



INVESTOR BRIEFING

OCTOBER 2021

GEORGE KURTZ, CO-FOUNDER AND CEO
MIKE SENTONAS, CHIEF TECHNOLOGY OFFICER



AGENDA

A large, stylized red eagle logo is positioned on the left side of the slide, facing right. The eagle is depicted with its wings spread, and its tail feathers are visible. The logo is rendered in a solid red color against the dark background.

Product Briefing from
George Kurtz and Mike Sentonas

Partner Interviews

- Accenture
 - AWS
-

Customer Interview

- Zoom
-

Q&A

SAFE HARBOR

This presentation includes express and implied “forward-looking statements”, including forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. Forward-looking statements include all statements that are not historical facts, and in some cases, can be identified by terms such as “anticipate,” “believe,” “estimate,” “expect,” “intend,” “may,” “might,” “plan,” “project,” “will,” “would,” “should,” “could,” “can,” “predict,” “potential,” “continue,” or the negative of these terms, and similar expressions that concern our expectations, strategy, plans or intentions. Forward-looking statements contained in this presentation include, but are not limited to, statements concerning our product roadmap and future initiatives, the performance and benefits of our products, strategic plans or objectives, our estimates of market size and opportunity, and our growth prospects. By their nature, these statements are subject to numerous risks and uncertainties, including factors beyond our control, that could cause actual results, performance or achievement to differ materially and adversely from those anticipated or implied in the statements. Such risks and uncertainties are described in the “Risk Factors” section of our most recent Form 10-Q filed with the Securities and Exchange Commission. Although our management believes that the expectations reflected in our statements are reasonable, we cannot guarantee that the future results, levels of activity, performance or events and circumstances described in the forward-looking statements will be achieved or occur. Recipients are cautioned not to place undue reliance on these forward-looking statements, which speak only as of the date such statements are made and should not be construed as statements of fact. Except to the extent required by federal securities laws, we undertake no obligation to update these forward-looking statements to reflect events or circumstances after the date hereof, or to reflect the occurrence of unanticipated events.

Information in this presentation on new products, features, and functionality, including our expectations with respect to the development, release and timing thereof, is for informational purposes only and should not be relied upon.

Certain information contained in this presentation and statements made orally during this presentation relate to or are based on studies, publications, surveys and other data obtained from third-party sources and CrowdStrike’s own internal estimates and research. While CrowdStrike believes these third-party studies, publications, surveys and other data to be reliable as of the date of this presentation, it has not independently verified, and makes no representations as to the adequacy, fairness, accuracy or completeness of, any information obtained from third-party sources. In addition, no independent source has evaluated the reasonableness or accuracy of CrowdStrike’s internal estimates or research and no reliance should be made on any information or statements made in this presentation relating to or based on such internal estimates and research.

OUR VIEW FROM A **LEAD POSITION**



A GLOBAL LEADER IN ENDPOINT & WORKLOAD SECURITY



A LEADER



**A Leader in Magic
Quadrant™ for Endpoint
Protection Platforms**



A LEADER



**CrowdStrike offers superior
endpoint security with a
cloud-native architecture**



RANKED #1



**Ranked #1 for Modern
Endpoint Security 2020
Market Shares**

Gartner: Magic Quadrant for Endpoint Protection Platforms, G00450741, May 2021

Forrester: The Forrester Wave™: Endpoint Security Software As A Service, Q2 2021, May 2021

