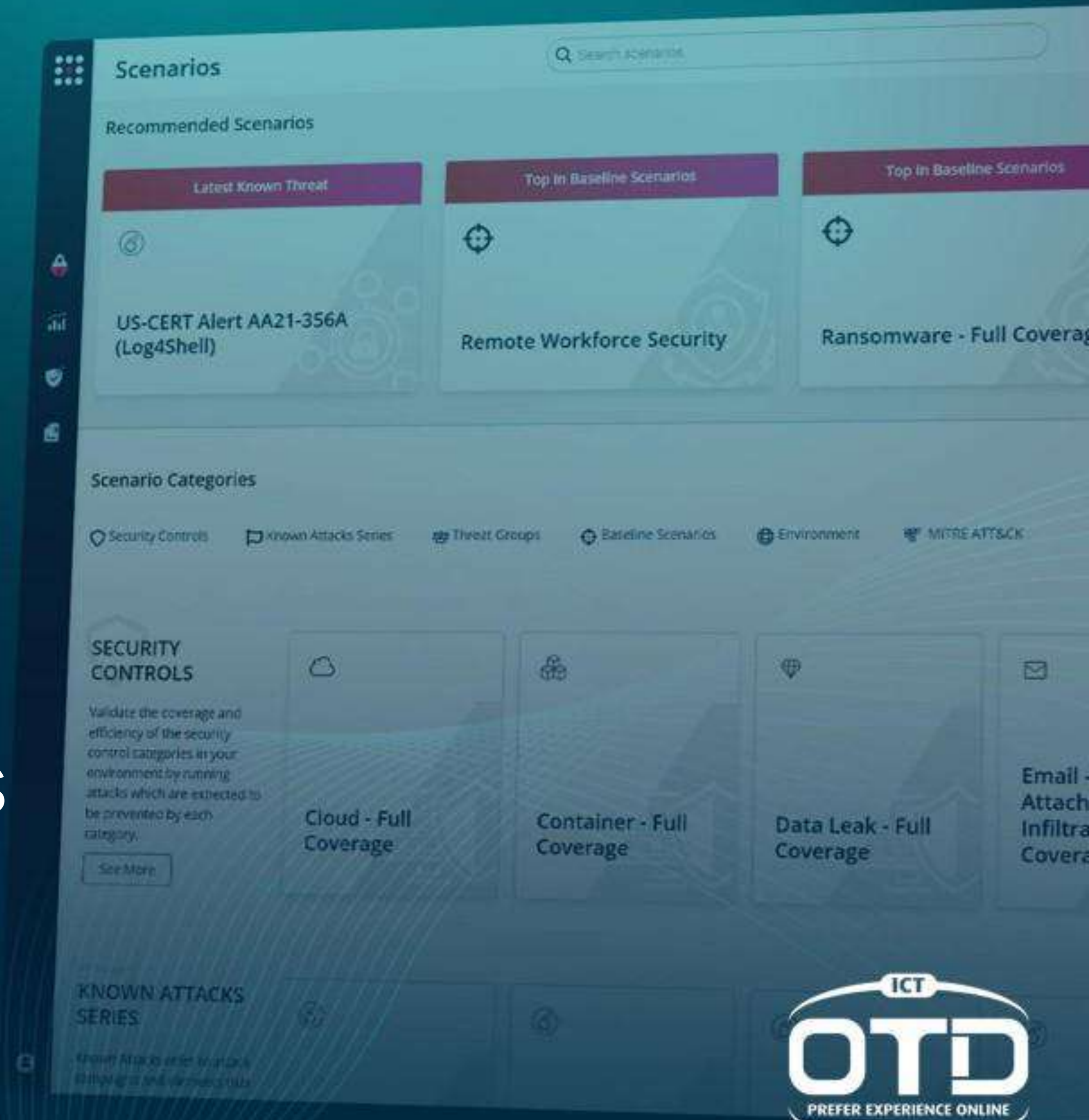
SafeBreach

Leveraging Cyber Attacks To Improve Your Defenses

2023



Validate the coverage and efficiency of the security control categories in your environment by running attacks which are expected to be prevented by each category.

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

Modern Enterprise Security is Getting **More Complicated**, not Less.

On average enterprises deploy **75** cybersecurity-related tools on their networks

95% of successful breaches are a result of a known attack

61% of organizations have difficulty prioritizing cyber risk reduction efforts.

