Data World

YOUR VALUE-ADDED DISTRIBUTOR

Data World Computer & Communication Limited

It Just Takes Two: A Two-Stage Approach in Cost-Effectively Enhancing Your Organizational Cyber Hygiene

兩步到位: 高效提升機構資訊保安的方法

Roger Lee
CISA, CCNP
Assistant Manager, Pre-Sales Division
24 Jan 2022 (Mon)

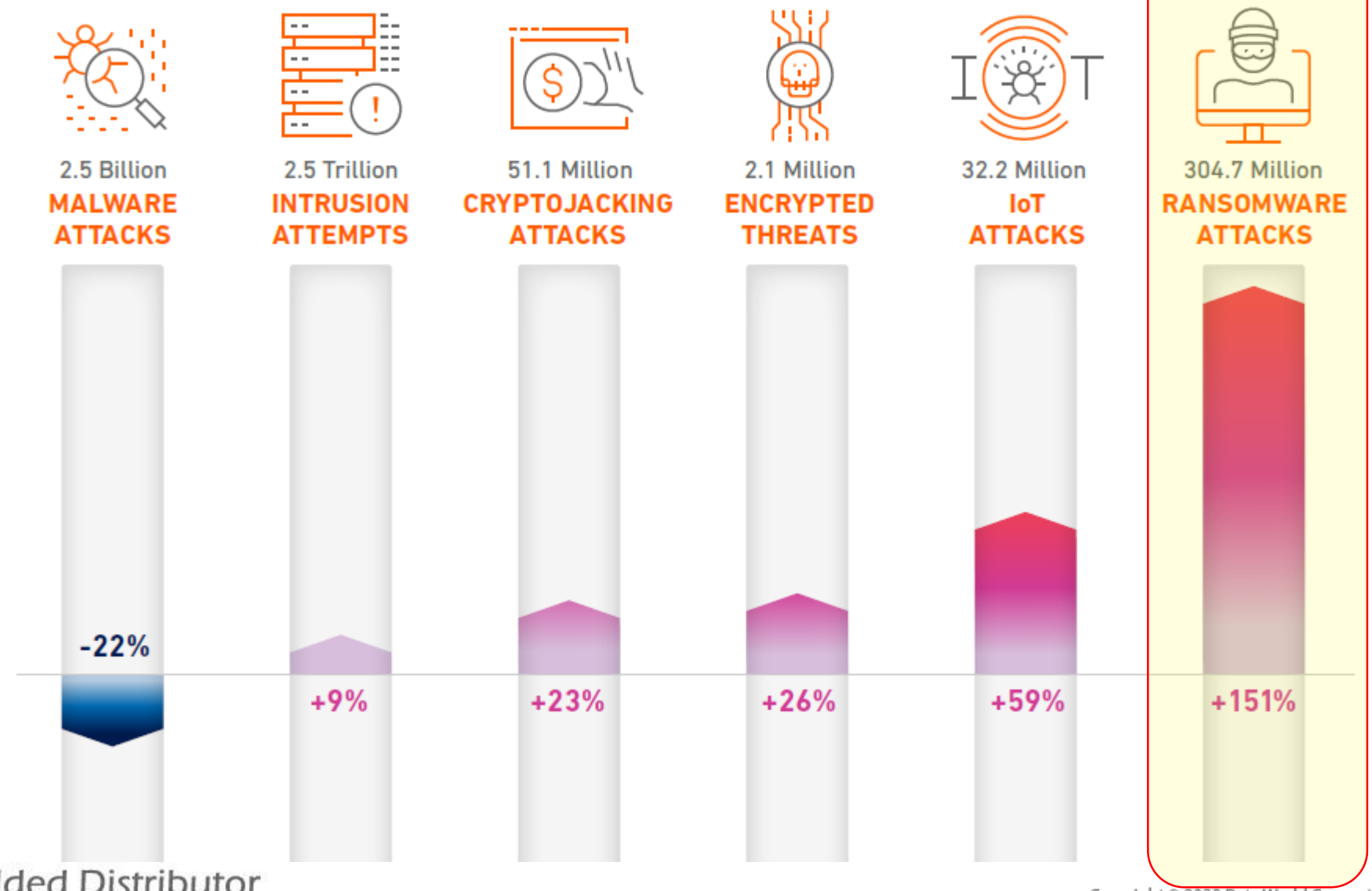
Agenda

- What's happening now?
- How a Typical Attack works? What can we do?
- Step 1 (On-the-Fly): Cloud-based Email Hygiene for Microsoft 365
- Step 2 (Landing): More than a NGAV: Endpoint Detection & Response (EDR)

Data World
Your Value - added Distributor

What’s happening now ?

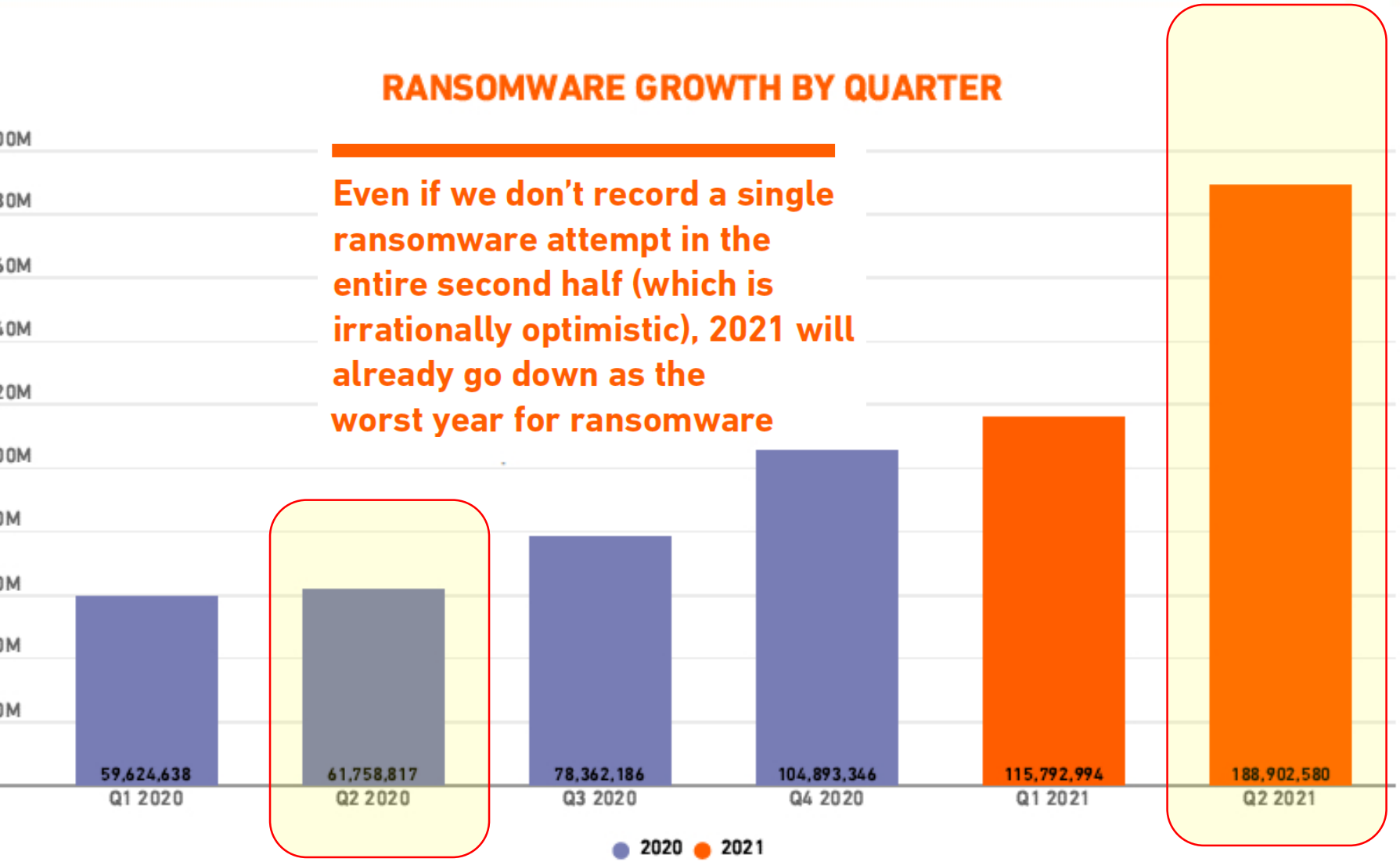
Year 2021 First Half – Global Cyberattack Trends



Already eclipsing the 304.6 million ransomware attempts logged for the entirety of 2020

Data World
Your Value - added Distributor

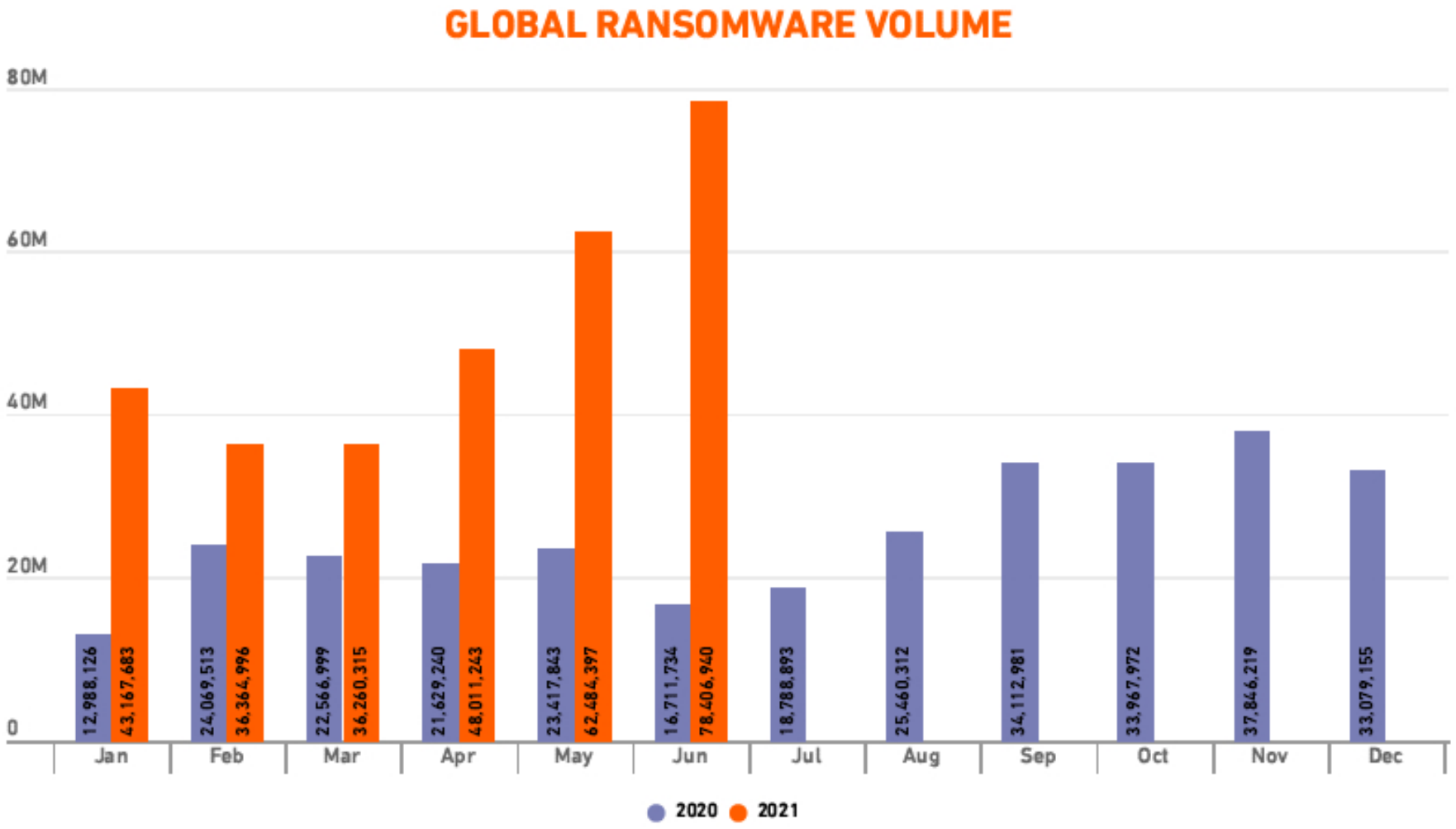
Ransomware Continues its Record-Shattering Run



Q2 2021 was the worst quarter for ransomware since SonicWall began keeping records — and it isn't even close.

