY EXPLOIT KITS & SPAM

Maze Ransomware

Dear [redacted] your files have been encrypted by RSA-2048 and ChaCha algorithms
The only way to restore them is to buy decryptor

These algorithms are one of the strongest
You can read about them at wikipedia

If you understand importance of situation you can restore all files by following instructions in DECRYPT-FILES.html file

You can decrypt 1 file for free as a proof of work
We know that this computer is a home computer
So we will give you appropriate price for recovering

CROWDSTRIKE

TWISTED SPIDER - ECRIME

ORIGIN:
EASTERN EUROPE, RUSSIAN FEDERATION

TARGET NATIONS:
AUSTRIA, CANADA, CHINA, COLOMBIA, CZECH REPUBLIC, FRANCE, GERMANY, ITALY, UNITED KINGDOM, UNITED STATES

TARGET INDUSTRIES:
CONSULTING & PROFESSIONAL SERVICES, GOVERNMENT, MANUFACTURING, STATE & MUNICIPAL GOVERNMENT, TECHNOLOGY

TOOLS:
MAZE

WHAT?

- RESPONSIBLE FOR MAZE RANSOMWARE – FIRST OBSERVED AROUND MAY 2019
- MAZE MAY BE USED AS RANSOMWARE-AS-A-SERVICE BUT MORE LIKELY OPERATED BY A SINGLE GROUP

SO WHAT?

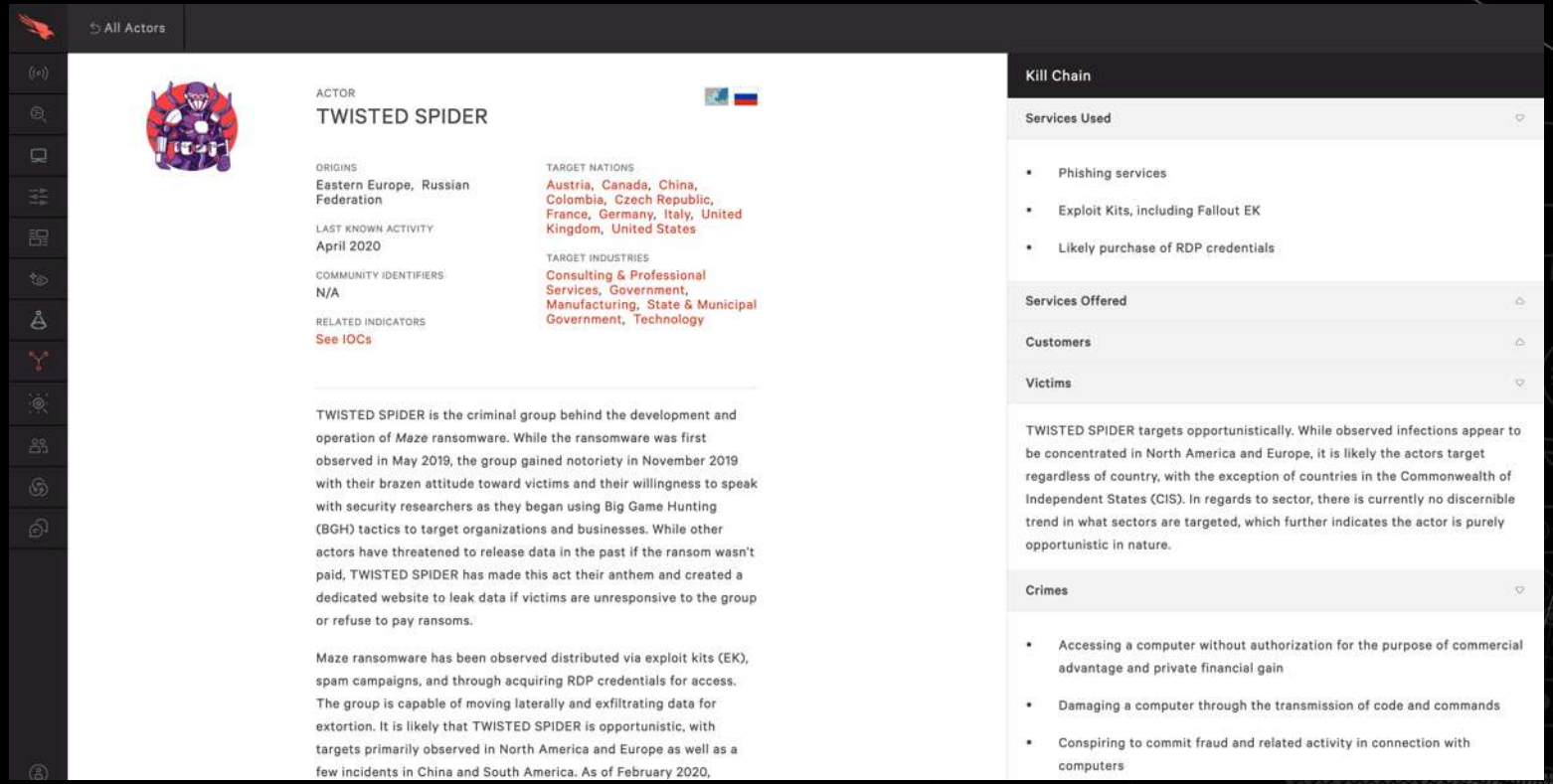
- TWISTED SPIDER ENGAGED IN BIG GAME HUNTING, GENERATING $7.5M IN THEIR HIGHEST 2019 PAYOUT
- ENGAGES IN EXTORTION FOR PAYMENT – FAILURE TO PAY OFTEN RESULTS IN DATA LEAKAGE