Teams Need to Leverage the Attack to Improve Defenses

Test efficacy of security controls, prioritize future investments

Data-driven approach with reportable metrics

Find likely attacker paths through the organization to highly sensitive assets

Continuously improve the maturity of defenders

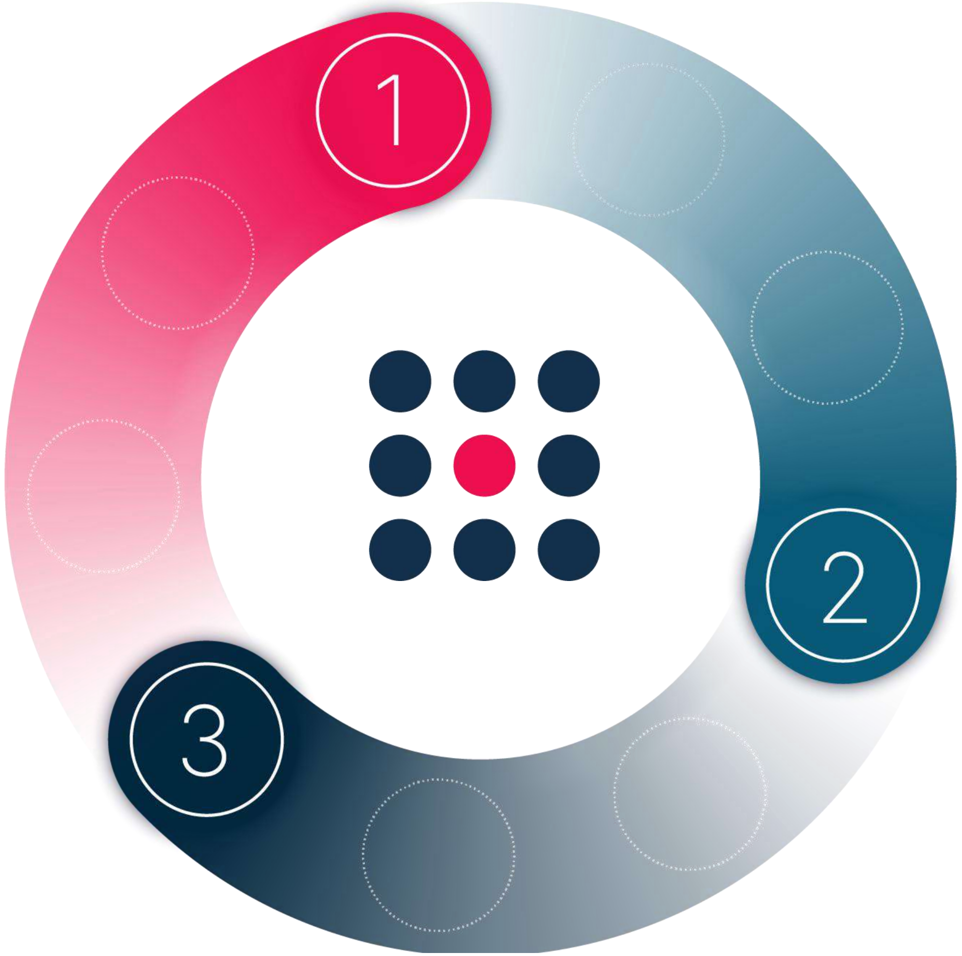
Attack. Remeditate. Report. Repeat.