Data World
Your Value - added Distributor

Ransomware Continues its Record-Shattering Run



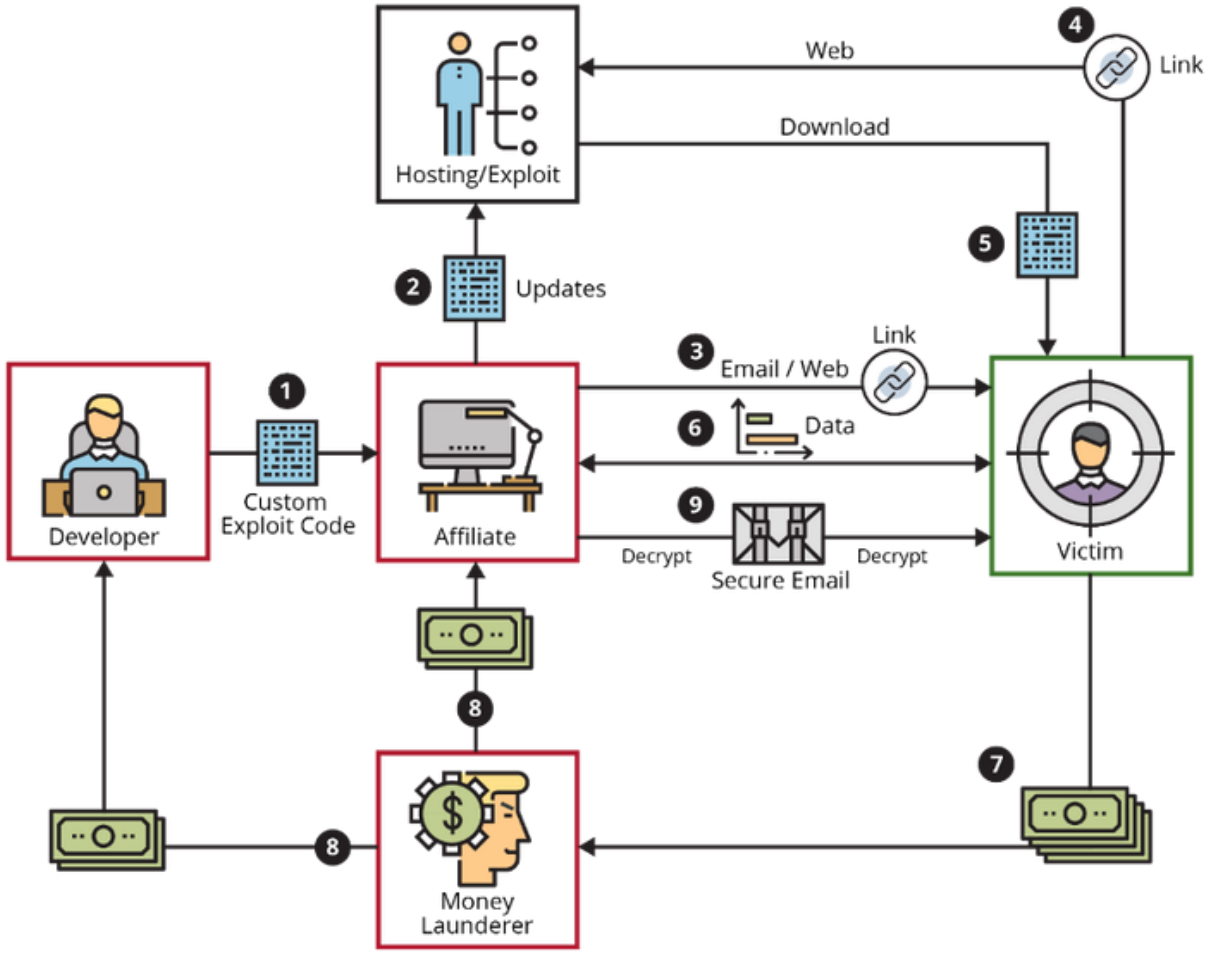
The month-by-month ransomware data gives a much more nuanced view.

Why is Ransomware Rising?

- CyberInsurance
- Ransomware-as-a-Service
- Success of Double Extortion

What is Ransomware-as-a-Service

- **Ransomware as a Service (RaaS)** is a business model used by ransomware developers, in which they lease ransomware variants in the same way that legitimate software developers lease SaaS products.
- May include 24/7 support, bundled offers, user reviews, forums and other features identical to those offered by legitimate SaaS providers



Data World
Your Value - added Distributor

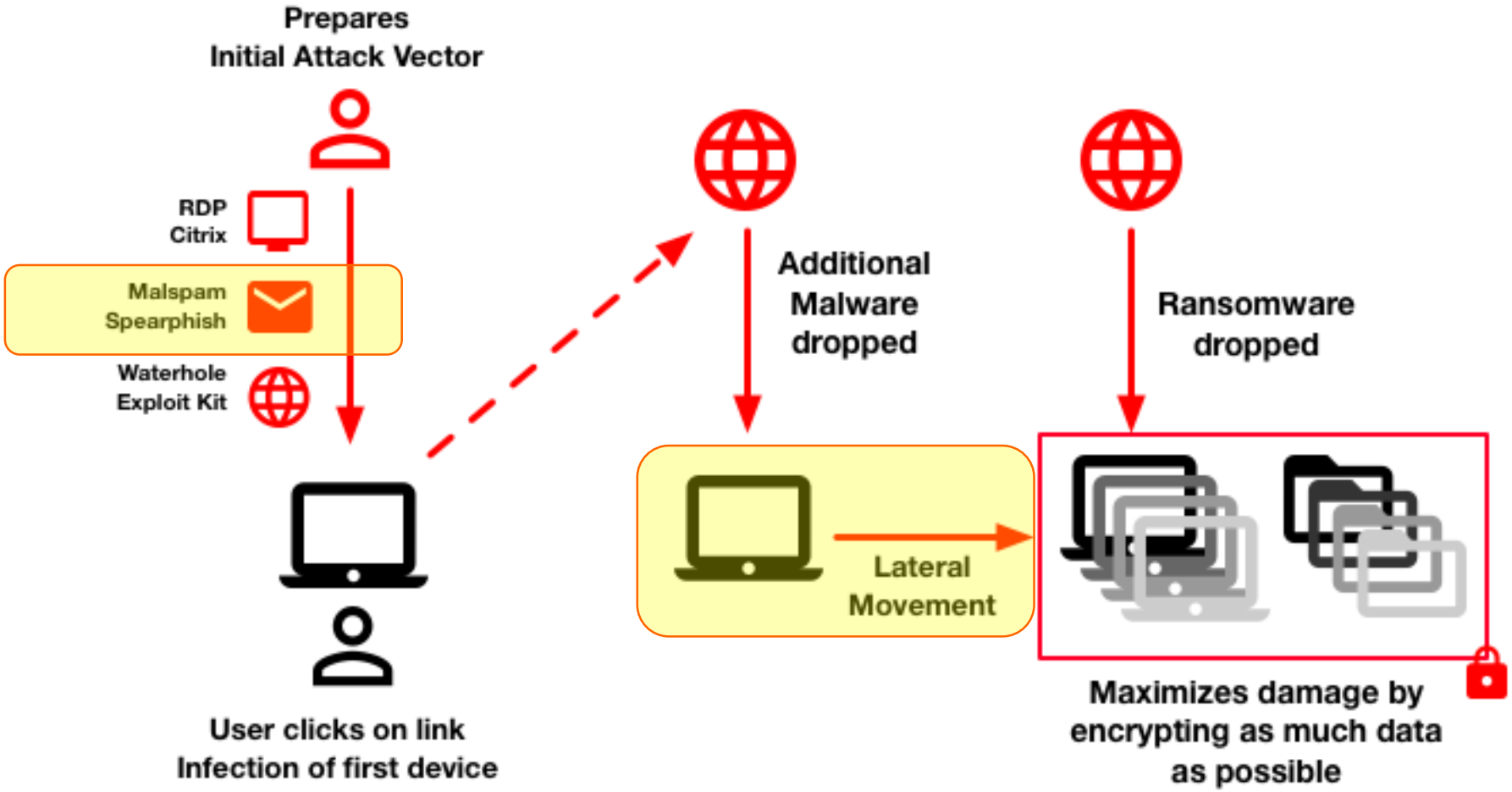
Ransomware as a Service statistics

- **RaaS** is not all that new and has been making headlines since 2016.
- While some RaaS can be acquired fairly inexpensively, some require large deposits.
- That said, kits can be purchased for as low as $175.
- Affiliate payment rates vary greatly but affiliates usually take the larger share.
- For example, the affiliate cut with **Netwalker** is up to 80 percent. **DarkSide** administrators take up to 25 per cent for attacks generating under $500,000 and 10 percent for ransoms above $5 million.

Data World
Your Value - added Distributor

How a Typical Attack Launch?

How a Typical Attack Launch?