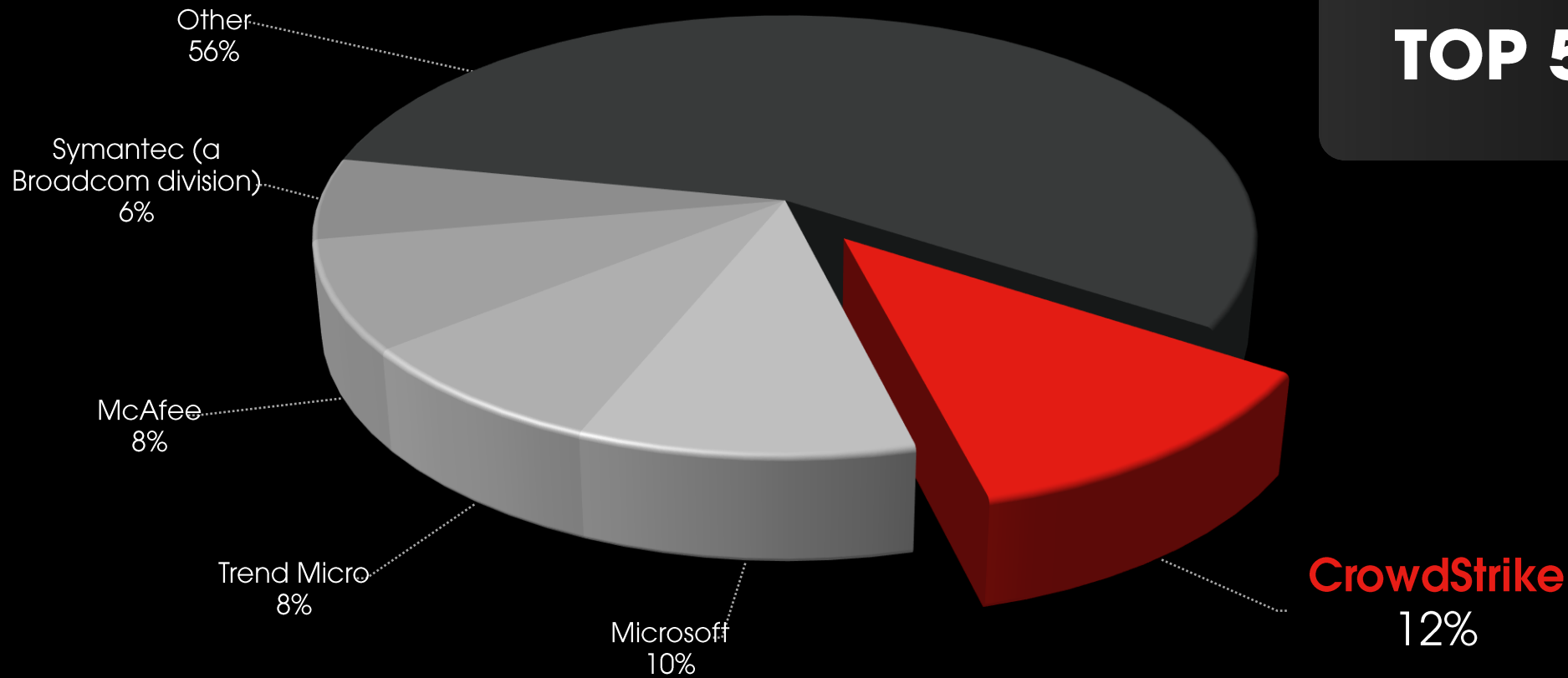
IDC: Corporate Endpoint Security Market Shares, 2020: Pandemic and Expanding Functionality Propelled Market Growth, Doc #US47768021, Jun 2021

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The Gartner content described herein (the "Gartner Content") represent(s) research opinion or viewpoints published, as part of a syndicated subscription service, by Gartner, Inc. ("Gartner"), and are not representations of fact. Gartner Content speaks as of its original publication date (and not as of the date of this [type of filing]), and the opinions expressed in the Gartner Content are subject to change without notice. GARTNER and MAGIC QUADRANT are registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

#1 FOR MODERN ENDPOINT SECURITY

2020 WW MARKET SHARES

TOP 5 VENDORS



WHAT DOES CLOUD NATIVE MEAN?

