PRODUCT ANNOUNCEMENT

Brought to you by:

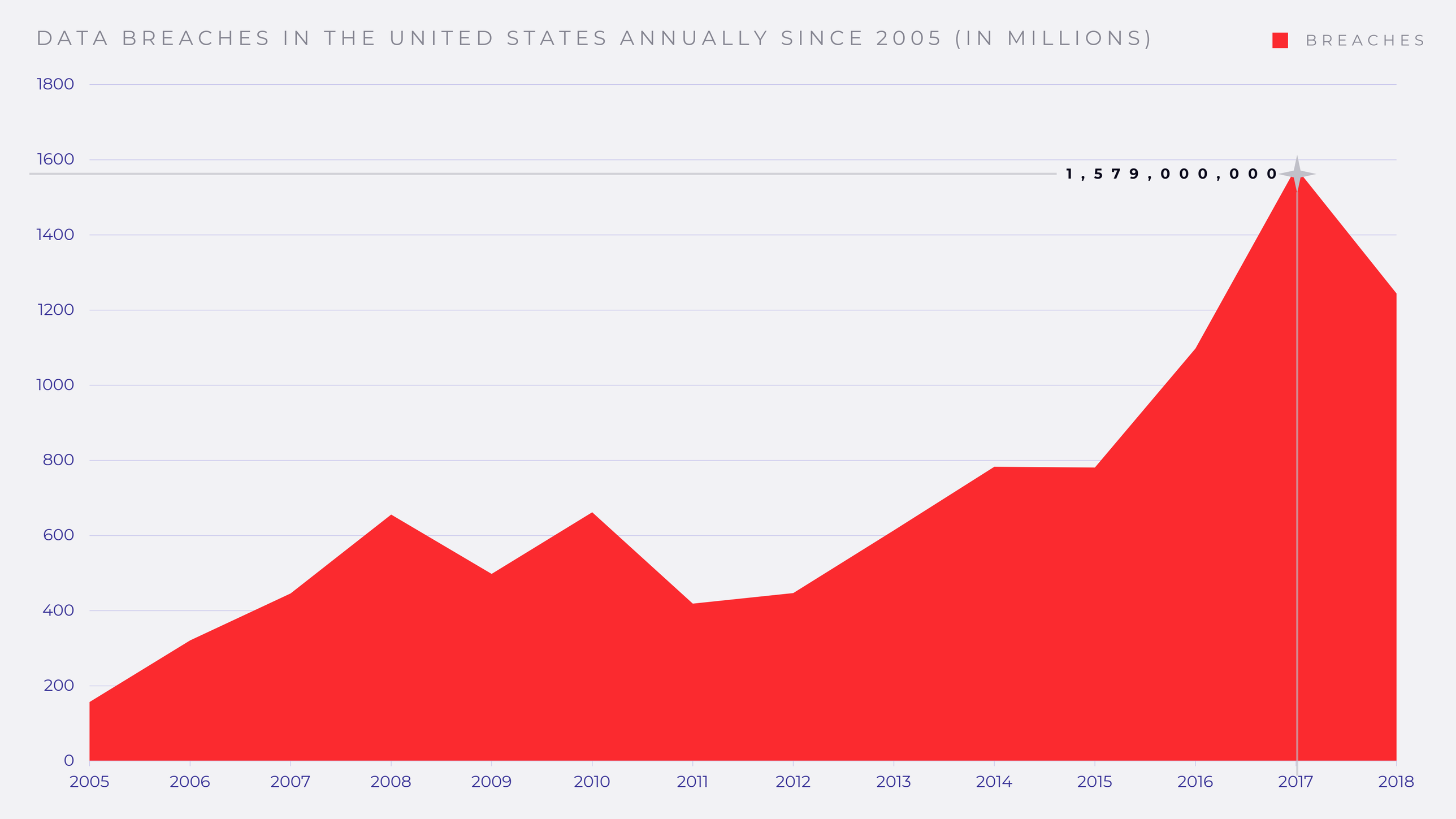
COMODO
CYBERSECURITY

Visit us online at
enterprise.comodo.com
for more information

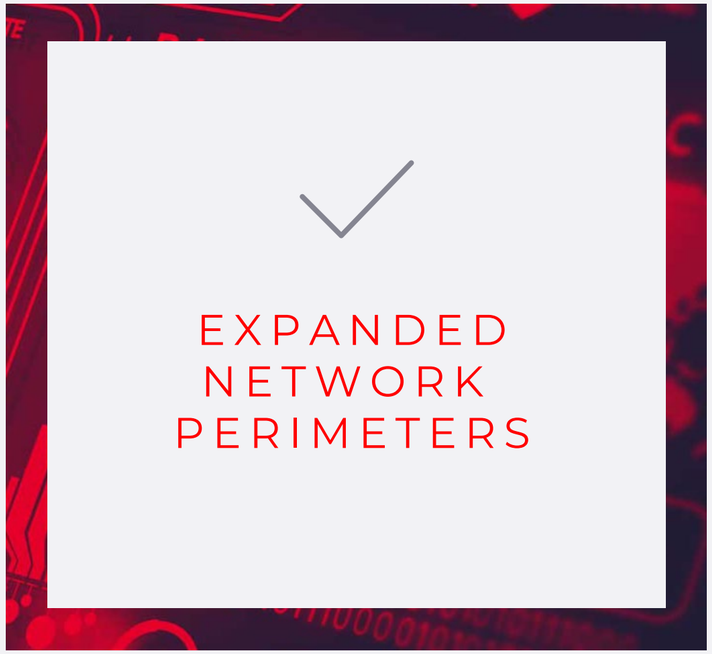
1

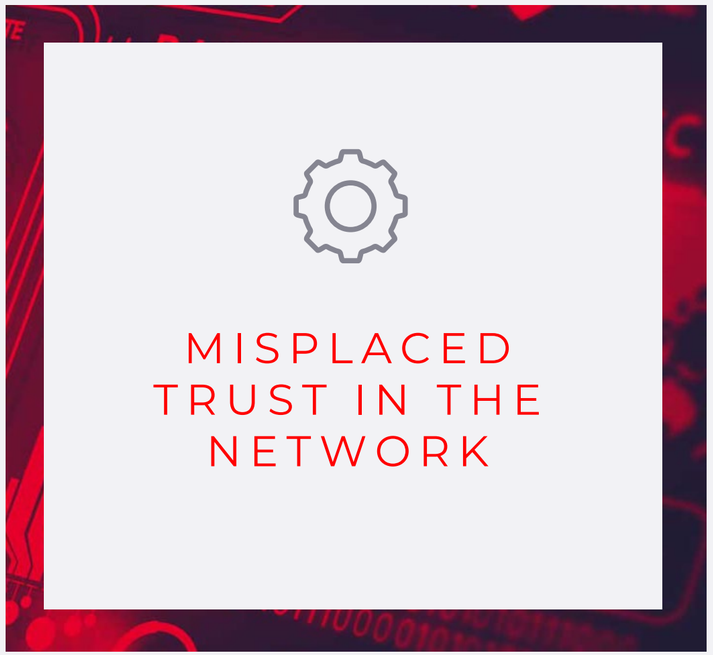
BREACHES TODAY CONTINUE TO RISE

DATA BREACHES IN THE UNITED STATES ANNUALLY SINCE 2005 (IN MILLIONS)



VULNERABILITY VECTORS





39 SEC

How often a cyber attack occurs

22%

Use stolen credentials to commit their data breach

1 IN 10

Attack groups use malware to disrupt business operations

3%

Company folders that are protected

THE COST OF A BREACH

The average cost per lost or stolen record in a data breach

The average total cost of a data breach

The cost of lost business after a breach for US organizations

DATA BREACH CONSEQUENCES

Immediate Policy and Infrastructure changes

Ceding market share to your competitors

Termination of leadership team

Brand reputation lost or go out of business

“It’s about the only executive-level job I can think of where you are 100% accountable for the failures to come, even though it’s a guarantee that they will happen at some point. It’s like playing chess with a blindfold on — you cannot win.”