Data World

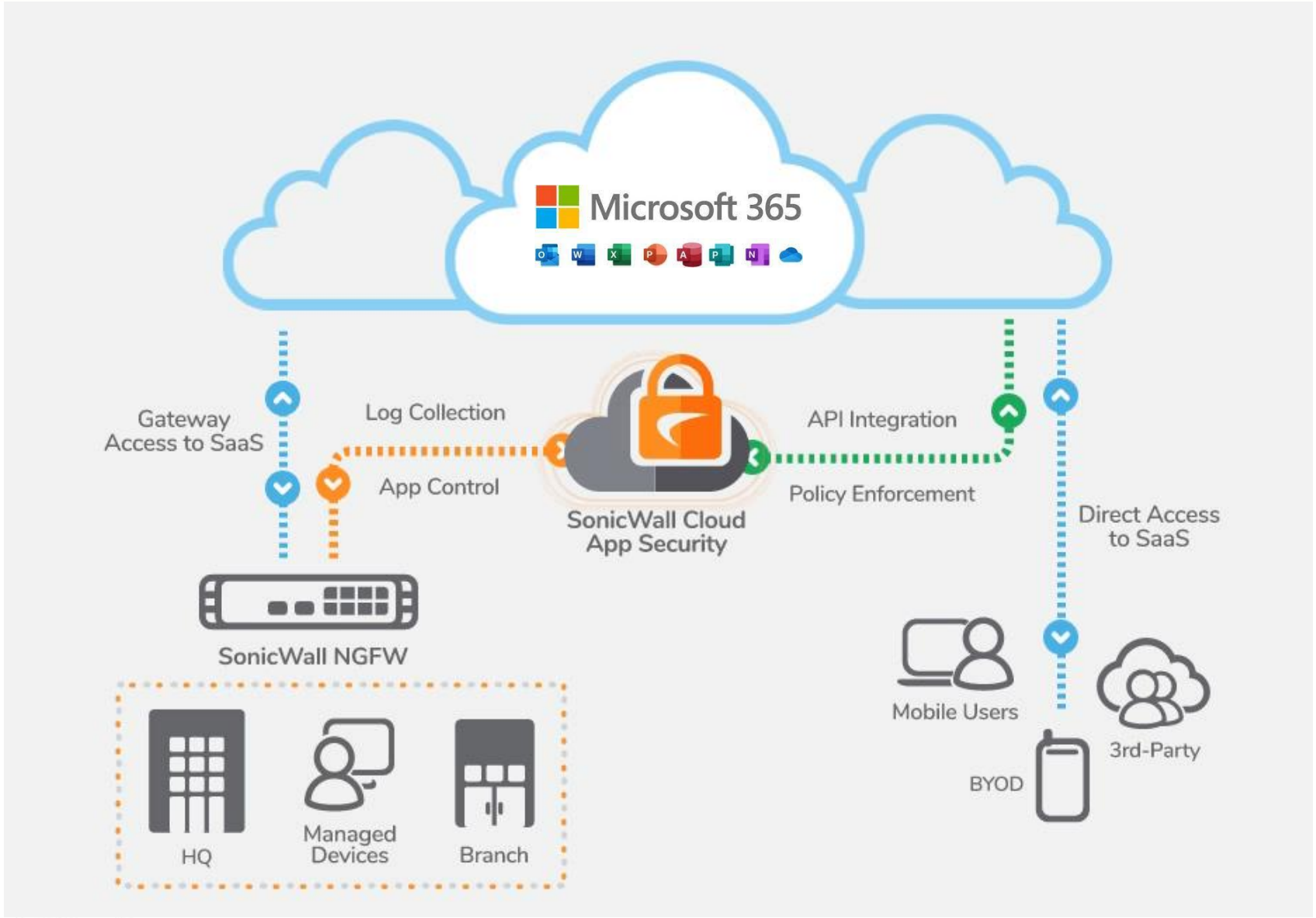
Your Value - added Distributor

What can we do?

STEP 1

On-the-Fly Tackling Strategy: Cloud-based Email Hygiene for Microsoft 365 / G-Suite

Embrace Cloud Applications Without Fear



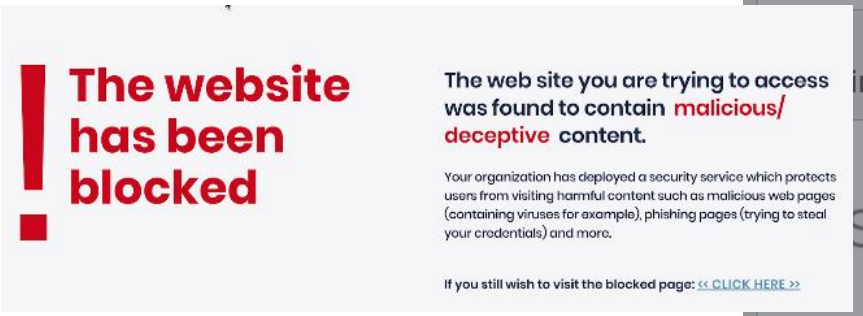
Data World

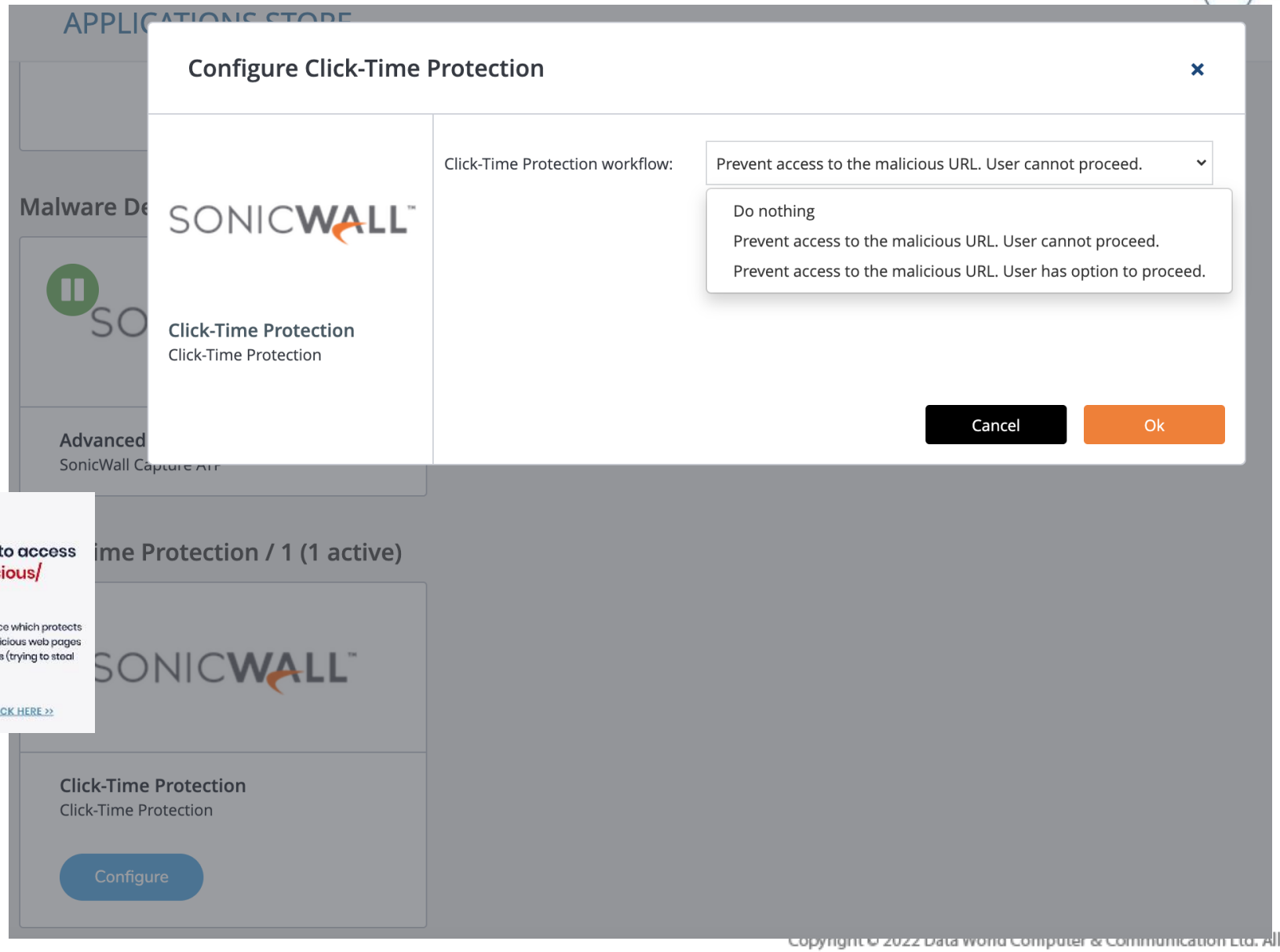
Your Value - added Distributor

Click-Time Protection on Incoming Email Links

How does it work?

- Work based on URL "rewrites“
- Every link within incoming emails is replaced with a CAS URL
- All Inbound, outbound or internal emails
- Test site before redirecting the user once verified as harmless