WHAT NEXT?

- THREAT INTELLIGENCE REPORTING
- CAMPAIGN TRACKING
- THREAT ACTOR PROFILING

CROWDSTRIKE

THREAT INTEL ON ACTOR PROFILE PAGE



CROWDSTRIKE

THE ADVERSARY ARE SWIFT AND FAST

SPEED IS EVERYTHING:

THE 1-10-60 RULE

CROWDSTRIKE

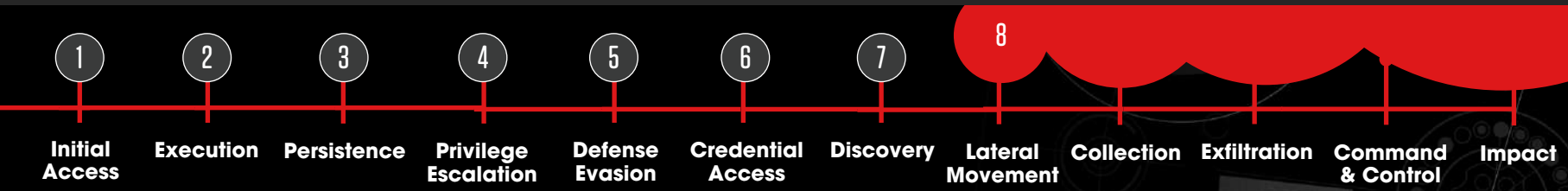
SURVIVAL OF THE FASTEST

TO STAY AHEAD YOU MUST:

DETECT IN 1min

INVESTIGATE IN 10min

RESPOND IN 60min



MITRE ATT&CK PHASE

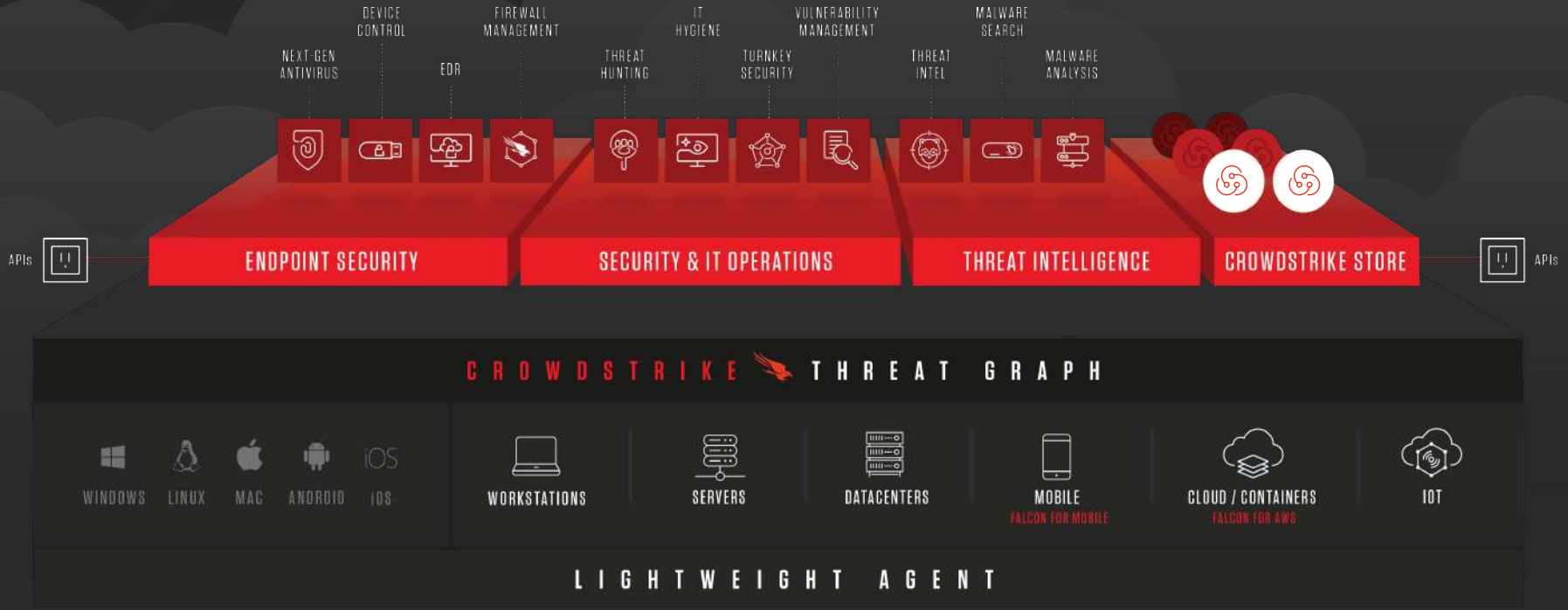
GARTNER , FEBRUARY 2019
PREPARE FOR ENDPOINT PROTECTION SHIFTING TO THE CLOUD

Recommendations

1. Evaluate cloud-delivered solutions well before your next renewal.
2. Choose vendors that offer a true elastic and agile cloud architecture supported by a range of service options such as incident response help and managed detection and response.
3. Seek fully integrated EPP solutions with EDR capabilities that use the same detection funnel, data repository, management console and agent.
4. Ensure that EPP detection capabilities include more modern behavioural approaches that are immediately adaptive to detect or block new attack techniques.