—Chase Cunningham, Forrester Security & Risk Analyst

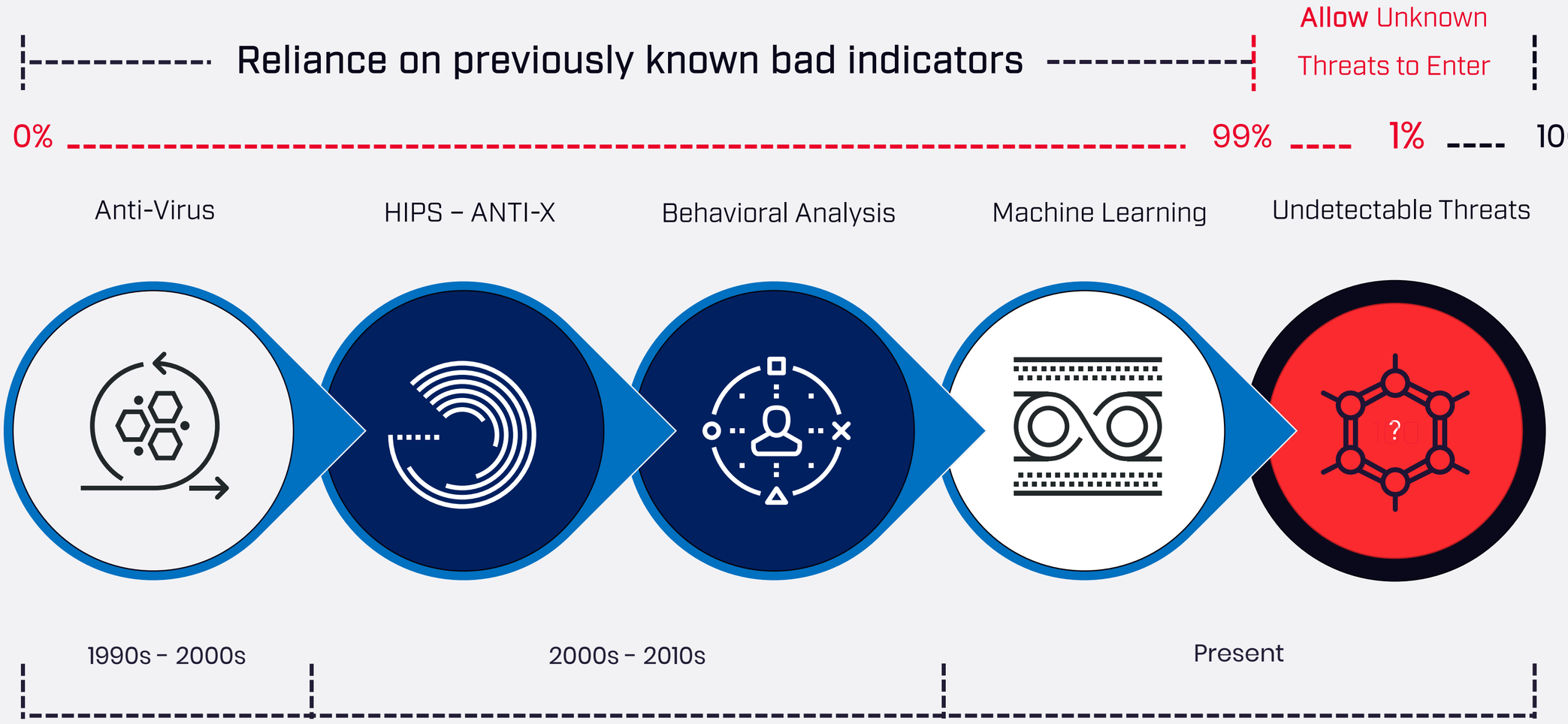
YAHOO	IBM	UBER	EQUIFAX
When Russian state security breached the search engine giant, the botched response and clumsy cover-up cost Yahoo's top lawyer his job and hit CEO Marissa Meyer with a seven-figure financial loss	Lax security procedures in IBM Eastern European offices led to a mass compromise of PII contained in Sweden's Department of Motor Vehicles databases. In this case, the customer took the blame and the Director General of Sweden's Transport Agency was fired for IBM's negligence	This hack exposed the personal information of 57 million Uber customers and drivers. Uber paid the scammers $100,000 ransom and attempted to get them to sign an NDA. The company's CSO and legal director for security were both fired for the ham-handed response	In the wake of this epic hack, which exposed PII of just about everyone in the United States, the CSO and CIO "retired", followed shortly by CEO Richard Smith. The company attempted to blame the incident on a single, unnamed individual who failed to update a software patch