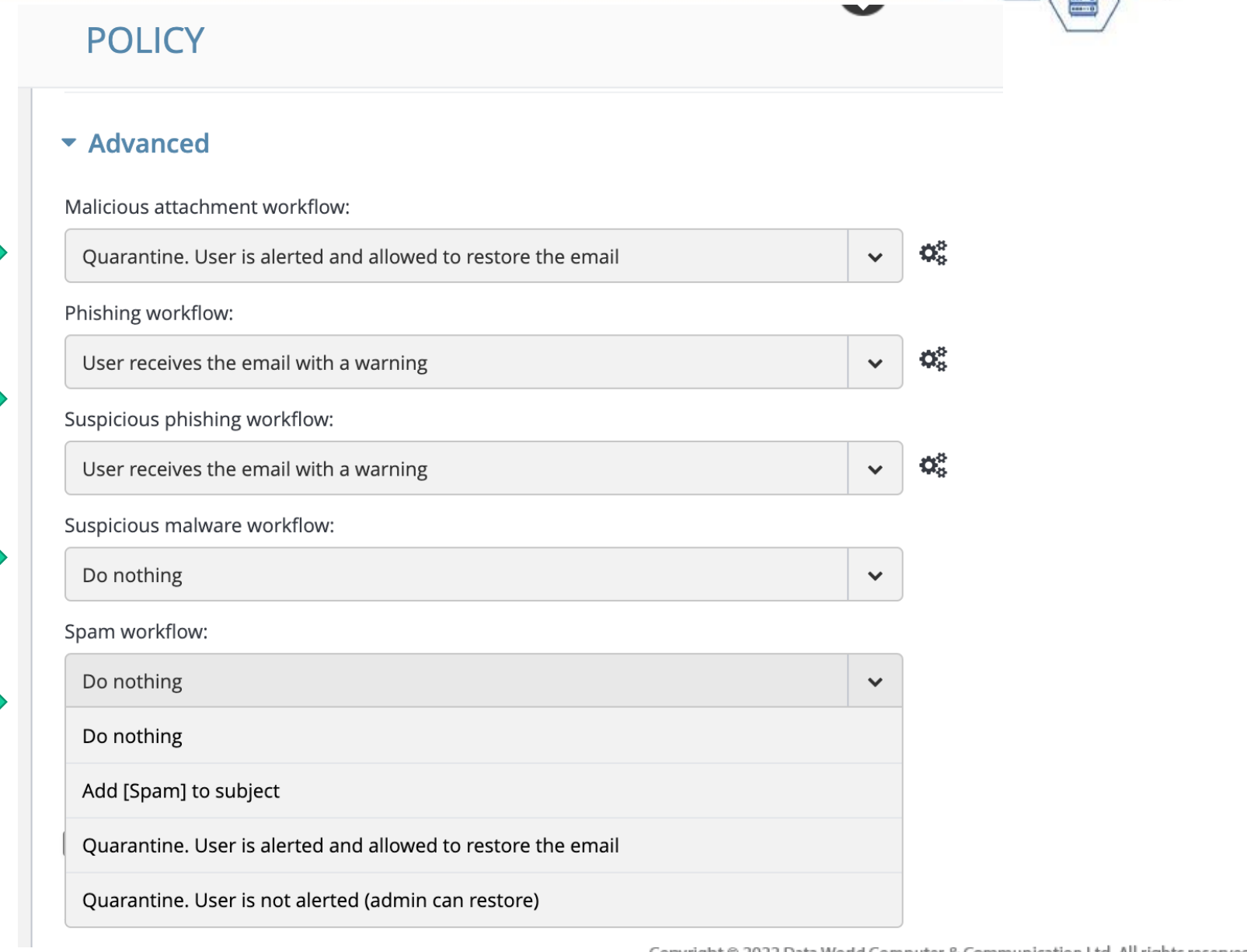




Data World
Your Value - added Distributor

Advanced Malicious Mail Control

- Malicious Attachment
- Phishing Mail
- Malware
- Spam Mail



Data World
Your Value - added Distributor

Comprehensive Protection For Office 365 and G-Suite

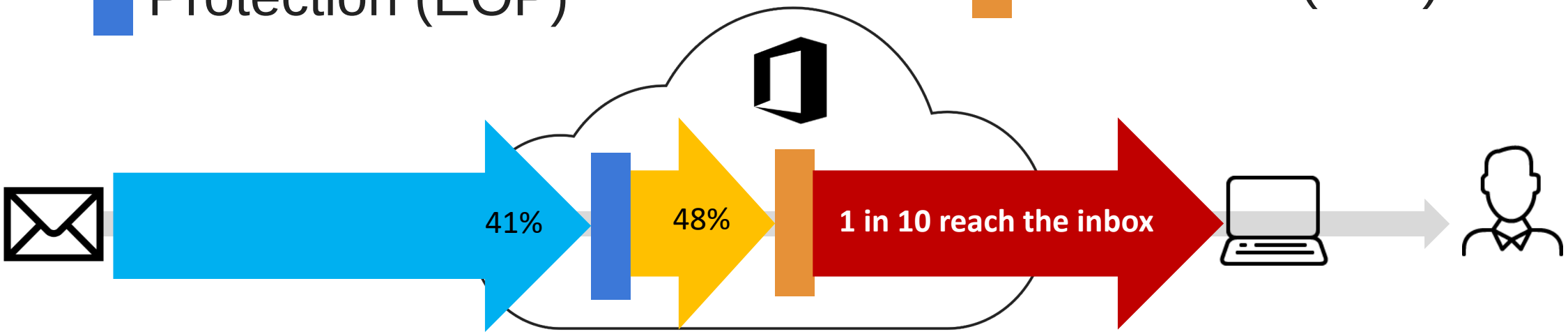
- Get powerful anti-phishing, attachment sandboxing and advanced URL protection
- Scan inbound, outbound and internal email in Exchange Online and Gmail
- Prevent confidential file uploads and unauthorized sharing on OneDrive and Google Drive
- Protect against account takeovers (ATO), insider threats, compromised credentials

Data World
Your Value - added Distributor

Without “Cloud App Security”

Exchange Online Protection (EOP)

Advanced Threat Protection (ATP)



41% of Phishing attacks blocked by EOP

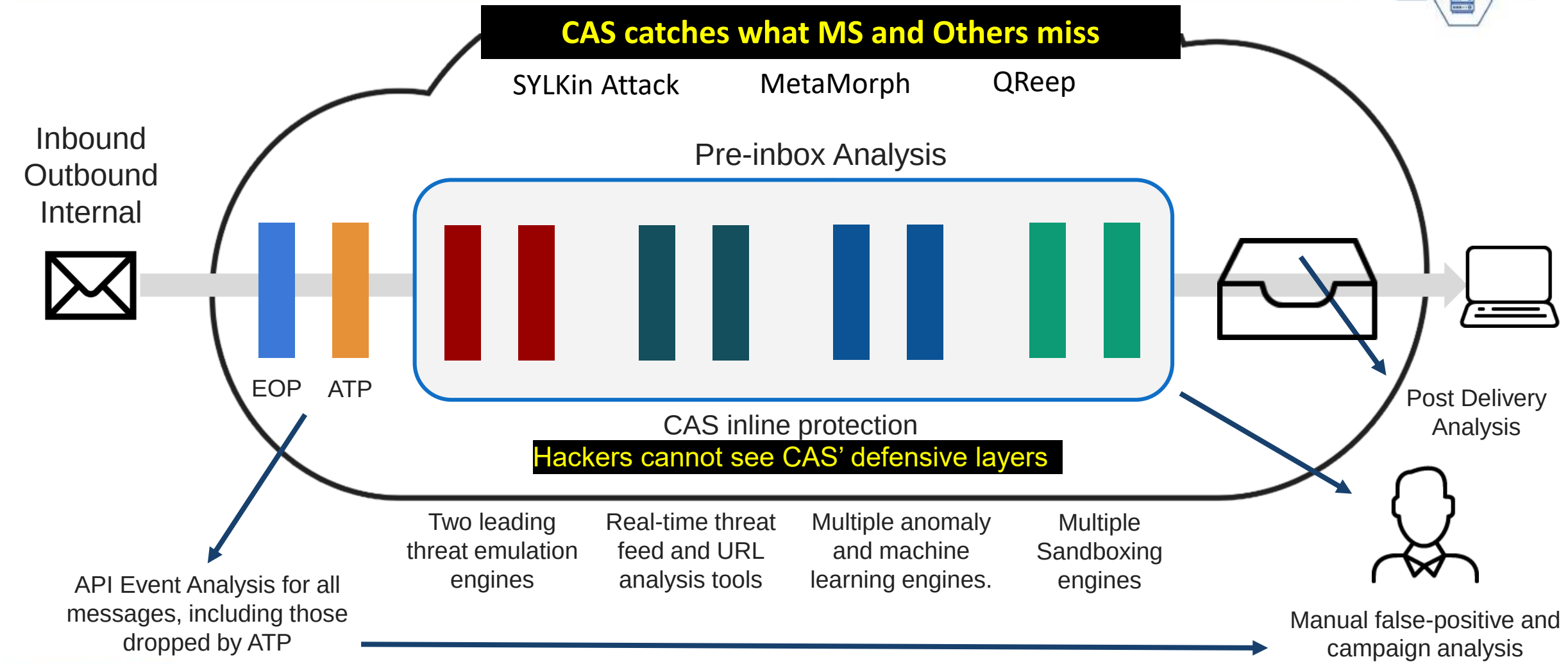
48% of Phishing attacks blocked by ATP

11% of Phishing attacks bypass both EOP +ATP

Data World

Your Value - added Distributor

With “Cloud App Security”

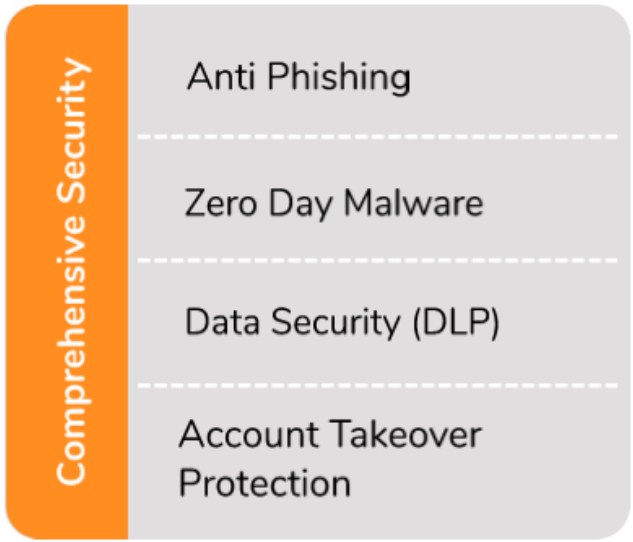


Data World

Your Value - added Distributor

Comprehensive Protection For Office 365 and G-Suite

- Get powerful anti-phishing, attachment sandboxing and advanced URL protection
- Scan inbound, outbound and internal email in Exchange Online and Gmail
- Prevent confidential file uploads and unauthorized sharing on OneDrive and Google Drive
- Protect against account takeovers (ATO), insider threats, compromised credentials

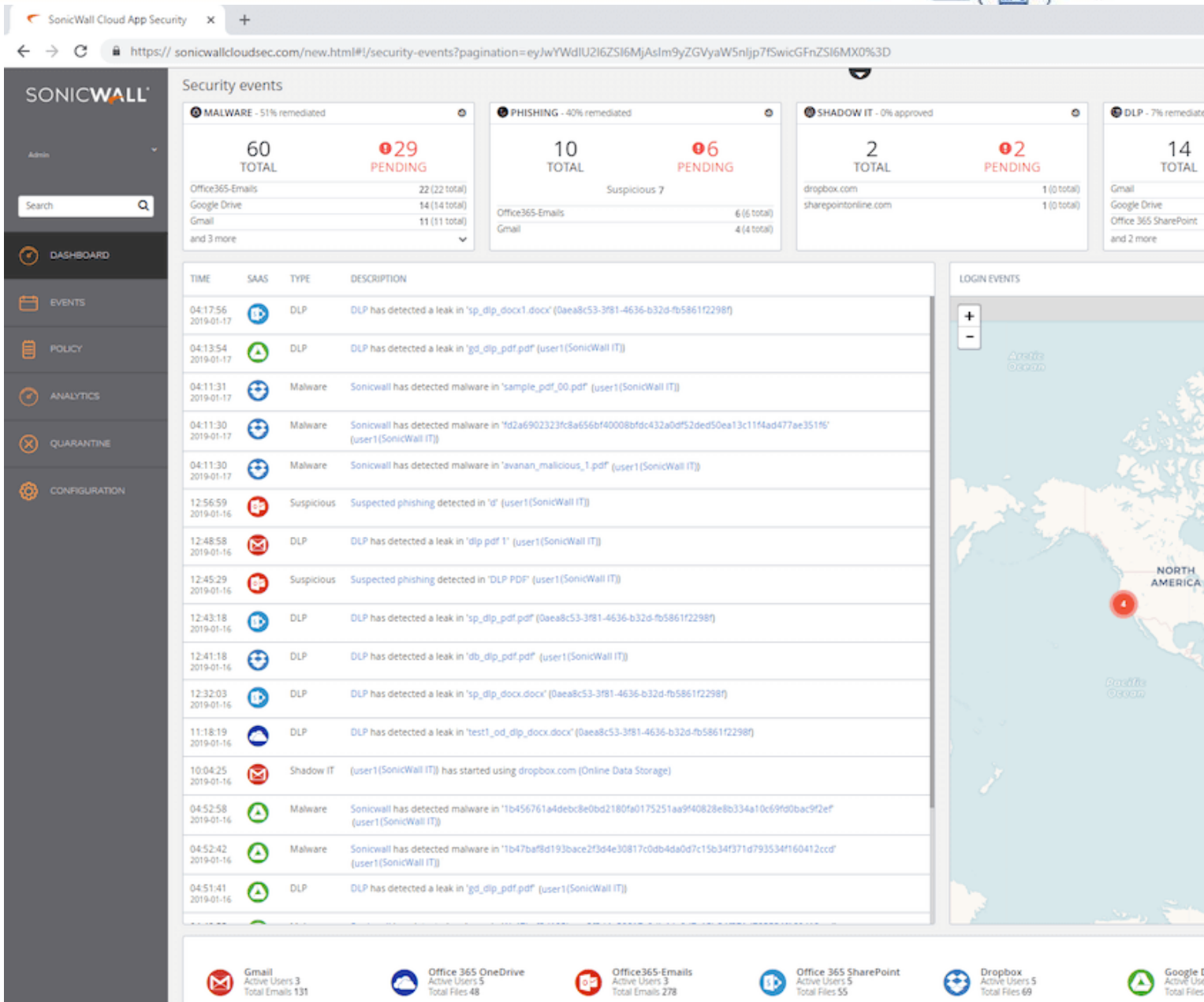


Data World

Your Value - added Distrib

Secure Your Sanctioned SaaS Apps

- Get granular visibility and control through native API integrations
- Identify compromised accounts using machine learning
- Set consistent data security policies across sanctioned applications
- Protect SaaS environments against ransomware and zero-day malware

