



# SafeBreach

IT OT

Red - Teaming

CYBER ATTACK B A S SOLUTION

FOR ICS AND CRITICAL INFRASTRUCTURE

"TAKE ADVANTAGE OF ATTACKS"  
To Improve Your Defense

OTD BİLİŞİM

GLOBAL VAD

ICT  
OTD  
PREFER EXPERIENCE ONLINE  
Since 2011

# Modern Corporate Security is becoming not Less Complex, **but More** Complex.

On average,  
organizations use **75** tools  
related to cybersecurity  
in their networks

**95%** of successful  
breaches are the result  
of known attacks

**61%** of organizations  
have difficulty  
prioritizing cyber risk  
mitigation efforts.



# Strengthening the Defense Systems of IT and OT Teams



Testing the effectiveness of security controls, prioritizing future investments



Data-driven approach with reportable metrics



Finding possible paths to high-sensitivity assets that attackers will follow across the organization



Continuous improvement of the experience of defenders

## Did You Know...

94%

of organizations recently surveyed experienced an OT/IoT security event in the prior 12 months

80%

of industrial organizations only run an ICS security assessment once/year or less

3

Engineering workstations, HMIs, and operations servers (all running a commercial OS such as Windows or Linux) are the top 3 control system components at greatest risk for compromise in an OT attack



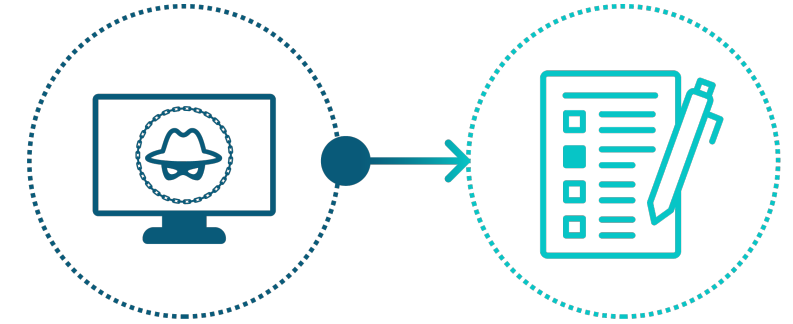


# Many OT Attacks Begin as IT Intrusions

Many attacks begin with ingress through the IT network.

Once inside, adversaries conduct reconnaissance to gain credentials and identifying vulnerable paths to the OT network.

The attacker will then leverage previously compromised systems, credentials, or applications to access systems in higher security zones—such as the OT DMZ.



## Information Sources

System or process documentation

Keystroke logging

Screen monitoring

Network management consoles

Port scanning (active and passive)