Continuously Attack

Validate your security controls automatically and safely

Over **24K attack methods**

SLA - All US-CERT alert added within **24 hours**



Prioritize Results

Visualize the security posture

Integrate with vulnerability management platforms

Correlate with security controls to focus on the most impactful gaps

Drive Down Risk

Unique analytics and integrations to automate mitigation at scale

CISO dashboard to track progress and present board level KPIs

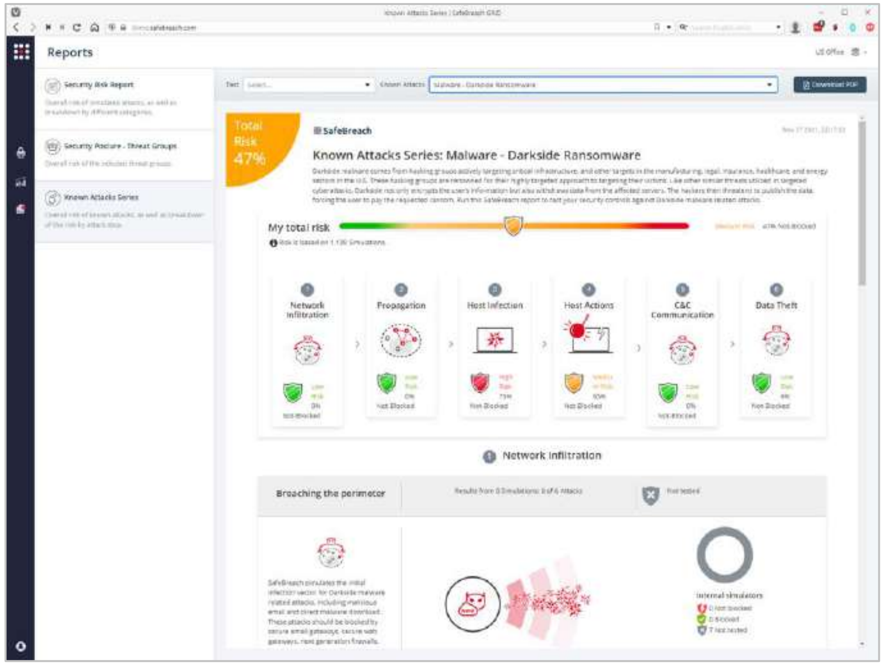
Attack with Purpose

Industry’s largest attack playbook, 24,000+ attack methods

Dedicated research team updates playbook within 24 hours of new certs and critical attacks

Create and/or customize attacks

Integrate with threat intelligence



Known Attacks Series: Malware - Darkside Ransomware

Threat Intelligence

Simulate attacks generated from IOCs of the latest threat

Alien Vault OTX

ThreatConnect

ThreatQ

Unit42

Continuously validate and optimize cloud and on-prem security control efficacy

Simulate attacks against your security controls to validate efficacy

Integrate with SIEM and security controls to correlate results and efficiently identify security gaps

Test the entire security ecosystem:

Cloud, container, network, web, endpoint, email, DLP

Security Controls

Automatically correlate simulated attacks with security events pulled from specific endpoint and network controls

- Tanium Threat Response
- SentinelOne
- Palo Alto Panorama
- Crowdstrike Falcon
- FireEye HX
- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint
- Carbon Black Defense
- Cisco AMP
- Cybereason
- Cisco Secure Email
- Cortex XDR
- BigQuery
- McAfee ePD
- Cisco Umbrella
- CylancePROTECT & CylanceOPTICS
- Amazon Web Services
- Microsoft Azure

SIEM

Automatically correlate simulated attacks with security events from multiple sources

- QRadar
- NetWitness Platform
- LogRhythm REST
- LogRhythm
- Google Chronicle
- Splunk
- Splunk v2 (REST)
- ArcSight Logger

Prioritize and automate remediation to efficiently mitigate risk

Actionable remediation steps to facilitate mitigation

Prioritize remediation by business risk

Integrate with SIEM, SOAR and Workflow management to automate remediation

Integrate with vulnerability management platforms to identify and prioritize exploitable vulnerabilities

Workflow and Automation

Receive notifications about system events and create incidents for automated remediation actions.

- ServiceNow
- Slack
- Jira Service Desk
- Email Notifications
- Syslog CEF (outbound)
- Cortex XSOAR
- Splunk Phantom

Vulnerability Management

Prioritize vulnerability by exploitability and impact based on SafeBreach simulations.

- Teneable Nessus
- Rapid7 Nexpose
- Qualys
- Tenable.io
- Tenable.sc

SafeBreach Dashboards

Report with Confidence

Schedule security posture metrics and other reports

Actionable MITRE framework & NIST mapping

Easily monitor trends over time

Report security visibility to management

SafeBreach Deployment

Simulators

Lightweight SW agent, deployed on **representative systems** internal and external

Assume attacker and target role in attacks to maintain safety

Windows, Linux, Mac, AWS, Azure, GCP and others

Management

SaaS, On premises or Disconnected options

Plans, orchestrates and aggregates results data into reports, visualizations and analytics