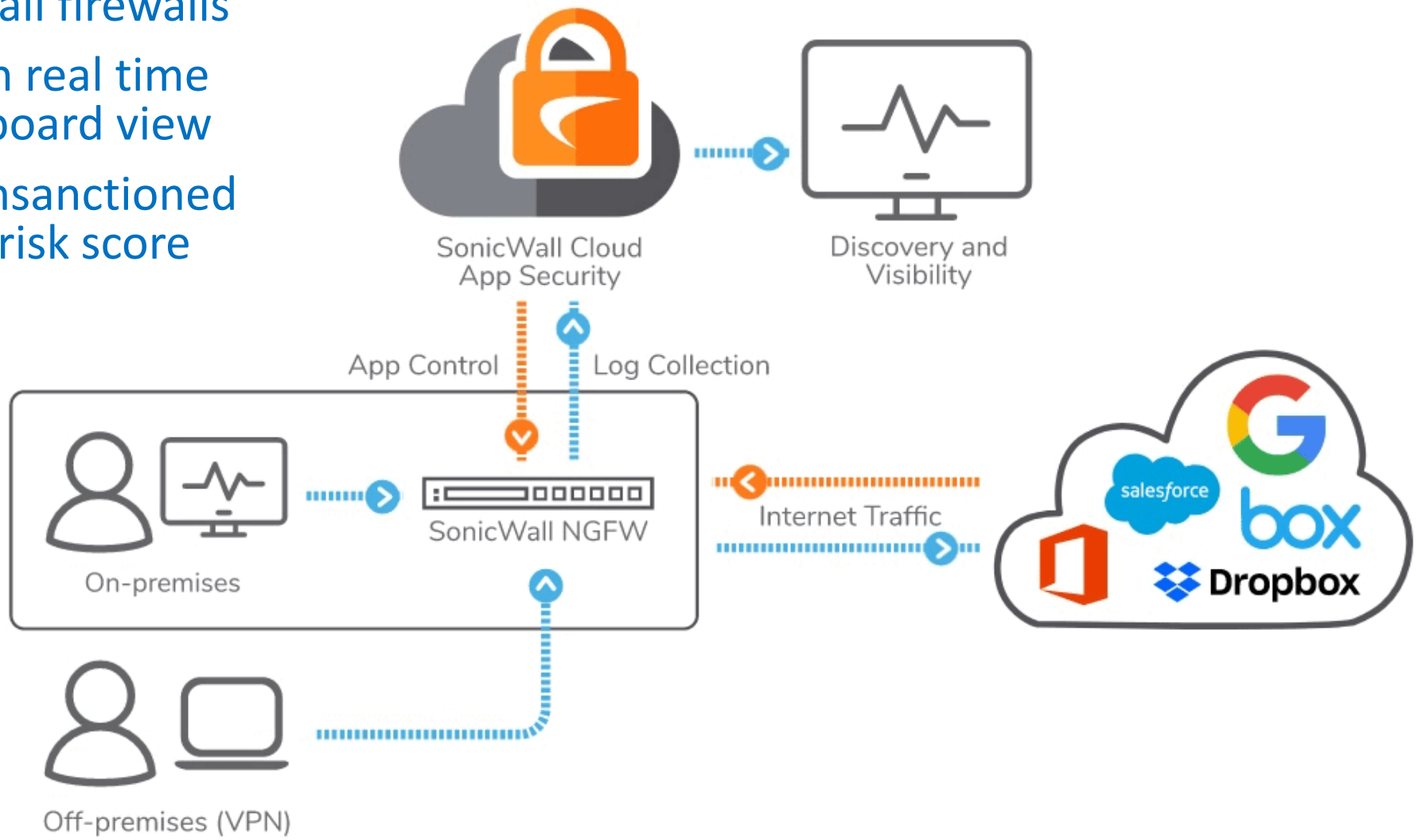


Data World

Your Value - added Distributor

Discover Shadow It

- Automate cloud discovery when deployed with SonicWall firewalls
- Monitor cloud usage in real time with an intuitive dashboard view
- Set policies to block unsanctioned applications based on risk score



Data World
Your Value - added Distributor

Key Takeaways

- Out-of-band, API-Mode Integration → Most ease way to implement
- **Basic:** Anti-Spam, Anti-Virus, Anti-phishing
- **Advanced:** Attachment file sandboxing and URL Sandboxing protection
- **Value-added features:** DLP, Shadow IT Discovery

Data World

Your Value - added Distributor

STEP 2

Landing Tackling Strategy: More than a NGAV: Endpoint Detection & Response (EDR)

The Progression of Endpoint Security

AV
Antivirus

- Antivirus software uses a database of known 'signatures' to detect computer viruses.

NGAV
Next Generation Antivirus

- NGAV includes more advanced features - such as no weekly updates - to close the 'gaps' in AV.

EPP
Endpoint Protection

- Endpoint Protection provides holistic protection on any internet-capable device on a network.

NGEP
Next Generation Endpoint Protection

- NGEP combines advnaced features including behaviour-based detection, machine learning and AI to combat malware. It is a system of security tools, always learning.

EDR
Endpoint Detection & Response

- Endpoint Detection & Response (EDR) detects and contains security incidents; and remediates endpoints to a pre-infection state.

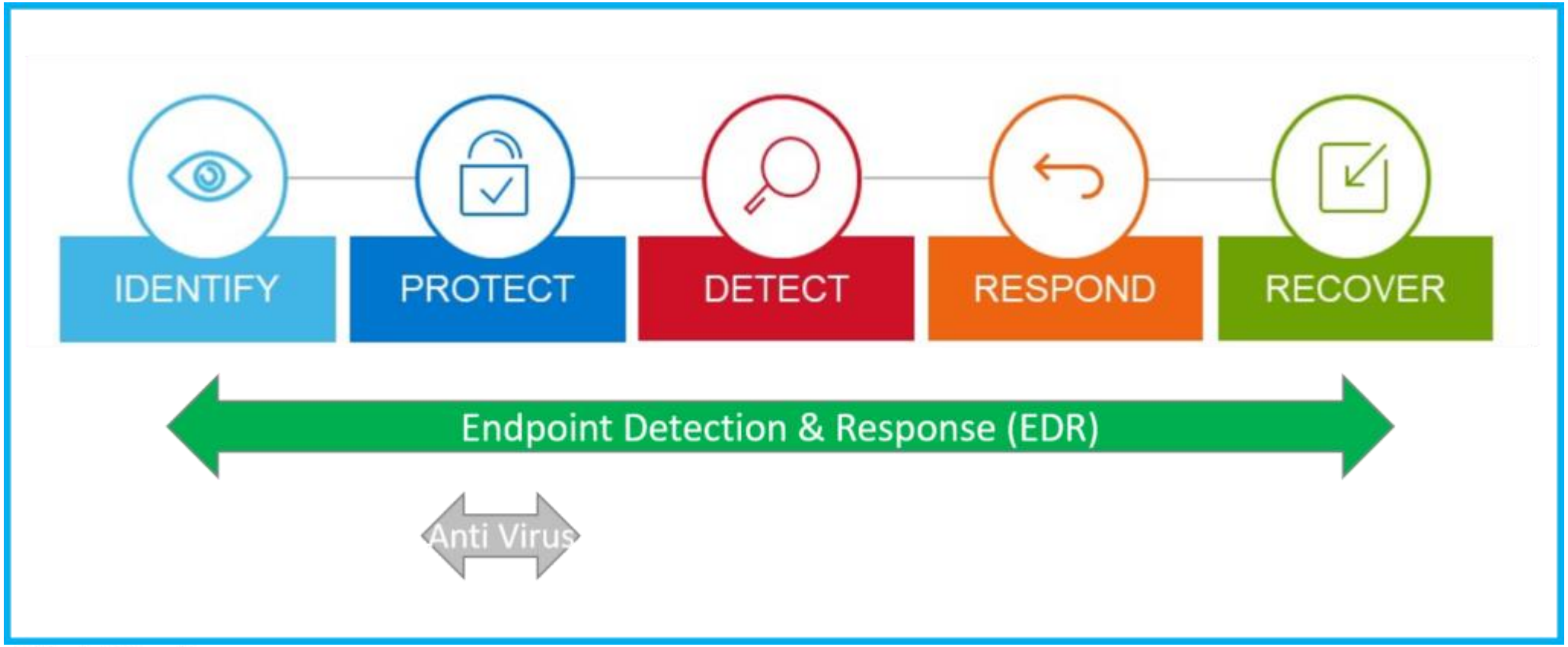
The Progression of Endpoint Security

Data World

Your Value - added Distributor

So, What is EDR?

- **Endpoint Detection and Response (EDR)** is a new form of cyber security technology that helps continuously **monitor, prevent**, **detect**, and **respond** to ever-changing cyber threats and **recover** quickly when ransomware or other exploits strike. If a attack does occur and is successful remediation and rollback features help reverse the effects of an attack and recover devices to their pre-attack healthy state significantly reducing business downtime.



Data World
Your Value - added Distributor

Sentinelone Endpoint Protection Platform
Partnering to bring best-of-breed protection

EXECUTABLES

FILELESS MALWARE

MALICIOUS DOCUMENTS

BROWSER EXPLOITS

LIVE SCRIPTS

CREDENTIALSTEALERS

EPP+EDR

Pre-Execution Static AI engines	**On-Execution Behavioral AI Engines**	**Post-Execution Automated EDR**
Replaces traditional signatures	Vector-agnostic	Auto-mitigate threats
Obviates recurring scans	Track all processes	Isolate & Rollback
Device Control	Detect malicious activities	Storyline-based Threat Hunting
Vulnerability Intelligence	Respond at machine speed	Custom Rules

Gartner peerinsights™

AV-TEST APPROVED CORPORATE ENDPOINT PROTECTION av-test.org 06/2015

MITRE ATT&CK™

vb 100 VIRUS virusbtn.com

100% Protection Score SE Labs AAA ENTERPRISE ENDPOINT PROTECTION SentinelOne

Data World
Your Value - added Distributor

SonicWall Capture Client
Best of Both Worlds: SentinelOne NGAV + SonicWall Platform

SentinelOne™

BETTER NGAV

- High-accuracy Protection
- Endpoint Remediation and Rollback
- Best-in-Class for MacBooks
- Application Vulnerability Intelligence
- Deep Visibility
- Remote Shell

SYNERGIZES WITH SONICWALL TECHNOLOGY

- Unified Management and Reporting
- Capture ATP Integration
- DPI-SSL Certificate Management
- Firewall Enforcement
- Content Filtering