SOURCE: CSOONLINE.COM

2

THE RISKS OF TODAY'S SECURITY POSTURES

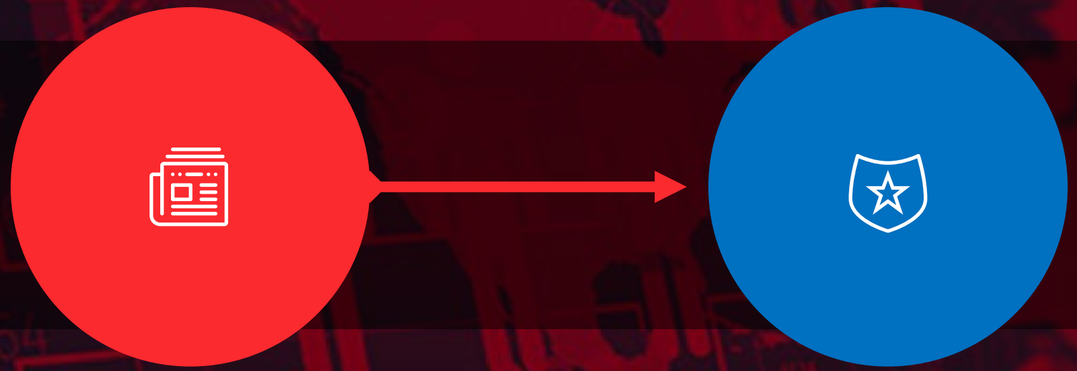
CHALLENGES OF DETECTION METHODS



LEGACY

"Trust" all internal traffic by default

Unrestricted access inside the network



MAINSTREAM

No traffic is inherently "trusted".

Access to all data or assets must be approved by policy

TRUST IS AN EMOTION THAT CANNOT BE APPLIED TO DIGITAL SYSTEMS

How can you stop the damage from an undetectable active breach?

COMODO

INTRODUCING

DRAGON ENTERPRISE

ENDPOINT PROTECTION PLATFORM

Unified Policy and Report Management makes Dragon Enterprise easy to manage and reduce operational costs. The product will also cover Managed Detection and Response services which could help reduce opex of customers even further. Our Security Services offer, MDR Threat and Asset Modelling, Risk Management, Anomaly Detection by Profiling, Dark Web Analysis and Automated Response.

THE LATEST EPP TECHNOLOGIES AND SECURITY

PATENTED UNKNOWN FILE CONTAINMENT

ACTIVE BREACH PROTECTION

ENDPOINT DETECTION & RESPONSE

At its' core, Dragon Enterprise provides full EPP functionality and Active Breach Protection with patented Unknown File Containment. Dragon combines Detection and Prevention in a unique method, while preventing attacks that may come from any threat vector, provides full attack chain visibility. Dragon's prevention capabilities are unmatched in market providing 100% coverage for Zero-Day attacks, and in the meantime delivers most powerful and extensive detection and Threat Hunting capabilities.