CROWDSTRIKE

FALCON PLATFORM PROTECTS ALL WORKLOADS



CROWDSTRIKE

CROWDSTRIKE STORE APPLICATIONS
A UNIQUE CYBER SECURITY ECOSYSTEM

ADVANCED THREAT HUNTING / DECEPTION
ACALVIO

APPLICATION WHITELISTING
AIRLOCK DIGITAL

ICS / IOT THREAT DETECTION
DRAGOS

VULNERABILITY RISK MANAGEMENT
NOPSEC

APPLICATION ANALYTICS
TRUEFORT

PATCH MANAGEMENT
AUTOMOX

ATTACK SURFACE MANAGEMENT
RISKIQ

UEBA / INSIDER THREAT
exabeam
MICRO FOCUS
INTERSET

CROWDSTRIKE

3 SMALL STEPS TO REPLACE YOUR AV

No infrastructure setup

No fine-tuning, rule writing

Install the Falcon Agent

Verify the installation

No reboot

No signatures updates

No scan

Remove legacy products

Financial Institution

77,000 AGENTS
1 DAY

Hospitality Chain

40,000 AGENT
5 DAYS

Technology Company

55,000 AGENTS
5 DAYS

Financial Institution

300,000 AGENTS
90 DAYS

WHAT WERE THE ANALYST SAYING IN 2018 AND NOW

2017

2018

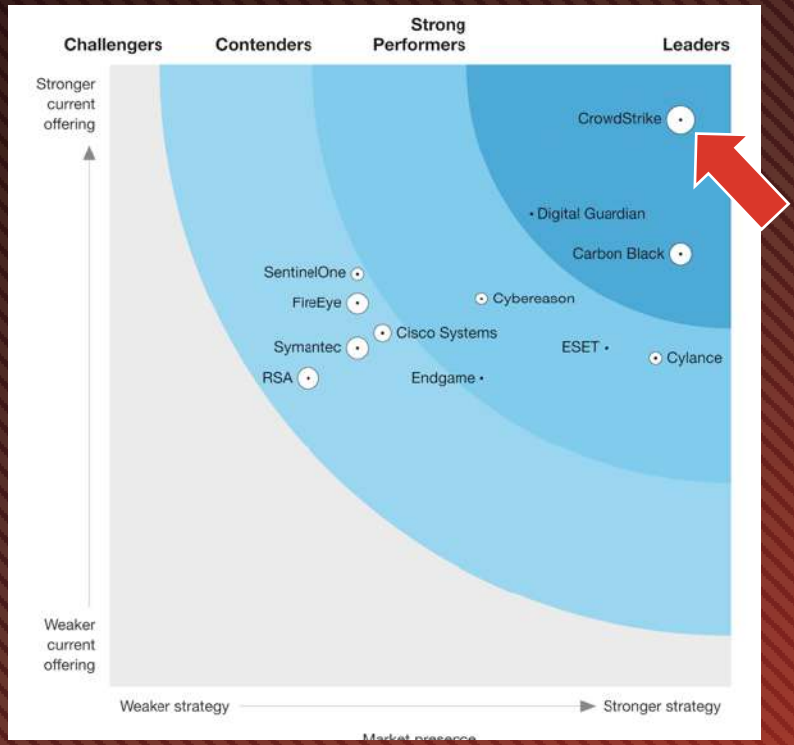
2019

FROM VISIONARY TO LEADER & COMPLETENESS OF VISION IN 3 YEARS

CROWDSTRIKE

FORRESTER WAVES

Forrester Wave for Endpoint Security Suites, Q2 2018



Forrester Wave for Endpoint Detection and Response, Q3 2018

CROWDSTRIKE

THE NEW STANDARD IN ENDPOINT PROTECTION

INDUSTRY ANALYSTS

Gartner

"CROWDSTRIKE NAMED A LEADER IN THE 2019 GARTNER MAGIC QUADRANT FOR ENDPOINT PROTECTION AND POSITIONED FURTHEST FOR COMPLETENESS OF VISION"

FORRESTER®

"CROWDSTRIKE IS THE ONLY VENDOR TO BE NAMED A LEADER IN BOTH ENDPOINT SECURITY SUITE AND EDR WAVES"

IDC

"LEADER IN IDC MARKETSCAPE FOR US INCIDENT READINESS, RESPONSE AND RESILIENCY SERVICES"

PRODUCT REVIEWS AND TESTS

AV comparatives — "FALCON CERTIFIED TO REPLACE LEGACY ANTIVIRUS"

SE Labs — "FALCON ACHIEVES AAA RATING IN SE LABS TEST"

MITRE — "MITRE VALIDATES FALCON AGAINST ATT&CK™ FRAMEWORK"

SC — "FIVE STAR RATING AND BEST BUY AWARD"

Gartner peerinsights.