SONICWALL®

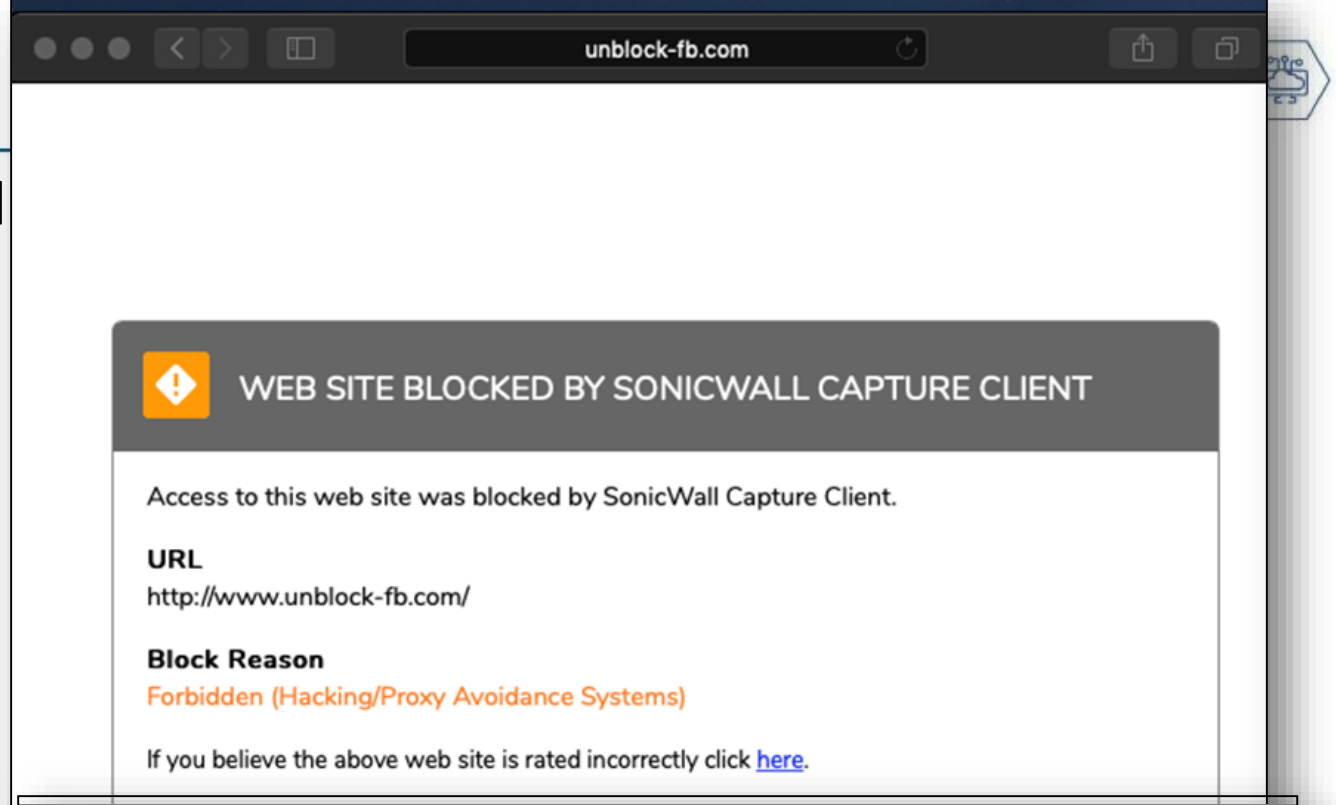
Mac OS

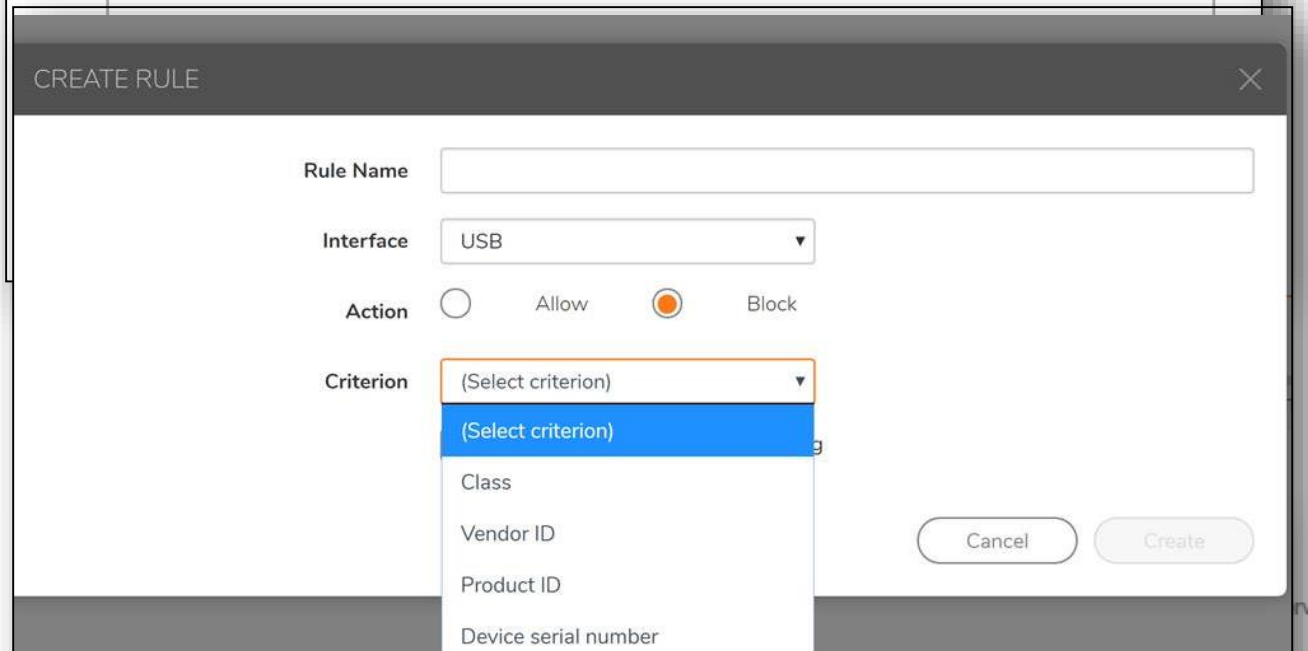
Data World
Your Value - added Distributor

Unified Client

NGAV, Content Filtering and Device Control

- Light-weight NGAV with no DAT files, only real-time AI-based threat prevention
- Protecting from exposure with
  - web content filtering
  - application vulnerability intelligence, and
  - removable device control
- One client, one management console - simplify operations!



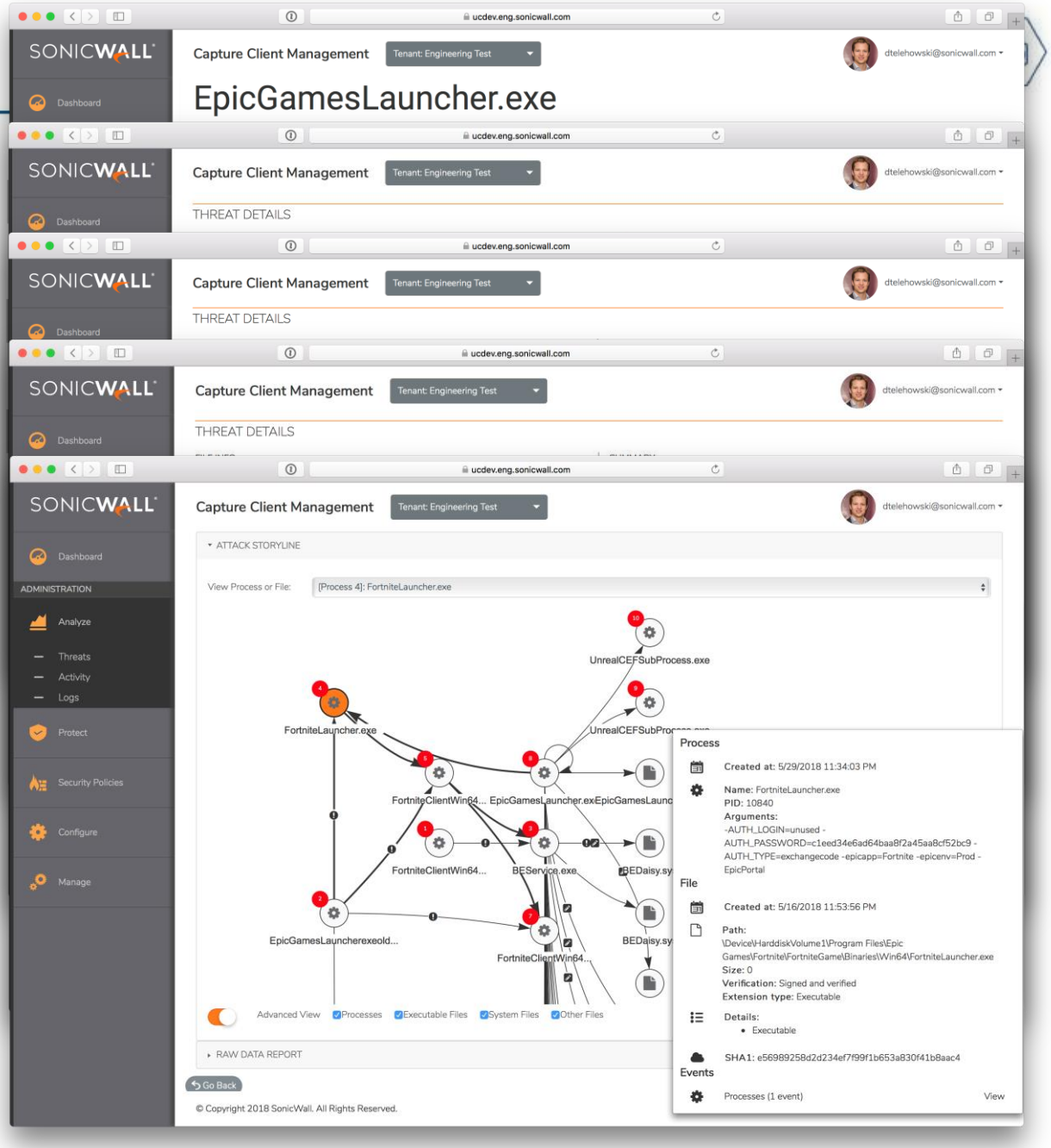


Data World
Your Value - added Distributor

Endpoint Detection & Response

Attack storyline and automated response

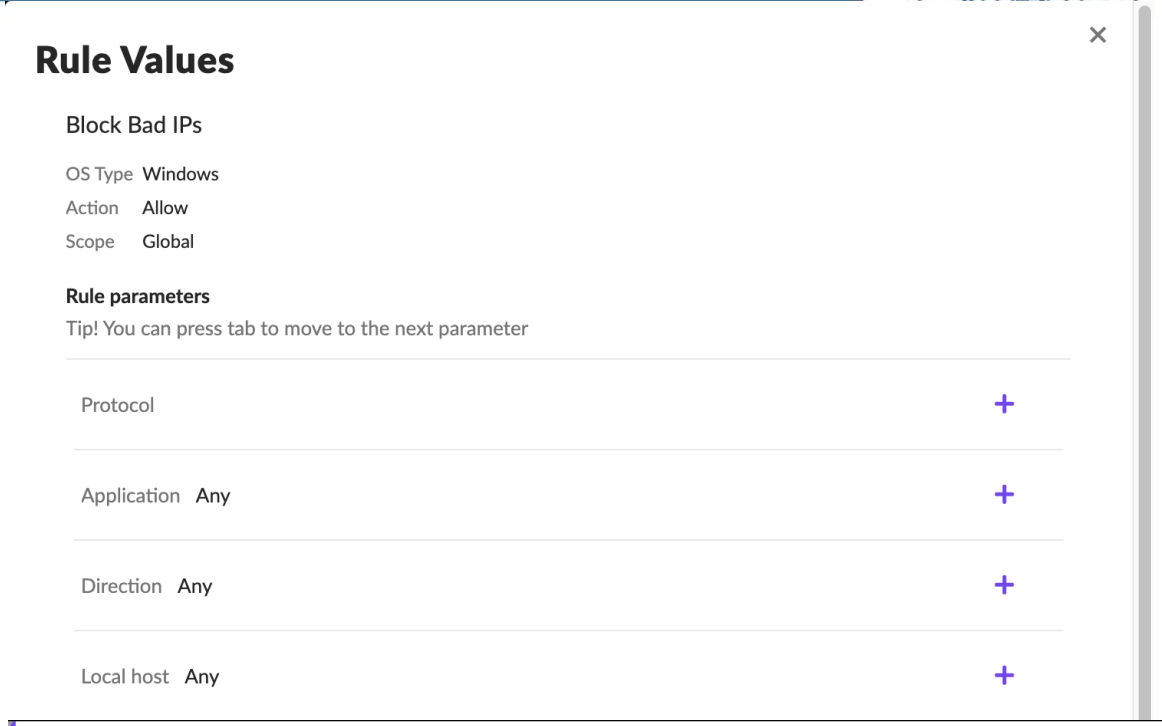
- Visually analyze threat execution with event statistics, IOCs and detailed intelligence
- Isolate potentially compromised endpoints and avoid lateral infections
- Rollback compromised endpoints and avoid paying a ransom