## Target Information

High level network architecture diagrams

Hostnames and IP addresses

Communication paths

Username and credentials



# The Perfect Storm

## ICS Insecure by Design



Flat networks

Weak authentication

No encryption

Insecure ICS protocols

Difficult/rare patching

## Increasingly Connected



Integrated IT/OT networks

Shop floor to top floor KPIs

Data analytics programs

Supply chain integration

Vendor remote access

## Active Threat Landscape



Nation-State attacks target ICS

Repeated warnings from DHS/FBI, GCHQ, Others

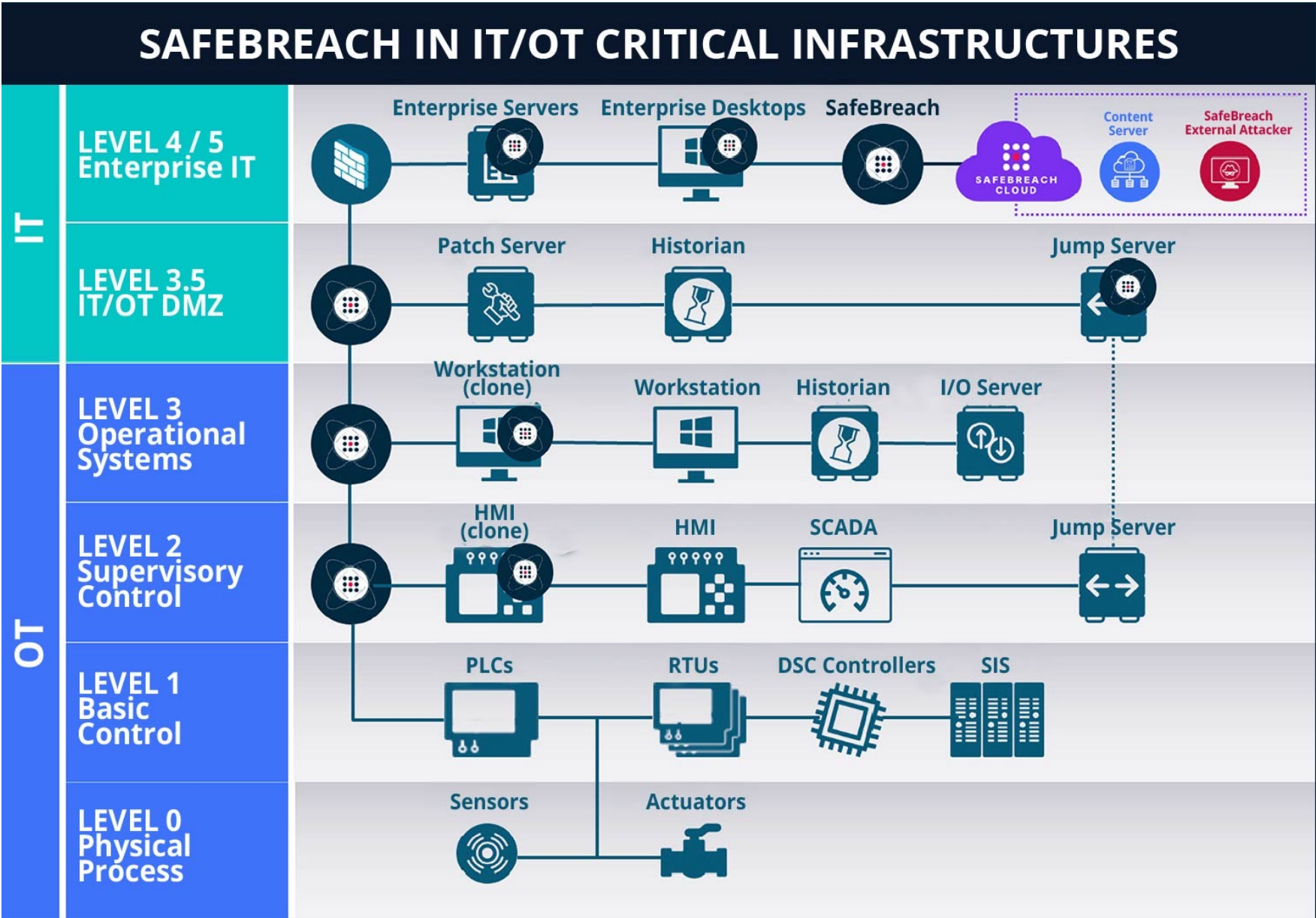
Billions in collateral damage from ransomware attacks