CONTAINMENT GIVES YOU 100% PROTECTION

Detection and protection goes hand in hand with Dragon Enterprise. Unlike solutions in market Dragon focuses on delivering Active Breach Protection by combining Endpoint and Network Security. Dragon prevents any breach at its' core by patented Unknown File Containment Technology. Other solutions ' detection capabilities are focused on detection first hence creates risk for Zero-Day Attacks. Dragon Enterprise covers the loose ends with Containment Technology providing 100% protection against Zero-Day Attacks and Unknown Files even if you are the Patient Zero.

ENHANCED FEATURES

Upgraded Core Agent

The new platform includes everything that is required to stop breaches and requires no reboot or additional configuration! Just by installing the lightweight agent, all features provided with Dragon can be activated and will work on and off network.

Improved UI & Usability

Dragon’s security architecture simplifies breach detection, protection and visibility by working for all threat vectors without requiring any other agent or solution.

Integrated Security Architecture

Integrated Security Architecture of Dragon Enterprise delivers Full Attack Vector Visibility including MITRE Framework. Dragon Enterprise provides full EDR and EPP. This unique approach provides visibility on all attack vectors and delivering active prevention in all.

CONTINUOUS THREAT HUNTING

Endpoint Detection & Response

Systems Information And Event Management

Network layer Protection

Integrated security Architecture of Dragon Enterprise doesn't only provide ease of use, but also provides best in market Threat Hunting capabilities. Unlike competitors who rely on endpoint-based metrics, or without requiring any SIEM solution, Dragon Enterprise makes analysis and detection of threats that can come from any vector easy and more comprehensive.