Integrates with Security Controls, SIEM, SOAR, VM, TI and Workflow platforms

Attack Playbook

Cloud service which holds thousands of updated attack methods

No software update required for new attacks, **attacks updated automatically**

Updated manually on disconnected management

Unleash the Power Of BAS

Security Control Validation

SC1	Organization Wide Security Posture
SC2	Posture Assessment per OU/BU
SC3	Environmental Drift Detection
SC4	MITRE ATT&CK Assessment
SC5	Endpoint Techniques Assessment
SC6	Email Security Assessment
SC7	Perimeter Validation
SC8	Data Leakage Assessment
SC9	Segmentation Control Validation
SC10	Compare Security Controls
SC11	SOC/IR Validation
SC12	M&A Risk Assessment

Threat Assessment

TA1	Imminent Threat Assessment
TA2	MITRE Threat Actor Assessment
TA3	TI Integrated Assessment

Cloud Security Assessment

CS1	Cloud Threats Assessment
CS2	CWPP Control Validation
CS3	Configuration Control Validation

Risk Based VM

VM1	Vulnerability Prioritization
VM2	Vulnerability Prioritization by Threat

WELLS FARGO
CNA
BARCLAYS
AIG
AUTODESK
T · · ·
American Airlines
TIAA
Microsoft
Morgan Stanley
at&t
SONY
CVSHealth.
REGENERON
Kellogg's
TIAA
Goldman Sachs
GILEAD
بنك أبوظبي الأول FAB First Abu Dhabi Bank
Southern Company
7 ELEVEN
Johnson&Johnson
UBS
ADT
PEPSICO
PayPal
DEPARTMENT OF STATE UNITED STATES OF AMERICA
teva
Deloitte.
experian.
WELLS FARGO
Kellogg's
REGENERON
Morgan Stanley
SONY
AUTODESK
Microsoft
CVSHealth
BARCLAYS
American Airlines
CNA
PayPal
Goldman Sachs