**ON-PREM
TECH**

**CLOUD
RETROFIT**

**CLOUD
NATIVE**
THE CROWDSTRIKE
APPROACH

LEGACY



ENDPOINTS AND WORKLOADS

PROCESSES

MODULES

IDENTITIES

ASSETS

CONFIGURATIONS

NETWORK

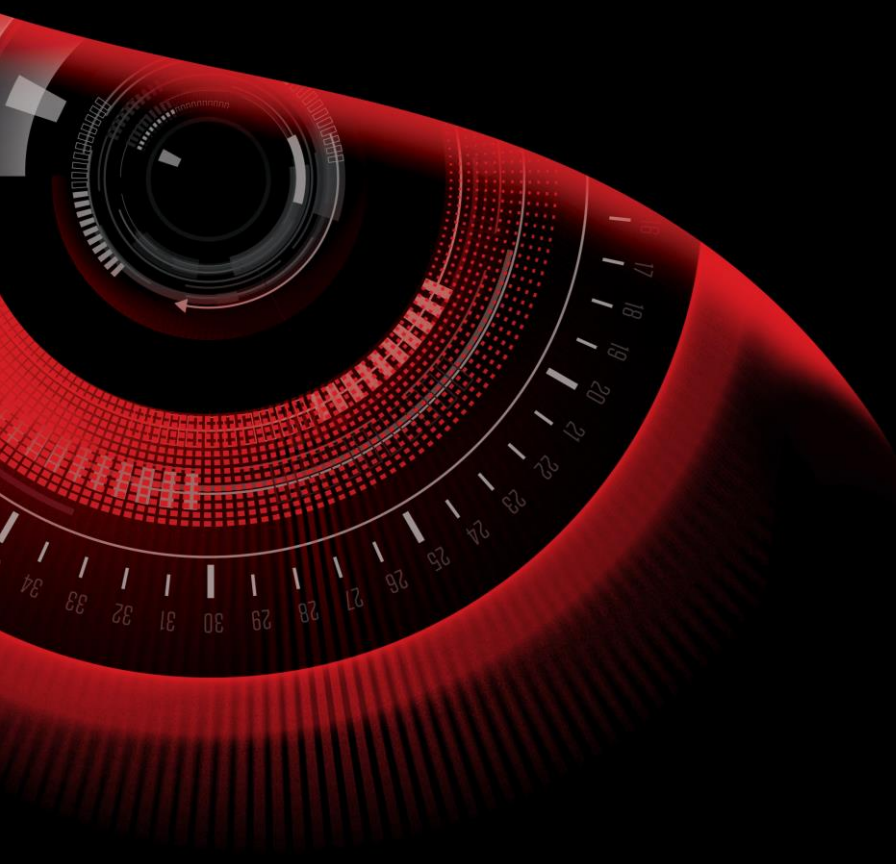
E-MAIL

SECURITY CLOUD

SAAS,
CASB

CLOUD
IAAS, PAAS

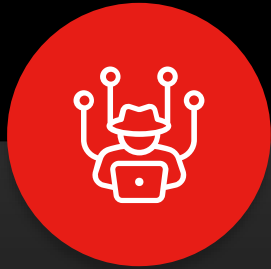




TOGETHER, WE WILL

**stop
breaches**

TODAY'S THREAT ENVIRONMENT



68%

OF DETECTIONS
WERE NOT MALWARE-
BASED



60%

INCREASE IN
INTERACTIVE INTRUSION
CAMPAIGNS



1 h32m

AVERAGE TIME
FOR AN ADVERSARY
TO MOVE Laterally IN A
VICTIM ENVIRONMENT

LEADING THREAT HUNTING



1 trillion

**HIGH-FIDELITY
SIGNALS PER DAY**



65,000

**POTENTIAL INTRUSIONS
STOPPED**



8 min.

**AVERAGE
INTERVAL**

BEST IN CLASS MALWARE PREVENTION



To get credit, the threat must be remediated so no malicious code is present.

- 1** All code must be removed from initial threat and any executable dropped files
- 2** Malicious process must be killed
- 3** Other persistent OS damage must be repaired
- 4** Remediation must complete in minutes

AVC keeps their own evidence, they don't trust vendor claims to score the result.



The attack must be crippled; points are lost for incomplete remediation even if neutralized.

- 1** Four points for complete prevention and/or remediation
- 2** Three points for neutralization (threat cannot run but may still have parts present)
- 3** Zero points for persistent remediation (malware in a retry loop which gets prevented, typically)
- 4** Minus four points for detection without remediation



**CONTINUOUS
INNOVATION**

The background features a series of overlapping, semi-transparent red geometric shapes, primarily parallelograms and rectangles, arranged in a perspective that suggests depth and movement. Interspersed among these shapes are several sets of small, white, right-angled chevrons pointing towards the right, creating a sense of flow and direction. The overall color palette is a gradient of dark reds and blacks, with the text providing a stark white contrast.

BUILDING ON

THE PLATFORM

The background features a dark red color scheme with a hexagonal grid pattern. Scattered throughout are binary digits (0s and 1s) and small padlock icons, some of which are highlighted with a glowing red effect. The overall aesthetic is technical and secure.

Introducing FileVantage

A woman with her hair in a bun is sitting at a desk, looking at a laptop with a frustrated expression. Her hands are clasped together on the desk. The scene is dimly lit with a red tint. Overlaid on the image is a quote in white text with red quotation marks.

“ I love my FIM ”
...said no one ever

INTRODUCING FILEVANTAGE

**NO
SURPRISES**

BETTER VISIBILITY INTO
YOUR ENTERPRISE



Low Overhead



No additional agents



Granular change tracking of customized files and configuration lists



Enterprise maturity with roles and access control



All integrated into the Falcon platform

Spotlight



A hand is shown holding a power drill, positioned over a wooden surface. The image is overlaid with a semi-transparent red filter. The text is centered on the left side of the image.