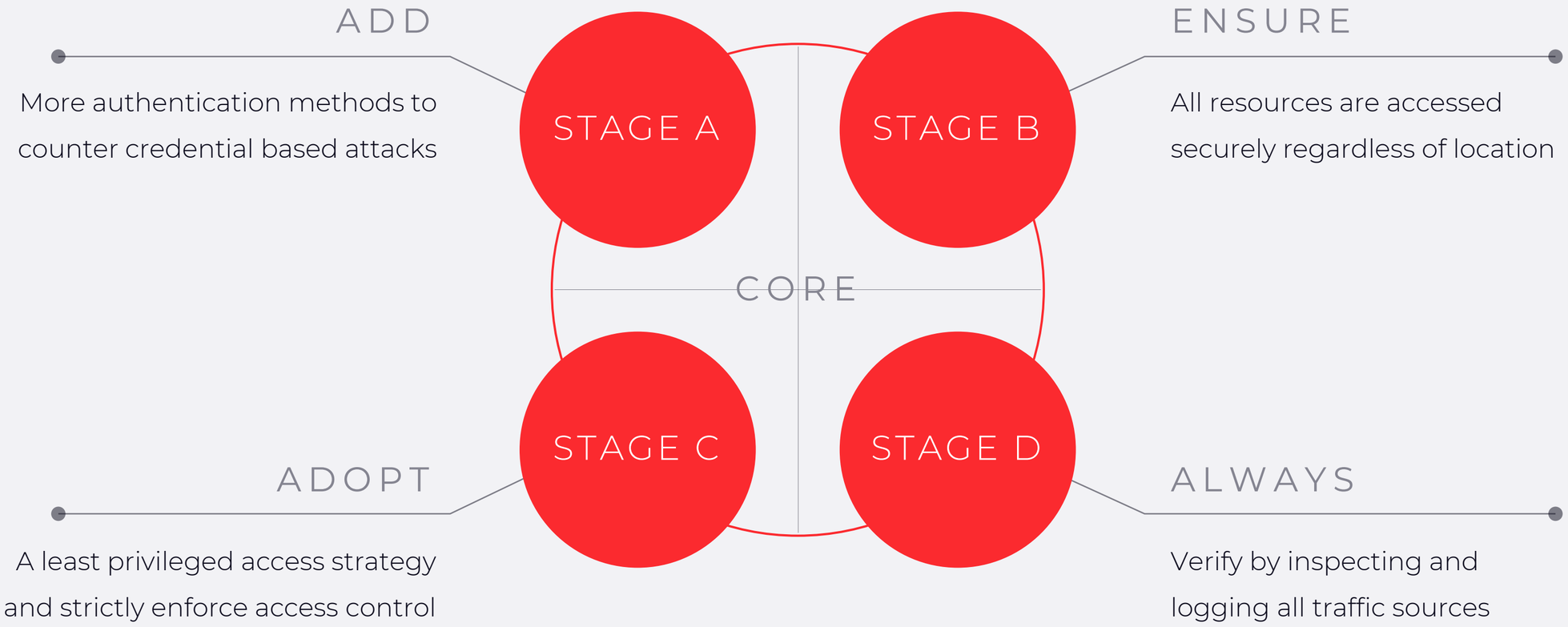
Patented Unknown File Containment

3

ARCHITECTURE & TECHNOLOGY

ZERO TRUST ARCHITECTURE EMBEDDED CORE

Dragon Enterprise delivers Zero Trust Architecture at its' core automatically not trusting anything the system faces and uses patented Unknown File Containment. Dragon Enterprise will run every single unknown file within a low overhead container and will only let them live after tested and verified within our Dynamic and Behavioral Malware Analysis System. Dragon Enterprise's Zero Trust Analysis system will run every single file within customer environment with our Static and Behavioral Analysis System and verdict every single file it faces. This system is the most complicated analysis engine in the World even backed by real human analysts.



COMODO PROPRIETARY ZERO TRUST METHODOLOGY

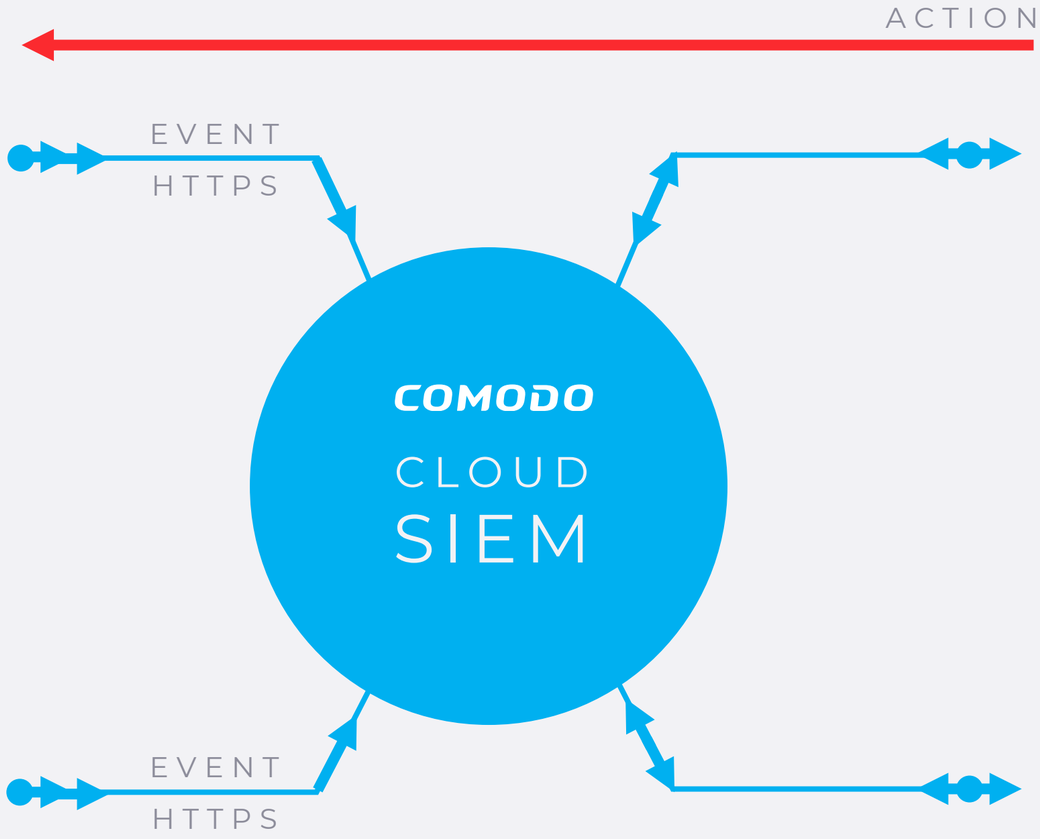
Dragon Enterprise's Threat Intelligence harnesses World's biggest database and updated every minute, will be accessible for Threat Hunting. Combining not only endpoint related data points Dragon uses network, email and DNS based data helping our customers to make better analysis.