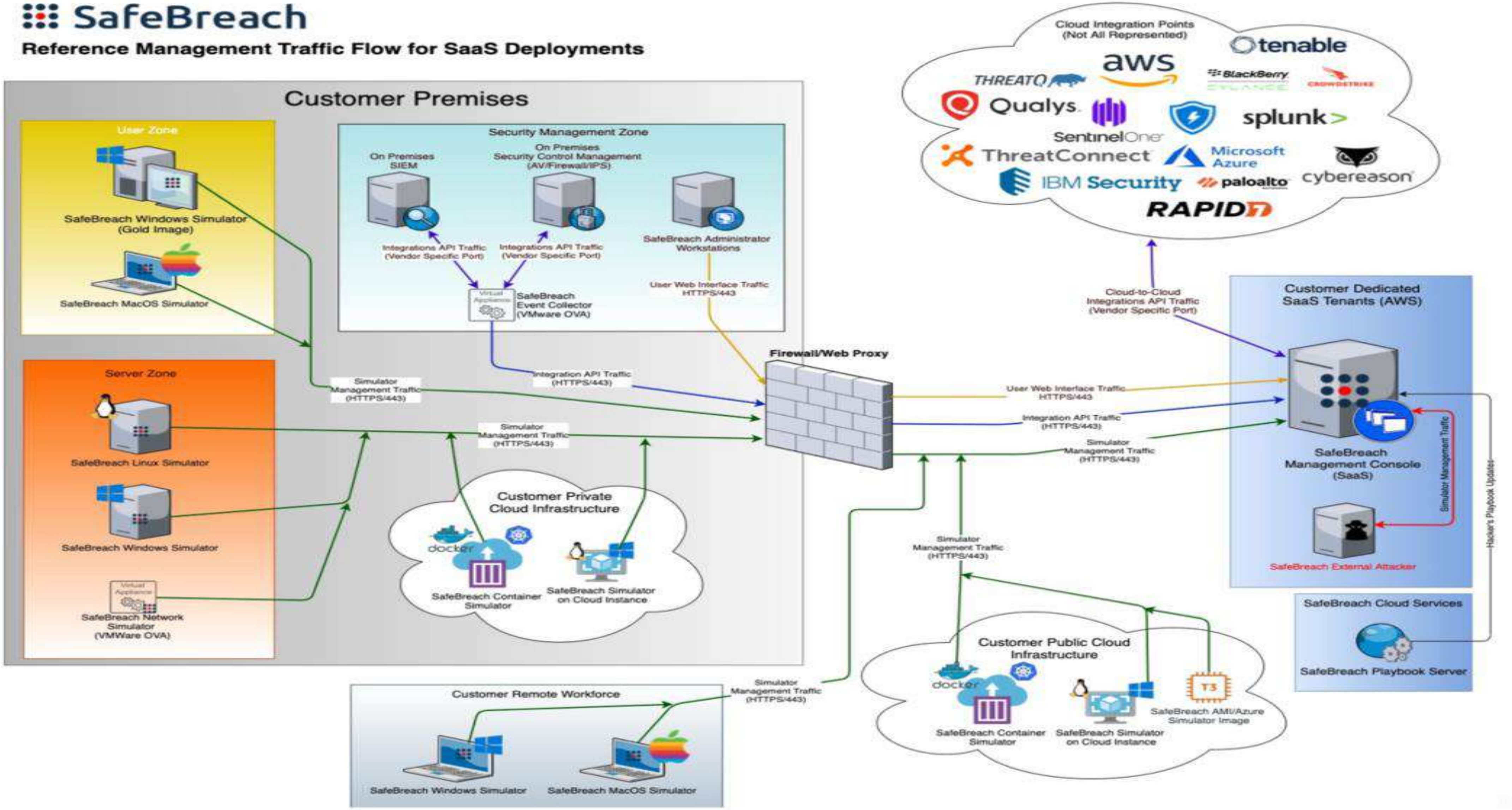
Trusted by Market Leaders

"A great value to us is that SafeBreach immediately updates the Hacker's Playbook with new attacks based on the US-Cert Alerts. In the case of attacks used against SolarWinds, this was exceptionally helpful to quickly test our controls, processes and our teams. To be able to report to the board that we launched attack simulations and the team was able to quickly discover the attack provided them with additional assurance that our team is alert and has the capability to detect and respond fast."

CISO, Top 10 U.S. Insurance Company

SafeBreach

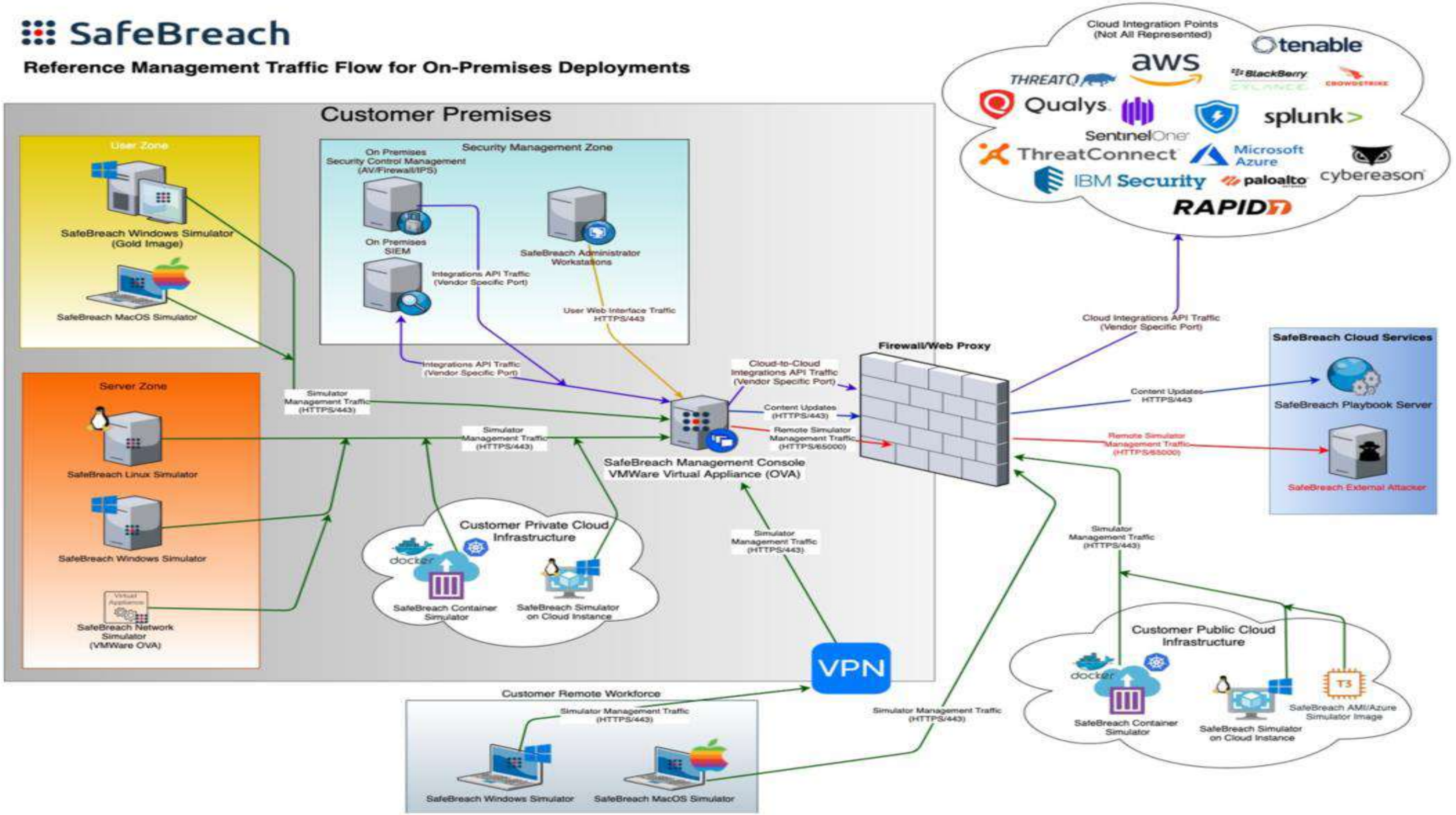
Reference Management Traffic Flow for SaaS Deployments