**If everything is a priority
nothing is a priority**

ProxyShell attacks ramping up on unpatched Exchange Servers

Security experts say active attacks on the series of Microsoft Exchange Server flaws, which can be chained to take control of servers, are already being launched in the wild.

[Shaun Nichols](#)

Published: 07 Sep 2021

ProxyShell Exchange Server Flaw Getting Used for Ransomware Attacks

By Kurt Mackie | 08/24/2021

'ProxyShell' Exchange bugs resurface after presentation

A critical vulnerability in Microsoft Exchange is once again making the rounds with attackers, following a Black Hat presentation from the researcher who found it.

[Shaun Nichols](#)

Published: 09 Aug 2021

FROM PWN2OWN 2021: A NEW ATTACK SURFACE ON MICROSOFT EXCHANGE - PROXYSHELL!

August 18, 2021 | Guest Blogger

The Windows print nightmare continues for the enterprise

KB5005652, meant to address "PrintNightmare" vulnerabilities, is causing some enterprise users to be prompted to reinstall print drivers or install new drivers — which they can't do without admin privileges.

Microsoft fiddles with Fluent while the long dark Nightmare of the Print Spooler continues for Windows

New Windows 11 toys, fresh new CVE pops out

[Richard Speed](#)

Fri 13 Aug 2021 // 14:31 UTC

25 

SPOTLIGHT ANNOUNCEMENTS



Announcing ExPRT.AI

Recommended remediation

Orchestration through Falcon Fusion

CLOUD SECURITY

aws





CLOUD SECURITY

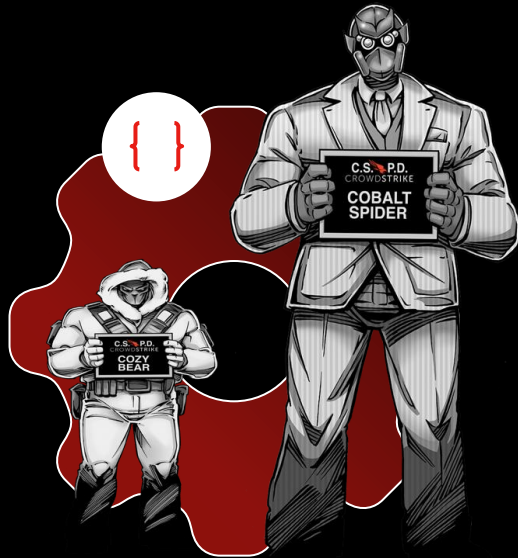
is a tangled web



**We need to stop
breaches in the cloud**

COMPLETE VISIBILITY & THREAT HUNTING ELIMINATES BLIND SPOTS

BUILD INFRASTRUCTURE



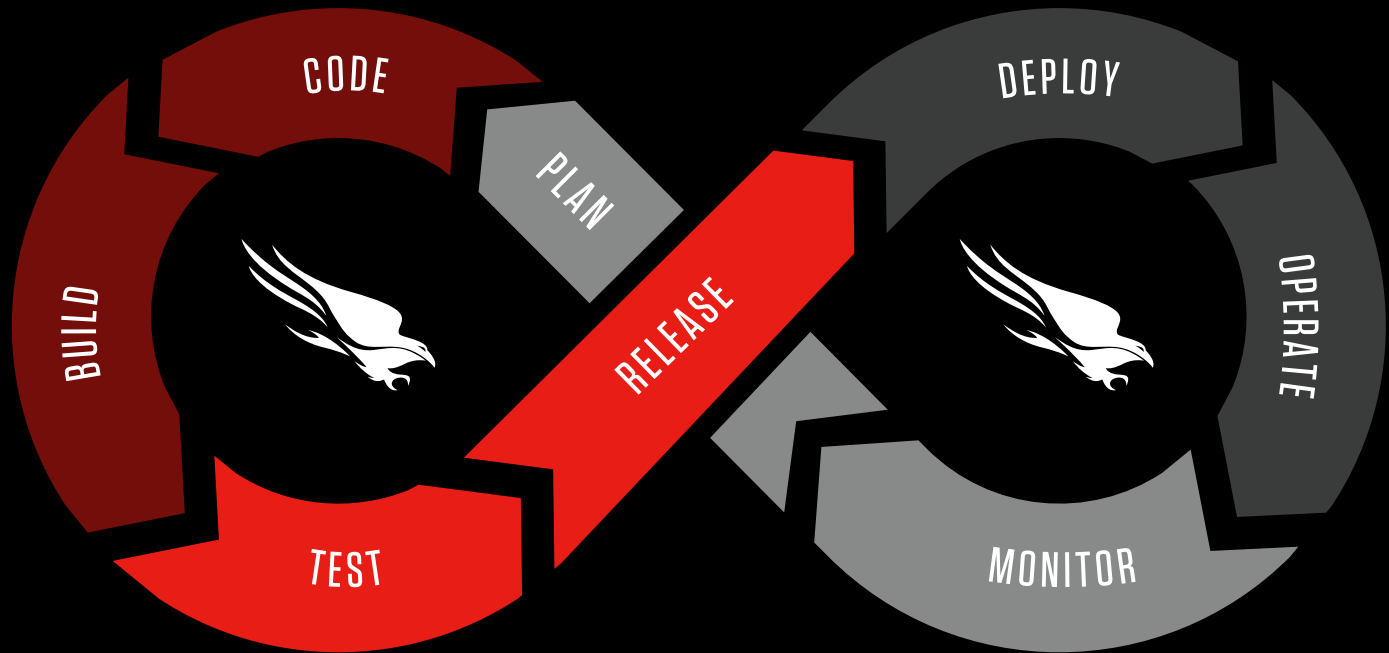
DEVOPS



CLOUD INFRASTRUCTURE



DevSECOps approach to stopping breaches in the cloud



Comprehensive
visibility into
hybrid cloud

Remedy
misconfigurations
(IOMs)

Industry
first Cloud
IOAs

Correlate runtime
and control plane
visibility

Image Assessment
and Kubernetes
protection

CWP COMPLETE





THE NEXT PHASE

OF THE JOURNEY

**Complexity in the
enterprise keeps
on increasing**



MAIN CUSTOMER CONVERSATIONS



THREAT LANDSCAPE

Dealing with a massive increase in sophisticated attacks



CLOUD & REMOTE FIRST

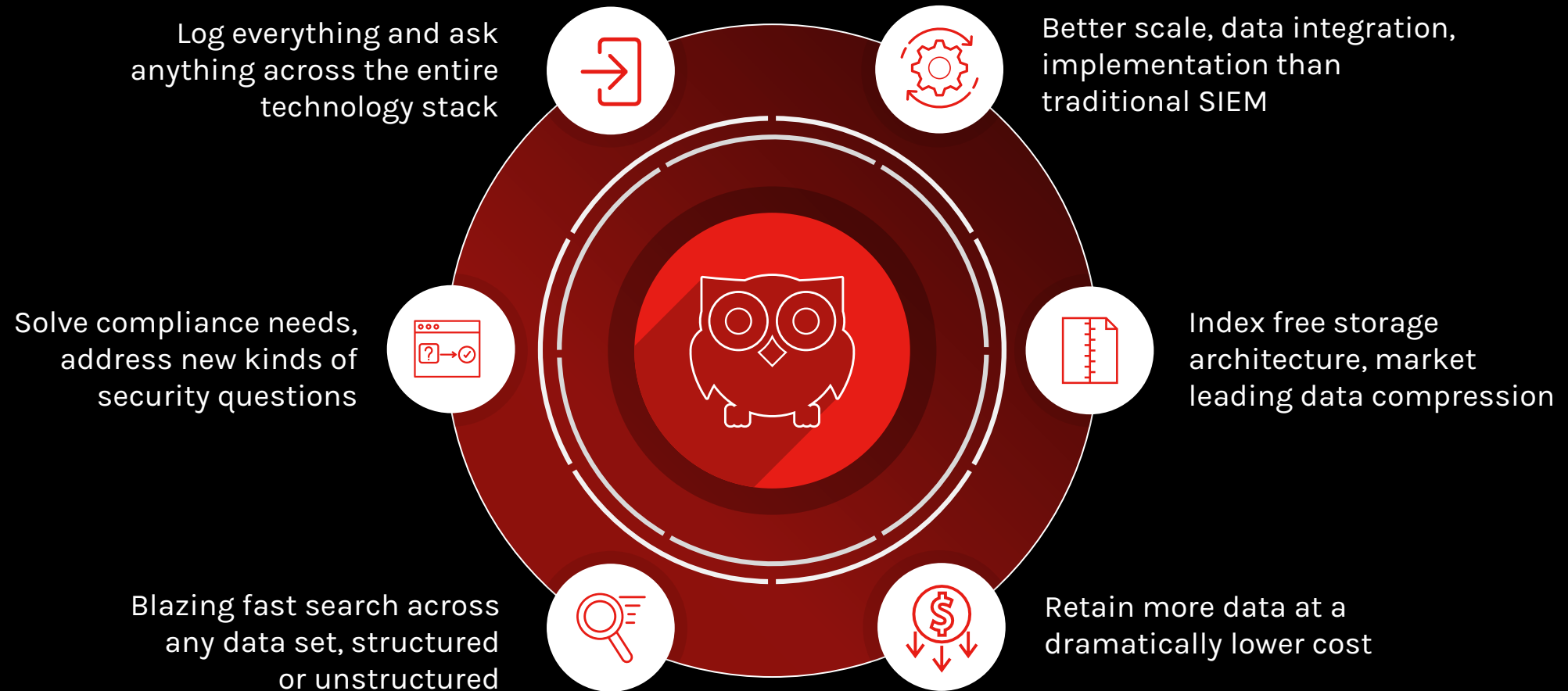
The enterprise network has become a whole lot bigger and more complex