Advanced hacking knowledge not required to access vulnerable systems

**POOR VISIBILITY INTO ICS NETWORK**



# Purdue Architecture



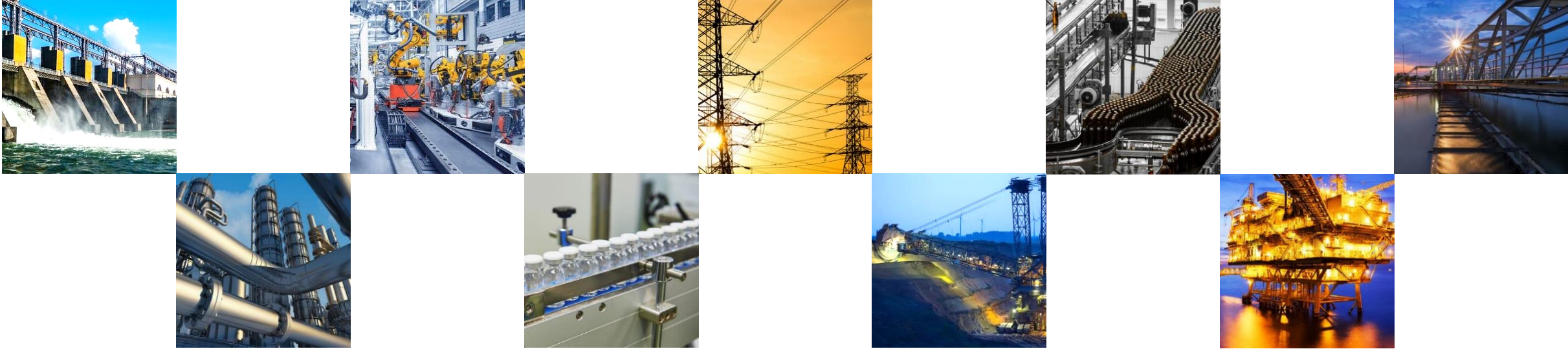


# BAS and the IT/OT Environment

How does this fit in your security program?







## Better Protection & Visibility From the Shop Floor to the Top Floor

Protect Production Uptime

Unify IT/OT Security Testing, Remediation & Reporting

Confidently Support OT Digital Transformation

Control Supply Chain Security Exposure

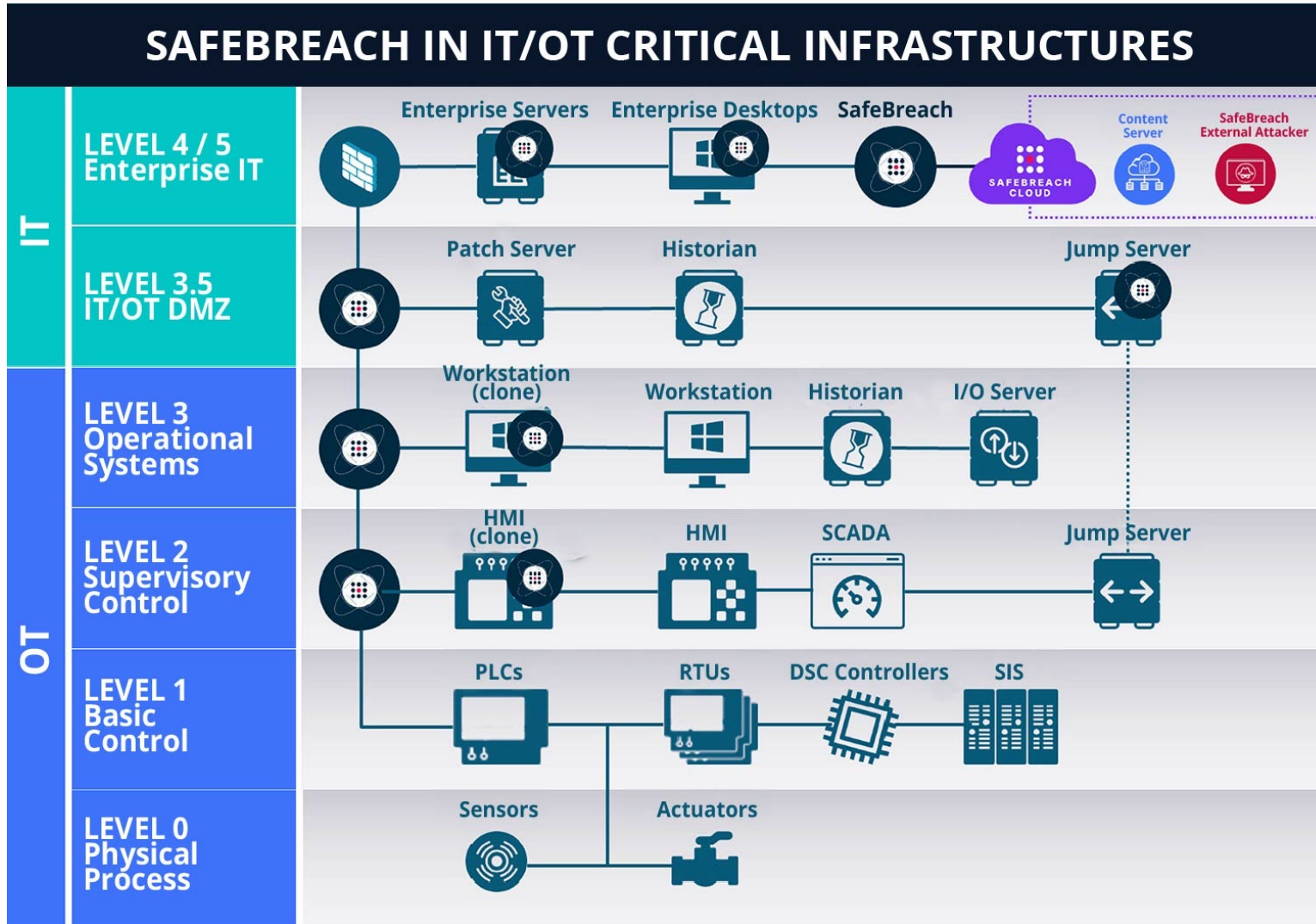
Increase Cooperation Between IT & OT Stakeholders