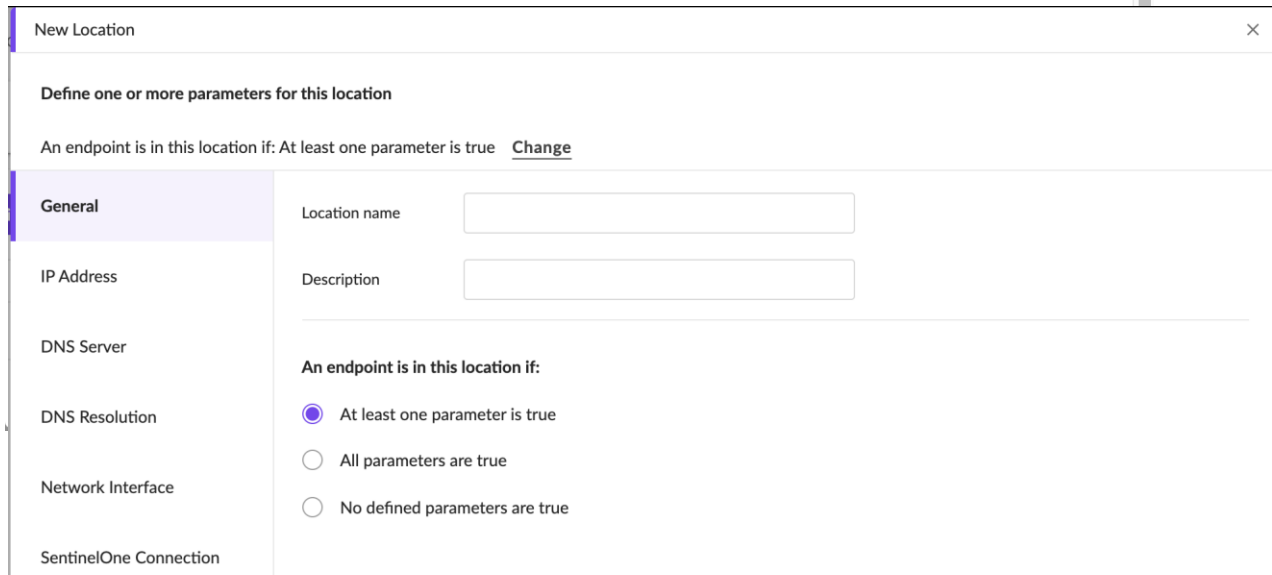


Data World
Your Value - added Distributor

Network Control

- Provide Firewall rules to the endpoint in order to function no matter where it is.
- Configurable network quarantine rules for advanced remediation and response
- Define location-specific rules – on-network, off-network, wired vs wireless etc.