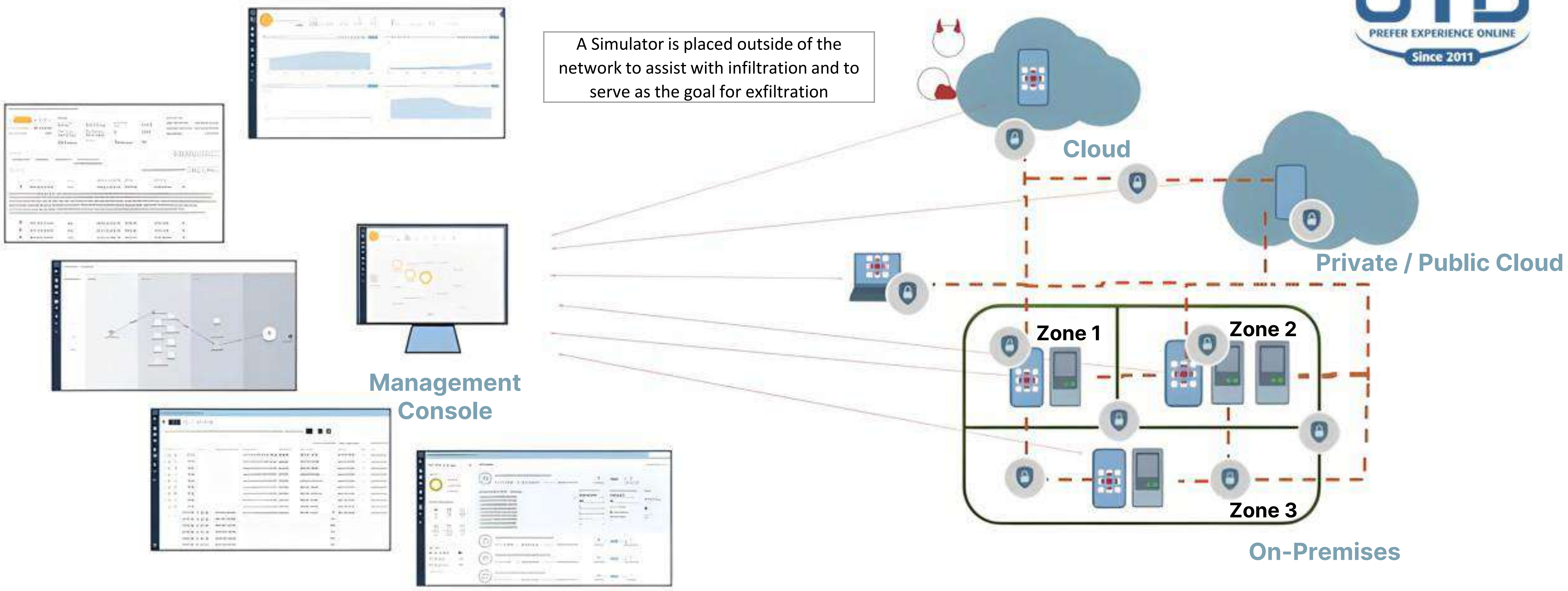
Customer Premises
User Zone
SafeBreach Windows Simulator (Gold Image)
SafeBreach MacOS Simulator
Server Zone
SafeBreach Linux Simulator
SafeBreach Windows Simulator
Virtual Appliance
SafeBreach Network Simulator (VMWare OVA)
Security Management Zone
On Premises SIEM
On Premises Security Control Management (AV/Firewall/IPS)
SafeBreach Administrator Workstations
Integrations API Traffic (Vendor Specific Port)
Integrations API Traffic (Vendor Specific Port)
Virtual Appliance
SafeBreach Event Collector (VMware OVA)
User Web Interface Traffic HTTPS/443
Integration API Traffic (HTTPS/443)
Simulator Management Traffic (HTTPS/443)
Simulator Management Traffic (HTTPS/443)
Customer Private Cloud Infrastructure
docker
SafeBreach Container Simulator
SafeBreach Simulator on Cloud Instance
Firewall/Web Proxy
Cloud Integration Points (Not All Represented)
aws
tenable
THREATQ
BlackBerry CYLANCE
CROWDSTRIKE
Qualys.
SentinelOne
splunk>
ThreatConnect
Microsoft Azure
cybereason
IBM Security
paloalto
RAPID7
Cloud-to-Cloud Integrations API Traffic (Vendor Specific Port)
Customer Dedicated SaaS Tenants (AWS)
User Web Interface Traffic HTTPS/443
Integration API Traffic (HTTPS/443)
Simulator Management Traffic (HTTPS/443)
SafeBreach Management Console (SaaS)
Simulator Management Traffic
Hacker's Playbook Updates
SafeBreach External Attacker
SafeBreach Cloud Services
SafeBreach Playbook Server
Simulator Management Traffic (HTTPS/443)
Customer Public Cloud Infrastructure
docker
SafeBreach Container Simulator
SafeBreach Simulator on Cloud Instance
T3
SafeBreach AMI/Azure Simulator Image
Simulator Management Traffic (HTTPS/443)
Customer Remote Workforce
SafeBreach Windows Simulator
SafeBreach MacOS Simulator