“SafeBreach enabled my team to identify gaps that put the OT network at risk and work more collaboratively with the team at the plant on a remediation plan.”

**SoC Director**  
**Power & Energy Provider**



# SafeBreach in an IT/OT Environment



SafeBreach performs both Network and Host level Attack Simulations on Levels 4 and 3.5

Validate Host Level Security Control (Dsktp, Srvr, Remote)

Validate Firewall Detection Rules

Verify Firewall ACL Rules

Verify Logging at SIEM and Security Control Level

SafeBreach performs attack simulations on Network between Levels 3.5 and 2 and cloned Level 3 hosts

Validate Firewall Detection Rules (Workstation clone)

Validate Firewall Detection Rules

Verify Firewall ACL Rules

Verify Logging at SIEM and Security Control Level

SafeBreach performs attack simulations on Network between Levels 2 and 3+ and cloned Level 3 hosts

Validate Host Level Security Control (HMI clone)

Validate Firewall Detection Rules

Verify Firewall ACL Rules

Verify Logging at SIEM and Security Control Level

Note: All simulations take place between SafeBreach simulators (icons). No simulations occur between non-SafeBreach systems.

Note: Will utilize any proxies in environment for testing.



## SafeBreach Sheds Light on 99% of Your OT Exposure

---

99% of **compromised systems** will be computer workstations and servers (HMIs)

---

99% of **intrusion dwell time** happens in commercial off-the-shelf computer equipment before any Purdue level 0-1 devices are impacted

---

99% of **malware** will be designed for those computer workstations and servers

---

99% of **detection opportunities** will be for activity connected to those computer workstations and servers

---

99% of **forensics** will be performed on those computer workstations and servers

---



# SafeBreach Helps Jumpstart Your IT/OT Security Integration

## Baseline

ASSESS, PLAN, & ORGANIZE

**GOAL :**

Identify key OT assets, evaluate architecture, & prepare response plans for incidents

**Key Tasks & Milestones:**

Conduct an architecture review with crown jewel analysis [attack simulation and analysis]

Complete an incident response plan [continuous security validation and BAS plan]

1-3 MONTHS

## Operationalize

OT RISK CONTROLS

**GOAL :**

OT security program with the resources and skill to detect and respond to incidents