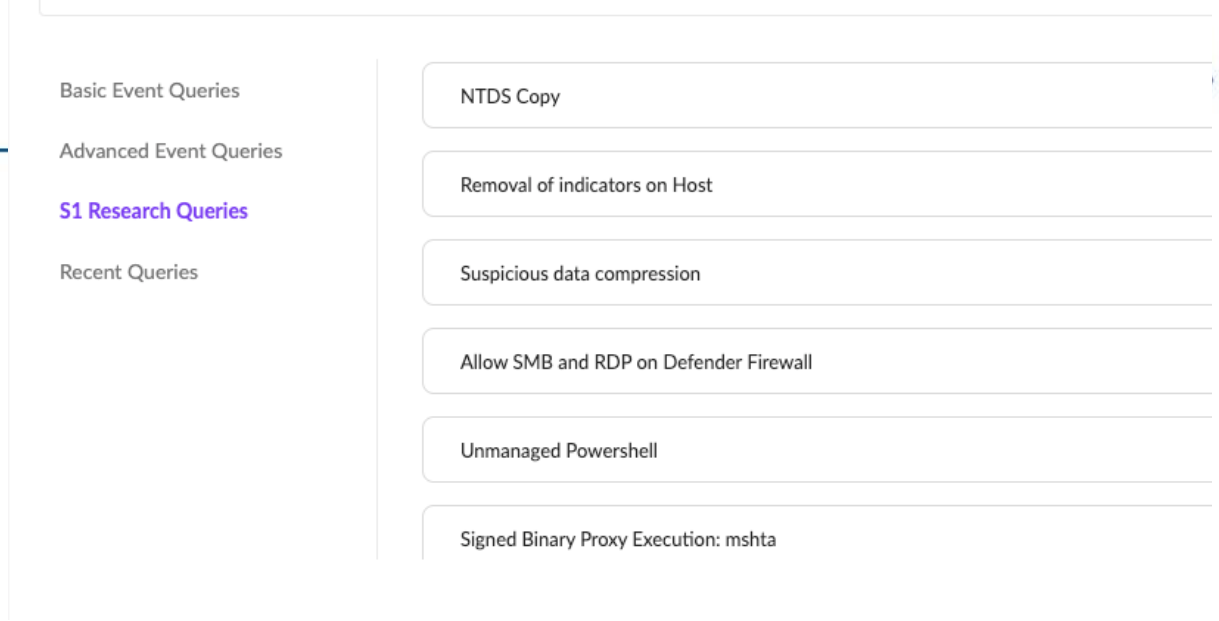


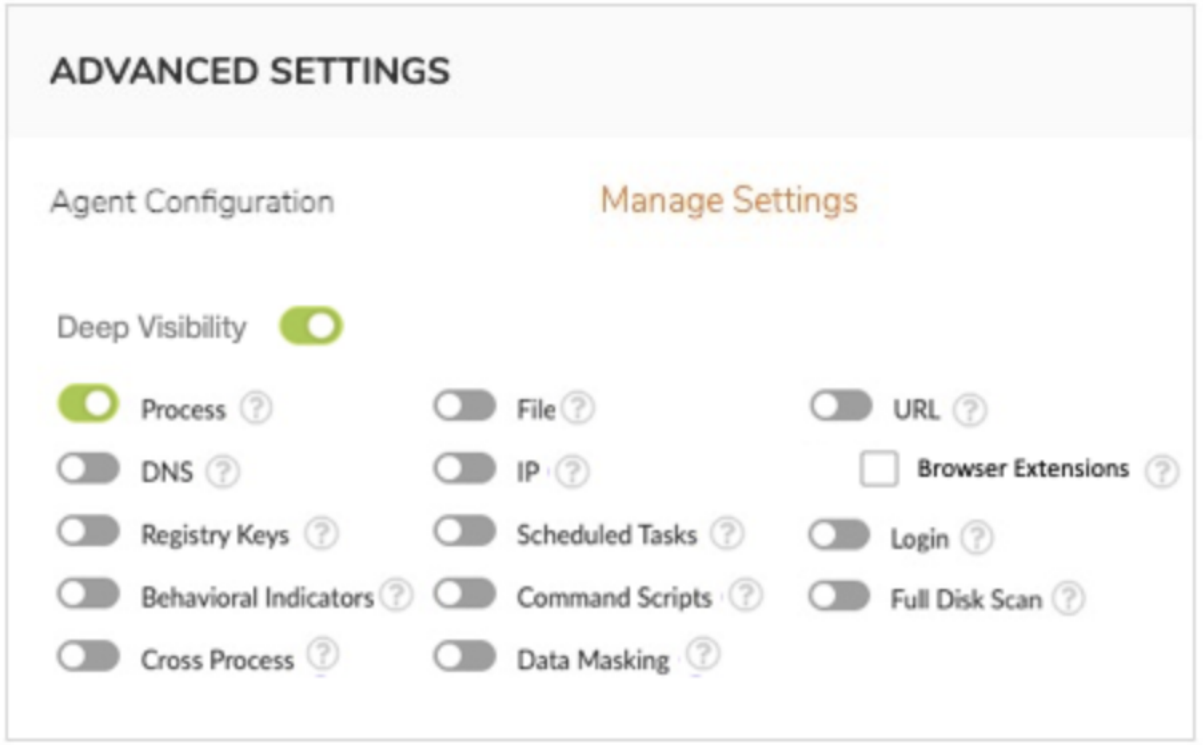


Data World
Your Value - added Distributor

Deep Visibility Threat Hunting

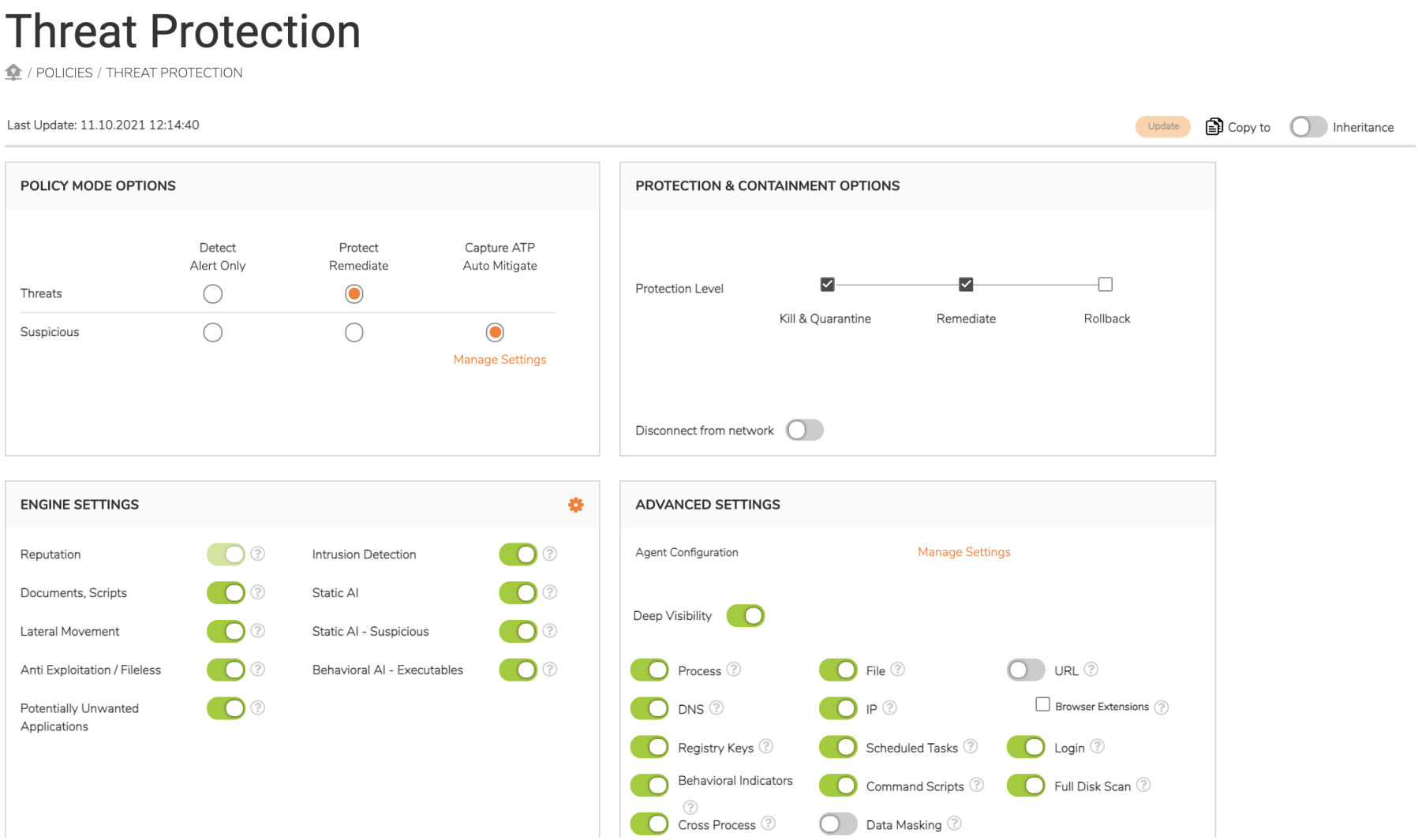
- Know the Unknown with Capture Client's Deep Visibility
  - Easily find "related" IOCs using Storyline-based hunting
  - Easy to use query interface with numerous tooltips and auto-complete
  - Out of the box queries to get you started
  - Customize what data to collect for Hunting





Data World
Your Value - added Distributor

Granular and scalable policy management



- "Quickstart" with default - Best Practice
- Customize for Groups
- Leverage Inheritance to scale across groups and tenants – MSSPs & Large Enterprises

Integrated Security with the SonicWall Platform

SONICWALL® | CAPTURE SECURITY CENTER

SINGLE PANE OF GLASS

MANAGEMENT & REPORTING

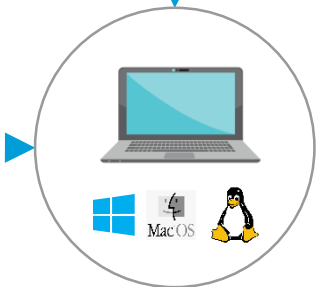
NETWORK+ENDPOINT ANALYTICS

SonicWall Firewalls

TZ, NSA, NSv

Firewall Endpoint Synergy

Capture Client Enforcement
DPI-SSL Enforcement
User & Device Telemetry Sharing
Block on Network; Notify on Endpoint



SonicWall Capture Client

Advanced Threat Prevention, Firewall Synergy and Endpoint Detection & Response

Data World

Your Value - added Distributor

Key Takeaways

- **Know the Unknown:** Protect everything that AV missed
- **Unified visibility and control:** Hunt for Hidden Threats
- **Saving Time on Mitigation:** Start with Best Practice, supporting auto-remediation
- **Value-added features:** Firewall-Endpoint Synergy

Data World

Your Value - added Distributor

Essential Remote Working Technology

Integrated Security with the SonicWall Platform

Integrated End Point Control

OPSWAT.
Included

Microsoft Intune

Desktop client

Mobile client

Client-less web access

Secure Access Gateway

SMA


SMA 6210/ 7210

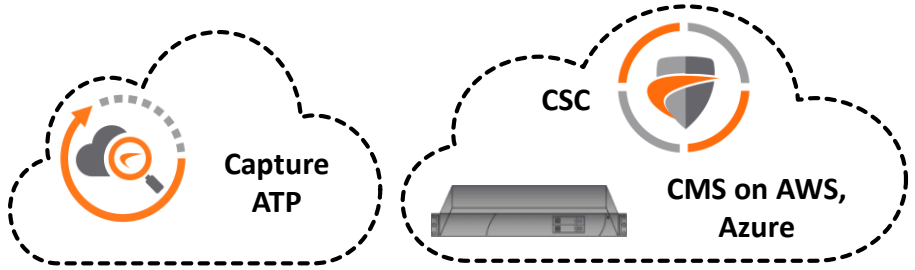

SMA 8200v


SMA 210/ 410


SMA 500v

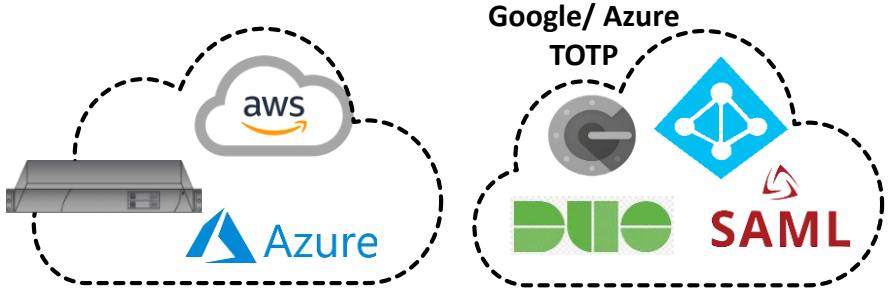
Physical and virtual form factors or cloud instances

Integrated Cloud Services



SonicWall Sandbox

SMA Management Systems



SMA on Public Clouds

MFA

Data World
Your Value - added Distributor

Firewall - NAC Solution, Coworking Synergy

Firewall – NAC Solution Coworking Synergy

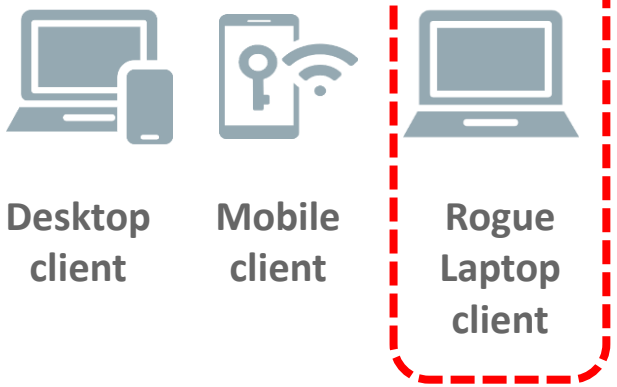
End Point Device

Network Access Control

Network Firewall

Agent / Agentless

CGX ACCESS | Easy NAC



Desktop client

Mobile client

Rogue Laptop client

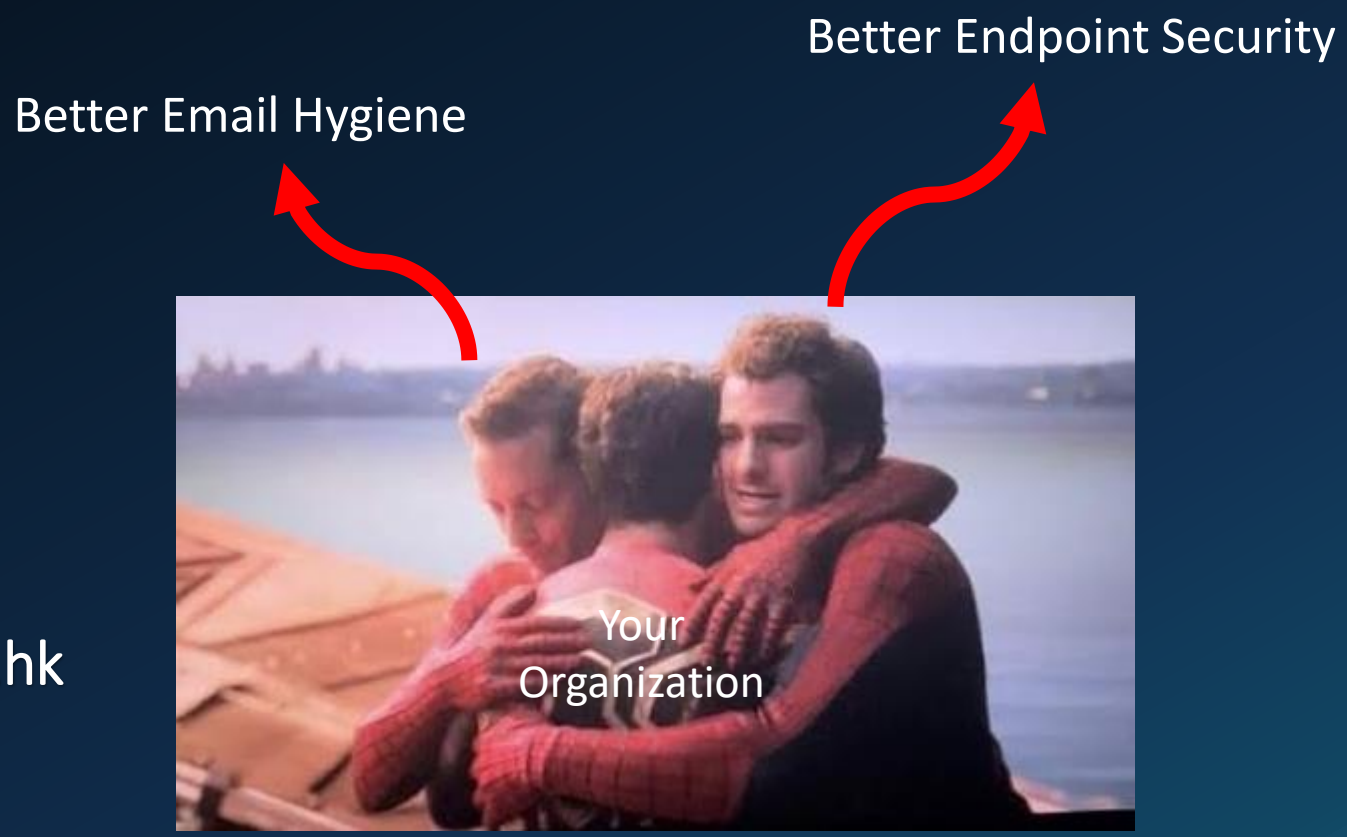
CGX ACCESS | Easy NAC

Physical / Virtual Firewall Appliances

Data World

Your Value - added Distributor

THANK YOU



For Enquiry, please contact
Tel: (852) 2565 8733
Email: marketing@dataworld.com.hk

DATA WORLD COMPUTER & COMMUNICATION LIMITED

Hong Kong Headquarter
Address: 18/F., Manhattan Centre, 8 Kwai Cheong Road, Kwai Chung, Hong Kong
General Enquiry: (852) 2565 7868 Sales Enquiry: (852) 2565 8733
Technical Support: (852) 2187 2267 HK | (853) 6545 2363 Macau
Fax: (852) 2590 7849
Email: marketing@dataworld.com.hk
Website: https://dwcc.dataworld.com.hk/