CLOUD-NATIVE ENDPOINT SECURITY

Protect devices accessing data using auto-containment and DNS protection

NETWORK MONITORING AND DNS PROTECTION

Utilization of a network sensor to Packet Capture AD Logs, Proxy, etc....



MANAGED DETECTION AND RESPONSE

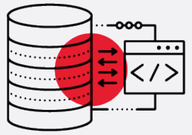
24 HR Monitoring and Correlations with SOC and Threat Intelligence

CLOUD APIs

Direct or indirect infrastructure and software services to users

DEFAULT DENY

File Executed Inside Network



Attackers create payloads to deliver to targeted or global campaign.

→

Blacklist Pass

Legacy AV doesn't detect malicious signature for newly created files.

→

Machine Learning

Machine Learning is not trained for newly bad indicators, bypassing statistical and behavioral models.

→

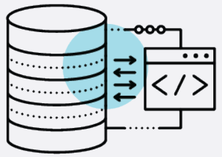
File Executed Infects Network

Endpoint is infected because all previous layers cannot identify relying on bad indicators.

As users tend to be the highest risk in every security system, Dragon Enterprise provides a unique User Behaviour Analysis and Detection feature, which enables our users to analyze single users based on their behavioral anomalies regardless of the number of machines they use, off-network or even offline usage.

DEFAULT ALLOW

File Executed Inside Network



→

File Identified as Unknown

→

Auto Containment Triggers Instantly

→

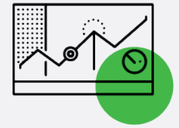
File Analyzed for Trusted Verdict

→

Known Good Verdict

→

File Safe on Endpoint



→

Known Bad Verdict

→

File Blocked from Endpoint

4

THE ZERO TRUST ARCHITECTURE

SECURITY ORCHESTRATED WITH INTELLIGENCE

Dragon Enterprise will extend endpoint security with its' network security components, adding additional layer of security and visibility for all your endpoints. Network component adds DNS layer protection, Secure Browser Isolation, Email On-Click Analysis, Email Containment and Encryption.

Dragon Enterprise Threat Intelligence harnesses World's biggest database and updated every minute, will be accessible for Threat Hunting. Combining not only endpoint related data points Dragon uses network, email and DNS based data helping our customers to make better analysis.

Set up granular access control policies to protect your micro perimeters

Implement a solution to prevent unverified devices from connecting to your network

A cloud-based SIEM can ingest and correlate large volumes of log data from a variety of tools and solutions

Must be able to monitor in real-time in order to verify by inspecting and logging all traffic sources

Depending on your in-house capabilities, these functions may best be outsourced

CUSTOMER OUTCOME

ENDPOINT ZERO TRUST

Stop attackers from using unknown files/scripts to move around your network and steal data.

NETWORK MONITORING AND PROTECTION

Stops malicious and unwanted traffic via DNS protections and monitoring network 24/7 for security incidents

CLOUD MONITORING

Cloud application monitoring helps customers identify threats from cloud-based applications that might have been compromised or attacked.

5

LET’S SEE THE PROOF WITH THE ALPHA DEMONSTRATION VIDEO