**Key Tasks & Milestones:**

Implement asset/networking monitoring for sites with crown jewel OT assets

Operationalize admin, asset validation, threat detection and investigation

Implement mitigation processes for critical OT vulnerabilities

3-12 MONTHS

## Optimize

MATURE OT RISK REDUCTION PROGRAM

**GOAL :**

Proactive risk reduction and program improvement

**Key Tasks & Milestones:**

Expand asset/network monitoring at high and medium risk OT sites

Validate defense controls - inventory, topology, traffic monitoring, vulnerabilities

Active vulnerability management and threat hunting programs

Integrate OT threat intelligence into security operations processes

12-24 MONTHS (+ONGOING)





# Attack. Solution. Reporting. Repetition.

## Continuous Attack

Validates your security controls automatically and securely

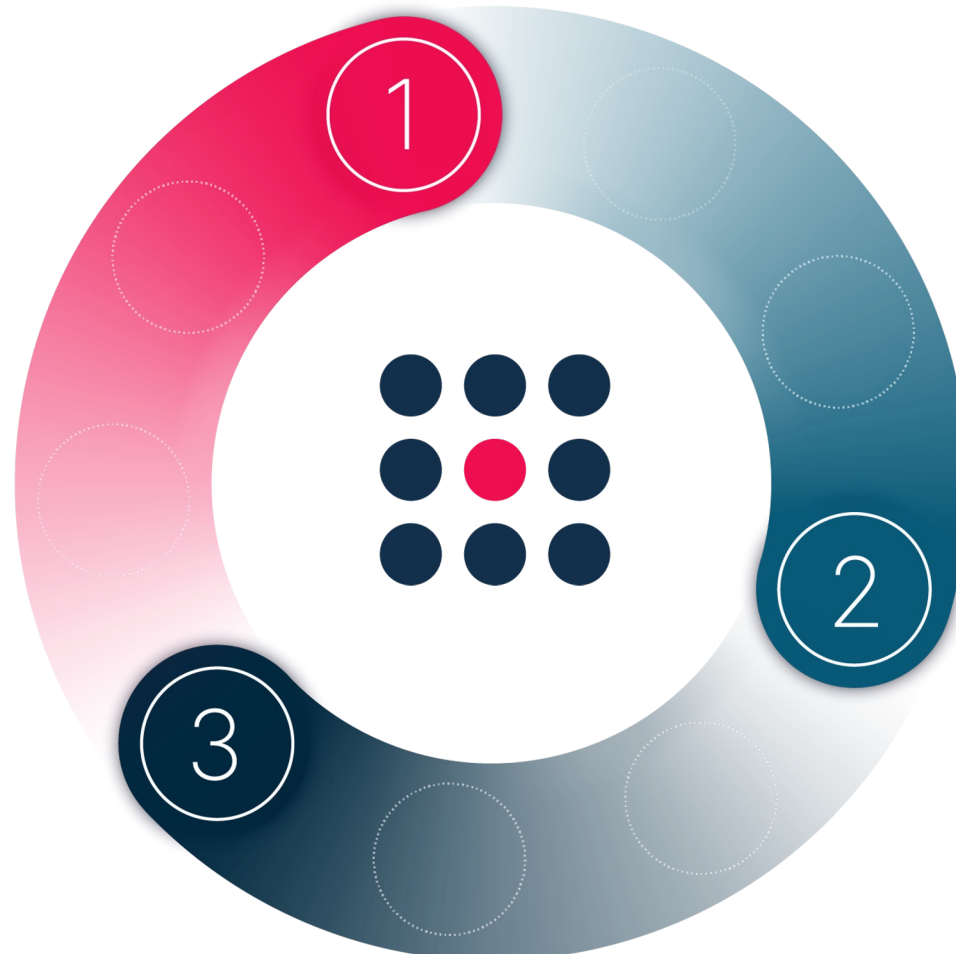
More than **30K** attack methods

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

## Drive Down Risk

Unique analytics and integrations to automate mitigation on a large scale

CISO dashboard to monitor progress and present dashboard-level KPIs



## Prioritization of results

Visualizes security posture

Integrates with vulnerability management platforms

Engages with security controls to focus on the most critical gaps



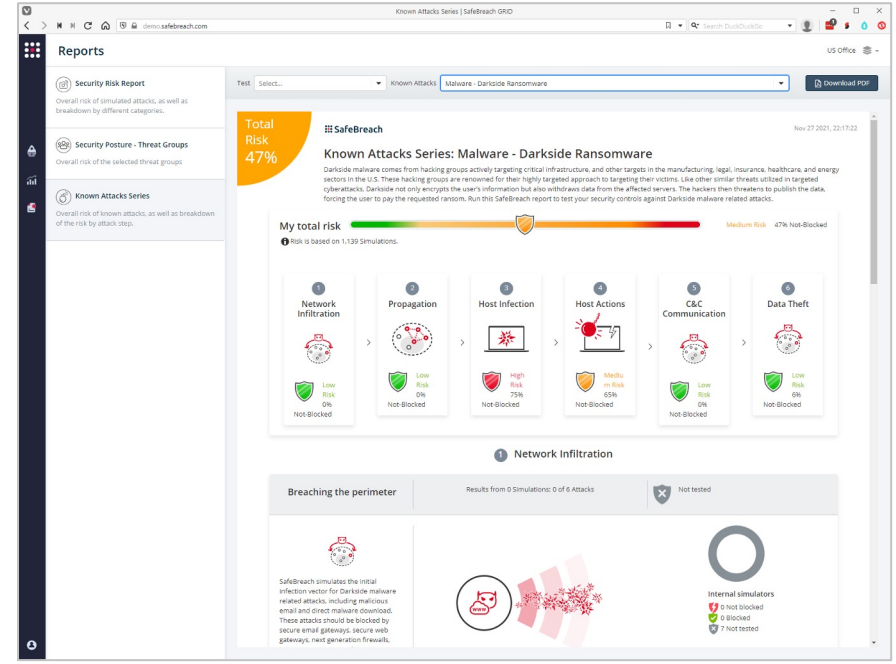
# Deliberate Attack

The industry's largest offensive tactics book (playbook), more than **30,000+** attack methods

Dedicated research team updates the playbook within **24** hours after new certifications and critical attacks

Creates and/or customizes attacks

Integrates with threat intelligence



## Threat Intelligence

Simulates attacks generated from IOCs of the latest threat

 Alien Vault OTX	 ThreatConnect	 ThreatQ	 Unit42
-------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------



# Continuously validates and optimizes cloud and onsite security control effectiveness



















Simulates attacks against your security controls to verify effectiveness

Integrates with SIEM and security controls to correlate results and efficiently identify vulnerabilities

Tests the entire security ecosystem:  
Cloud, carrier, network, web, endpoint, e-mail, DLP

## Security Checks

Automatically correlates simulated attacks with security events received from specific endpoints and network controls

 Palo Alto Panorama	 Crownstrike Falcon	 FireEye HX	 Tanium Threat Response	 SentinelOne	 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 simulated attacks with security events from multicorrelatestiple sources

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



# SIEM

Automatically correlate simulated attacks with security events from multiple sources.