SafeBreach

Reference Management Traffic Flow for On-Premises Deployments



ICT OTD
PREFER EXPERIENCE ONLINE
Since 2011



A Simulator is placed outside of the network to assist with infiltration and to serve as the goal for exfiltration

The Management Console (MC) communicates with each Simulator independently and securely (Port 443) and instructs them to execute simulations. The Simulators communicate their results back to the MC, which then analyzes and generates the various dashboards, possible kill chain views, recommendations and reports.

This environment represents 3 segmented zones with various security controls such as AV. EDR. Proxy, Secure Web Gateway, NexGen firewall, IPS. Sandbox, etc.

Legend

SafeBreach Simulator

Security Control

Represantative Systems

Remote Usee w/Simulator

Communacition Path for MC to Simulators

Potential Simulation Paths

Network Segmentation

Defined Exfiltration Goal

Defined Exfiltration Goal

Additional Slides

CUSTOMER CASE STUDY

Top 3 US Insurer

Challenge

Assess cyber risk and improve posture across OUs and non integrated entities

Solution

SafeBreach Deployed across OUs and NIEs and continuously tests across infiltration, host level, lateral movement and exfiltration

SafeBreach Dashboards are reported quarterly to C-level and BoD

Benefit / ROI

Ability to track program progress based on a uniform set of KPIs

Ability in show posture improvement over time

Ability to identify and remediate thousands of gaps

CUSTOMER CASE STUDY

Top 3 US FIS

Challenge

Asses segmentation controls across most valuable segments

Assess resilience to imminent threats in a short time

Solution

SafeBreach deployed across valuable segments, integrated to SIEM, and continuously validates segmentation

SafeBreach SLA utilized to test US-CERT security posture

Benefit / ROI

Reduction of attack surface from > 80% to < 5% on network controls

Ability to report imminent threat resilience and mitigation plan in days

CUSTOMER CASE STUDY

PayPal

Challenge

Asses M&A cyber risk early in the process to identify gaps and plan merger

Solution

M&A team deploys and runs SafeBreach baseline test in every DD process and evaluates cyber posture within days

Benefit / ROI

Assess acquired risk on time to make an impact

Assess associated merger budget and impact

Efficient and fast assessment process

Differentiation: Future Proofing Your Business

Automated Mitigation

Provides actionable data for automated mitigation with your orchestration at scale.