MORE VULNERABILITIES

New critical vulnerabilities impacting core technology stacks nearly every week

HUMIO BRINGS INDUSTRY-LEADING LOG MANAGEMENT TO FALCON



HUMIO CASE STUDIES

FINANCIAL SERVICES COMPANY

MULTINATIONAL INFORMATION TECHNOLOGY COMPANY

MULTINATIONAL CONSUMER GOODS COMPANY

PRE-HUMIO PAIN POINTS

Struggling to take in 20TB/day with ELK and Greylog
Very long query times (40+ minutes)

Struggling with 10TB/day with Elastic
Queries causing system impacts

Struggling with EUBA topping out at 1TB/day, based on ELK

HUMIO ADVANTAGES

6.5X increase in TB/day ingested

7X increase in TB/day ingested

8X Increase in TB/day ingested

Saves time in troubleshooting support issues and shortens time to code release.

Reduced friction and increased efficacy in issue tracing
Faster code releases, and happier developers

Able to capture all security logs
Displaced product that couldn't deliver



HUMIO WILL OPEN THE DOOR
TO DO SO MUCH MORE



XDR

BEYOND THE HYPE

ENRICHES

EDR data with telemetry from targeted, vendor-specific security data

X

PROVIDES

real-time threat detection, alerting, prevention and hunting across multiple technologies and domains

D

PROACTIVE


proactive automated responses across multiple technologies and domains

R



ANNOUNCING

Falcon XDR

A large, bold, black 'X' logo is positioned on the left side of the slide. The background is a dark red color with a subtle geometric pattern of overlapping triangles and lines. The text is centered in a white, sans-serif font within a dark red rectangular area.