★★★★★

CUSTOMER INSIGHTS

HIGHEST SCORE OF 4.9/5 IN BOTH EDR AND ENDPOINT PROTECTION PLATFORMS

AWARDS AND RECOGNITION

SC Awards Winner — NAMED BEST SECURITY COMPANY FOR TWO CONSECUTIVE YEARS

CNBC DISRUPTOR 50 2017 — CROWDSTRIKE NAMED CNBC DISRUPTOR FOR TWO CONSECUTIVE YEARS

Forbes — FORBES CLOUD 100 LIST FOR TWO CONSECUTIVE YEARS

CROWDSTRIKE

FORRESTER TOTAL ECONOMIC IMPACT (TEI) STUDY

OF CROWDSTRIKE FALCON®

In **October 2019** Forrester Research was commissioned to conduct an ROI study of the CrowdStrike Falcon Platform

ROI
316%

PAYBACK
< 3 MONTHS

The Top 25 Cybersecurity Companies of 2019

December 10, 2019

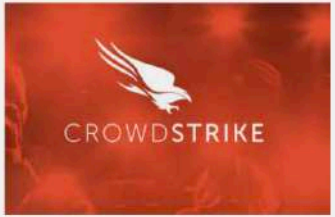
The Software Report is pleased to announce The Top 25 Cybersecurity Companies of 2019. For the past two months, we collected hundreds of nominations from professionals in the cybersecurity field. They provided their candid feedback on the strength of each company's technology, caliber of the company's organization, management team effectiveness and ability to stay ahead of the latest cybersecurity threats, among other attributes.

After thorough review of each company's nomination survey results, we selected those who scored the highest. We paid particular attention to those who demonstrated consistency across each performance area. The following company awardees represent this year's best of the best in cybersecurity.

1. Crowdstrike
Category: Endpoint Security
Location: Sunnyvale, California

Founded in 2011, CrowdStrike was borne out of the realization that existing security solutions on the market weren't enough to combat the sophisticated hackers that were infiltrating some of the nation's

https://www.thesoftwarereport.com/the-top-25-cybersecurity-companies-of-2019/#.XfKfWIRoHrE.linkedin



1. Crowdstrike
Category: Endpoint Security
Location: Sunnyvale, California

Founded in 2011, CrowdStrike was borne out of the realization that existing security solutions on the market weren't enough to combat the sophisticated hackers that were infiltrating some of the nation's largest and well-known corporations. Co-founders George Kurtz and Dmitri Alperovitch made a bet that marrying advanced endpoint protection with intelligence would be a better way to identify the perpetrators behind the attacks. And that bet has paid off. Today CrowdStrike is a premier cyber security company with presence in the U.S., Europe, and India. It employs about 2,000 and counts ADP, Rackspace, and Hyatt among its clients. The company provides security services to 12 of the 20 Fortune largest global companies, ten of the 20 largest financial institutions and five of the top ten largest healthcare provides. It's also a leading cybersecurity provider for the energy market.

CrowdStrike CEO Kurtz, a serial entrepreneur, is an internationally recognized cybersecurity expert, holding executive roles at McAfee before creating CrowdStrike with Alperovitch. His company was also who the Democratic National Committee turned to when it suspected it was hacked during the run-up to the 2016 election. CrowdStrike's IPO occurred in June of 2019.

CROWDSTRIKE

CUSTOMER TRUSTED

44 OF 100
FORTUNE 100 COMPANIES

37 OF 100
TOP GLOBAL COMPANIES

9 OF 20
MAJOR BANKS

5 OF THE TOP 10
LARGEST HEALTHCARE PROVIDERS

7 OF THE TOP 10
LARGEST ENERGY INSTITUTIONS

BERIN LAUTENBACH
CISO APAC,
Telstra

JOHN VISNESKI
Director, Information Security & Data Prot., Pokémon Company International

ROBERT THOMAS
Chief Operating Officer,
Mercedes-AMG Petronas Motorsport

ROLAND CLOUTIER
Sr. VP,
Chief Security Officer,
ADP

NIK PATEL
Head of Technology Security Services,
Credit Suisse

SCOTT STOOPS
Security Analyst,
Ashland University


START YOUR FREE TRIAL
crowdstrike.com/freetrial