CORTEX XSOAR BY PALO ALTO NETWORKS

splunk> phantom

Enterprise Ready

Scalable & Secure

Ease of deployment

Automated & Low Touch

Highest Coverage

Following the entire attack-chain with Cloud based, on-prem or air gapped deployment.

>24K attacks, the largest playbook in the market.

SLA – new threats added within 24 hours.

Windows

aws

docker

macOS

Azure

Google Cloud

Open Platform

IBM Radar

CROWDSTRIKE

ThreatConnect

Microsoft

tenable

RSA

RAPID7

CYLANCE

SafeBreach

paloalto NETWORKS

SentinelOne

cisco

now

Cb CARBON BLACK

Qualys.

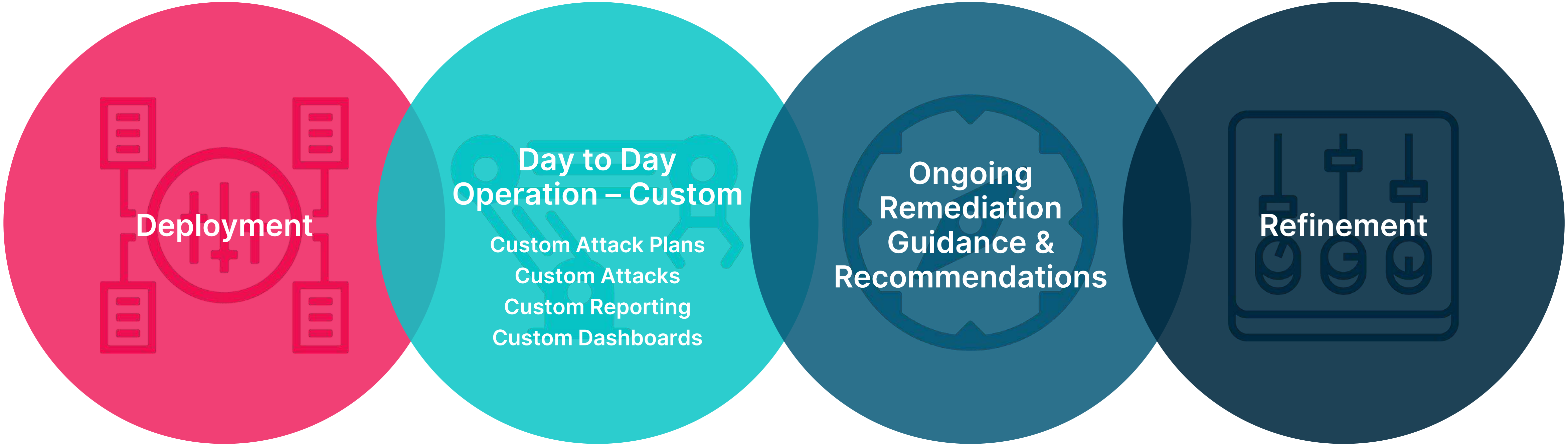
OVO

McAfee

splunk> phantom

Switch from Defense to Offense with SafeBreach-as-a-Service: The Most Complete BAS Solution

All the benefits of SafeBreach, without managing the platform



Deployment

Day to Day Operation – Custom

Custom Attack Plans
Custom Attacks
Custom Reporting
Custom Dashboards

Ongoing Remediation Guidance & Recommendations

Refinement

Allowing you to focus on, strategy, remediation, mitigation and standards creation, and strengthening your security posture

Unlock the full kill-chain through agentless web application security validation

SafeBreach for Web Application Security

Full kill-chain validation

Coverage includes OWASP® Foundation’s top ten security risks

A contextualized view of web application security posture

Fast and easy to deploy

Actionable ROI reporting on your WAF

SafeBreach

Thank You

Your Name
Email
Phone