Humio-powered and
Threat Graph integrated



Increased visibility into
indicators of attack

Real-time detection

Extending telemetry
sources for broader
security correlations

Importance of data science
accuracy of ML in improving
detection speed



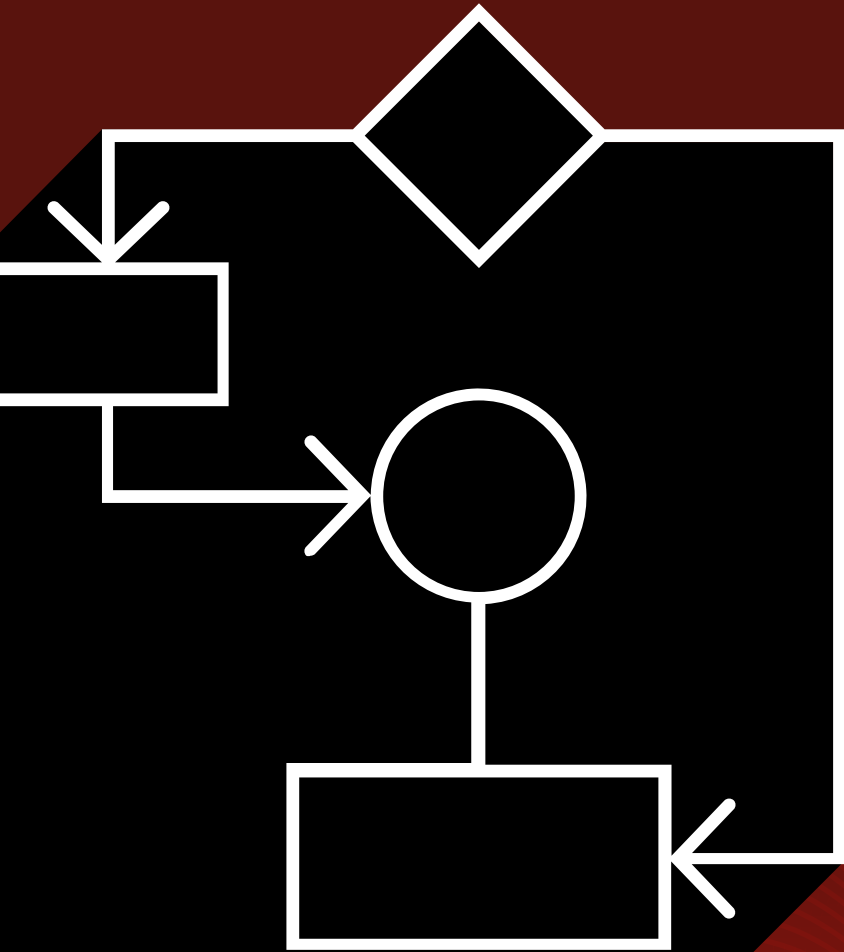
Faster Response



Internal Process



Automation



ANNOUNCING FALCON FUSION

Edit a workflow

Action

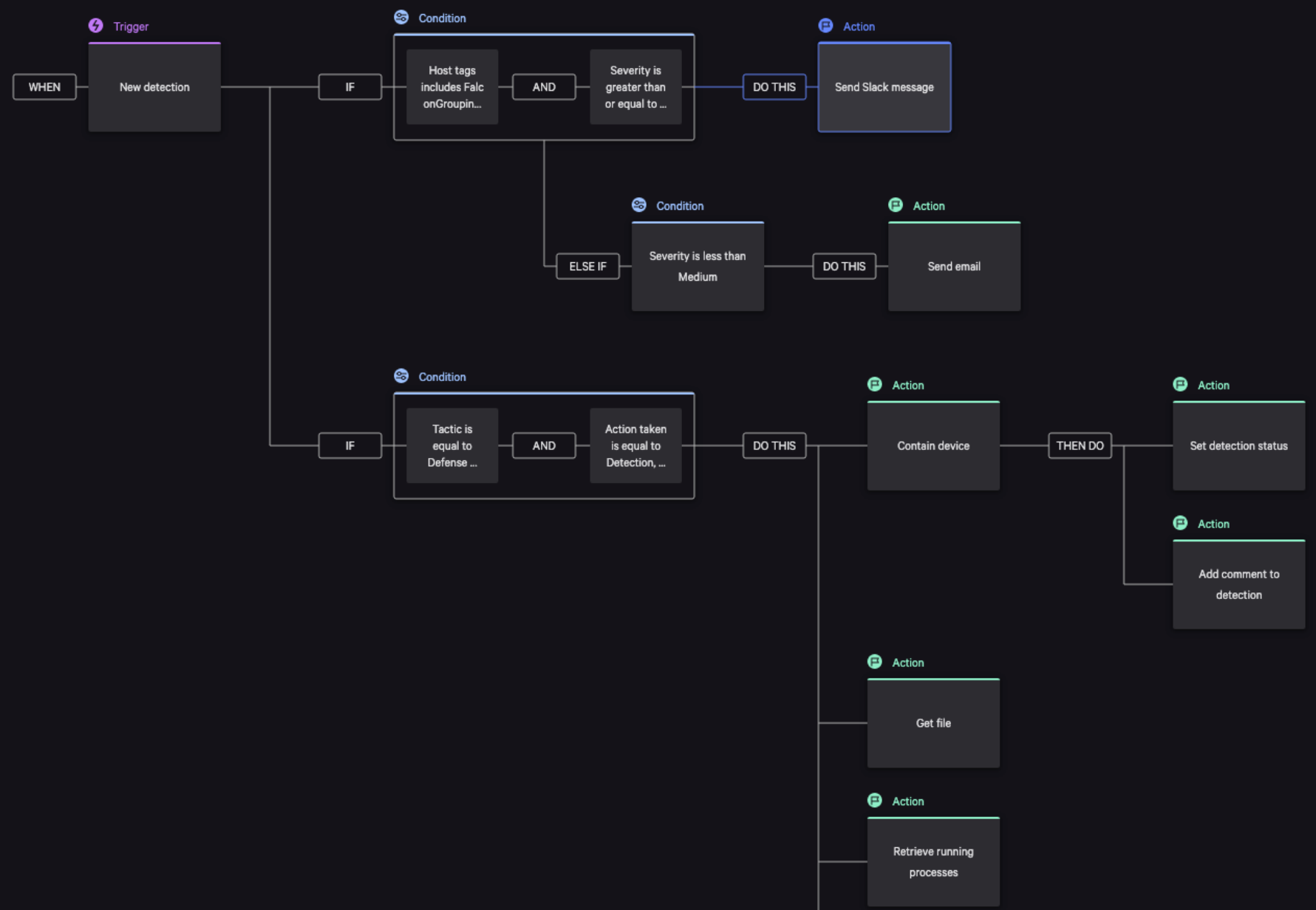
Customize action

Action type: Notifications

Action: Send Slack message

Channel: Workflow Notification Channel

Data to include: Action taken, Cloud service provider, Cloud service instance ID