ArcSight  
Logger



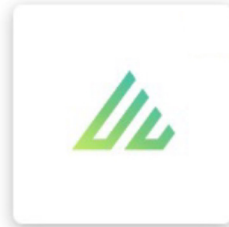
Microsoft  
Sentinel



Devo



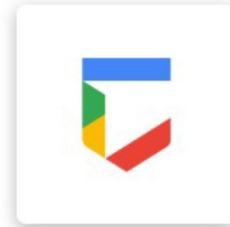
ElasticSearch



Exabeam v1  
(user-password  
authentication)



FortiSIEM



Google  
Chronicle



GuardDuty  
(SDK)



LogRhythm  
SOAP  
(deprecated)



LogRhythm



NetWitness  
Platform



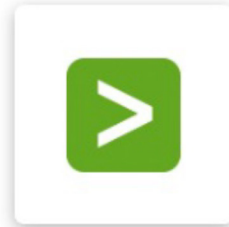
QRadar



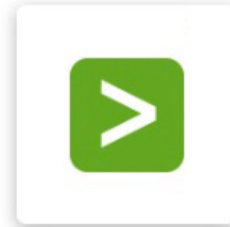
InsightIDR



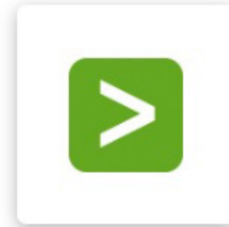
Securonix



Splunk SDK  
(deprecated)



Splunk



Splunk  
SOAR



Sumo  
Logic





# Safety Checks

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



Carbon Black Defense



CheckPoint NGFW



Cisco AMP



Cisco Secure Email



Cisco Umbrella



Cortex™ XDR



CrowdStrike Falcon



Cybereason



CylancePROTECT & OPTICS



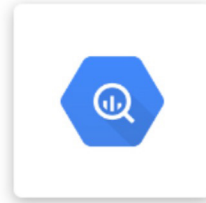
FireEye HX



Firepower



FortiGate NGFW



BigQuery



Trellix ePO



Microsoft Defender for Endpoint



Netskope SASE



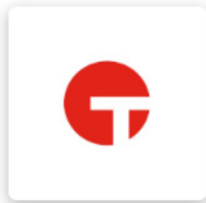
Microsoft Defender for Office 365



Palo Alto Panorama



SentinelOne



Tanium Threat Response



Trend Micro XDR



Windows Events



# Prioritizes and automates improvement to efficiently reduce risk

Actionable improvement steps to facilitate mitigation

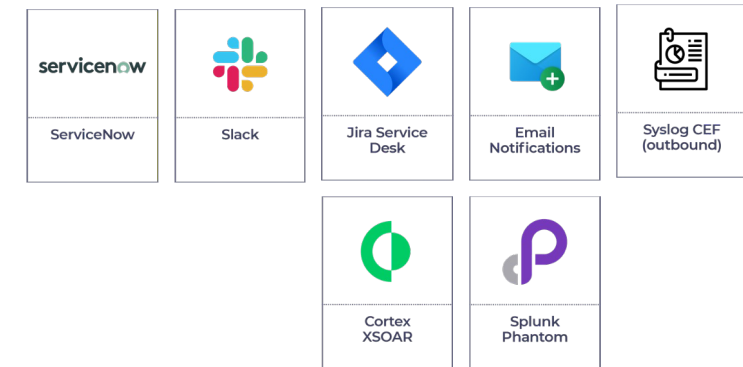
Prioritizes improvement according to business risk

Integrates with SIEM, SOAR and Workflow management to automate remediation

Integrates with vulnerability management platforms to identify and prioritize exploitable vulnerabilities

## Workflow and Automation

Receives notifications about system events and generates events for automatic remediation actions



## Vulnerability Management

Prioritizes vulnerability by exploitability and impact based on SafeBreach simulations



## Vulnerability Management

Prioritize vulnerabilities by exploitability and impact based on SafeBreach simulations.



Tenable  
Nessus



Qualys



Rapid7  
Nexpose



Tenable.io



Tenable.sc

## Threat Intelligence

Simulate attacks created from IOCs of the latest threats.