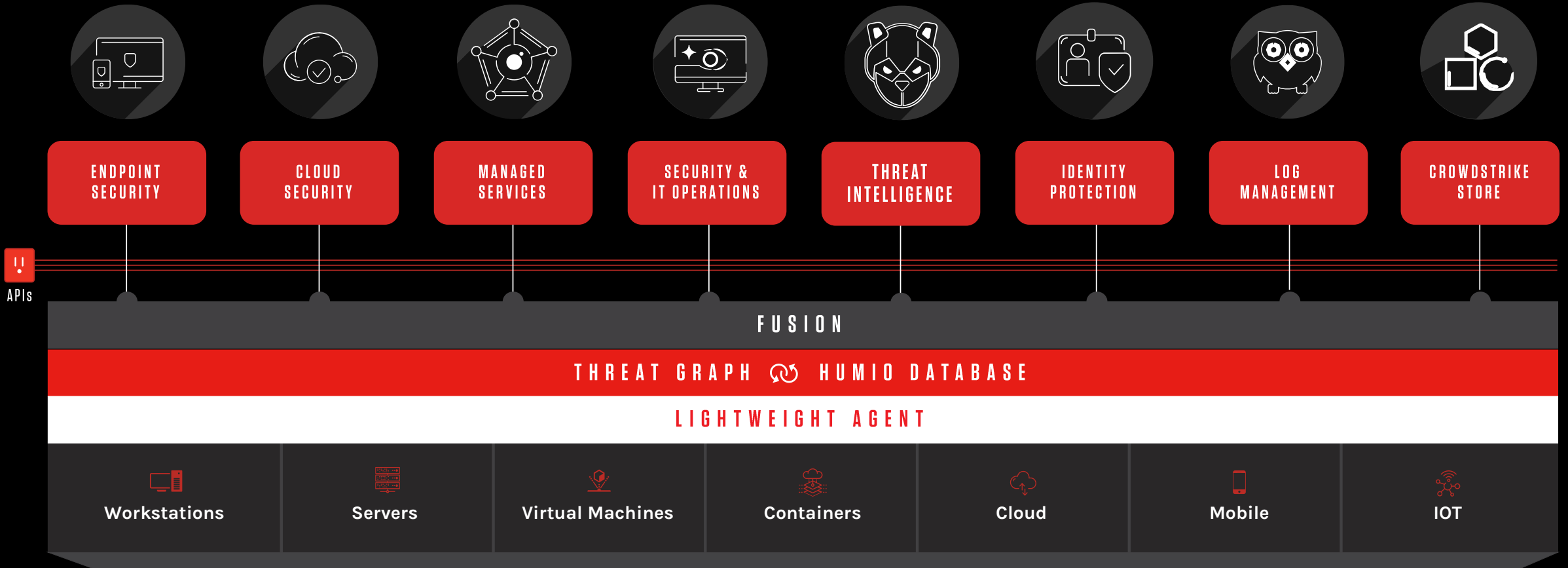


XXDR

FALCON

The background features a dark red gradient with several overlapping, semi-transparent black shapes that resemble stylized flames or abstract patterns. The overall aesthetic is bold and dramatic.

THE FALCON PLATFORM



ANNOUNCING THE CrowdXDR ALLIANCE

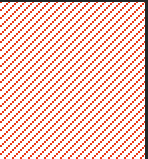
The Power of We



PARTNERS

The background is a dark red gradient with several thin, glowing red lines that intersect and form a network-like pattern. Small, bright red dots are scattered along these lines, creating a sense of depth and movement. The overall aesthetic is modern and technological.

Customers



Q&A