AlienVault  
OTX



Anomali



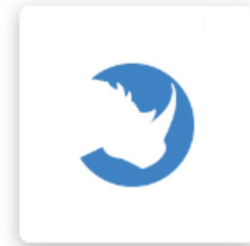
Falcon  
Intelligence



Recorded  
Future



ThreatConnect



ThreatQ



Unit42

# Differentiation: Future-proofing Your Business

## Automatic Reduction

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



## Highest Coverage

Track the entire attack chain with cloud-based, on-premises or air-gapped deployment.

Largest PlayBook on the market with >30K attacks.

SLA - New threats added within 24 hours.



## Enterprise Ready



Scalable & Secure



Placement Ease



Auto and Low Touch

## Open Platform





## **SafeBreach Panels**

# Secure Reporting

**Schedules security posture measurements and other reports**

**Actionable MITER framework and NIST mapping**

**Easily tracks trends over time**

**Reports security visibility to management**

# SafeBreach Deployment



## Simulators

---

Lightweight software agent deployed on internal and external representative systems

---

Play the role of attacker and target in attacks to ensure security

---

Windows, Linux, Mac, AWS, Azure, GCP etc.



## Administration

---

SaaS, Onsite or Standalone options

---

Reports results data, plans, organizes and compiles it into visualizations and analyses

---

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



## Attack Playbook

---

Cloud service hosting thousands of updated attack methods

---

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

---

Manually updated in disconnected administration

# Use the Power of BAS

## Security Control Verification

SC1	Organization-wide Security Posture
SC2	Posture Assessment per OU/BU
SC3	Environmental Drift Detection
SC4	ITRE ATT&CK Assessment
SC5	Endpoint Techniques Assessment
SC6	Email Security Assessment
SC7	Environmental Verification
SC8	Data Leak Assessment
SC9	Segmentation Control Verification
SC10	Comparison of Security Controls
SC11	SOC/IR Verification
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 Threat Assessment
CS2	CWPP Control Verification
CS3	Configuration Control Verification

## Risk Based VM

VM1	Security Gap Prioritization
VM2	Threat Based Security Gap Prioritization



# Companies that trust us...

## FINANCIAL SERVICES

WELLS FARGO BARCLAYS INDEPENDENT FINANCIAL™  
 AIG MERCHANTRADE Wafra BREWIN DOLPHIN  
 L&T Finance BANK OF CANADA / BANQUE DU CANADA Jack Henry & ASSOCIATES INC.  
 Goldman Sachs PayPal MAX FINANCIAL SERVICES greendot bank  
 Morgan Stanley BRINKS GRUPO FINANCIERO BANORTE  
 TIAA UBS FAB First Abu Dhabi Bank SCB ไทยพาณิชย์  
 experian Jefferies Allica Bank INVESTNET  
 shva The payments arena DAVIVIENDA ISRAEL DISCOUNT BANK BanCERT Comunidad Bancaria de Ciberseguridad  
 Cboe KB Kookmin Bank BANCO INDUSTRIAL  
 bank hapoalim AXIS BANK RAYMOND JAMES

## HEALTHCARE

Cleveland Clinic MARKEN  
 SHARP CVS Health  
 teva children'shealth?  
 CovenantHealth GEHA

## PHARMACEUTICALS & BIOTECHNOLOGY

Hovione Johnson & Johnson  
 GILEAD MCKESSON  
 REGENERON insmid  
 ICON HilltopHoldings

## PRODUCTION

MARS BOSCH Cipla  
 MASCO Titan. Olin  
 Wabtec CORPORATION GE MODINE Always Innovating. Always Improving.  
 ACME BRICK IAI TESLA ArcelorMittal

## INSURANCE

JACKSON TRAVELERS  
 PRUDENTIAL BlueCross BlueShield  
 CNA AON SOMPO Digital Lab GENERALI  
 cigna healthcare Marsh McLennan





# Companies that trust us...

## TECHNOLOGY



## FOOD & BEVERAGES



## CONSULTING



## LEGAL



## SERVICES



## EDUCATION



## VEHICLES



## TRANSPORTATION



## COMMUNICATION



## ENTERTAINMENT



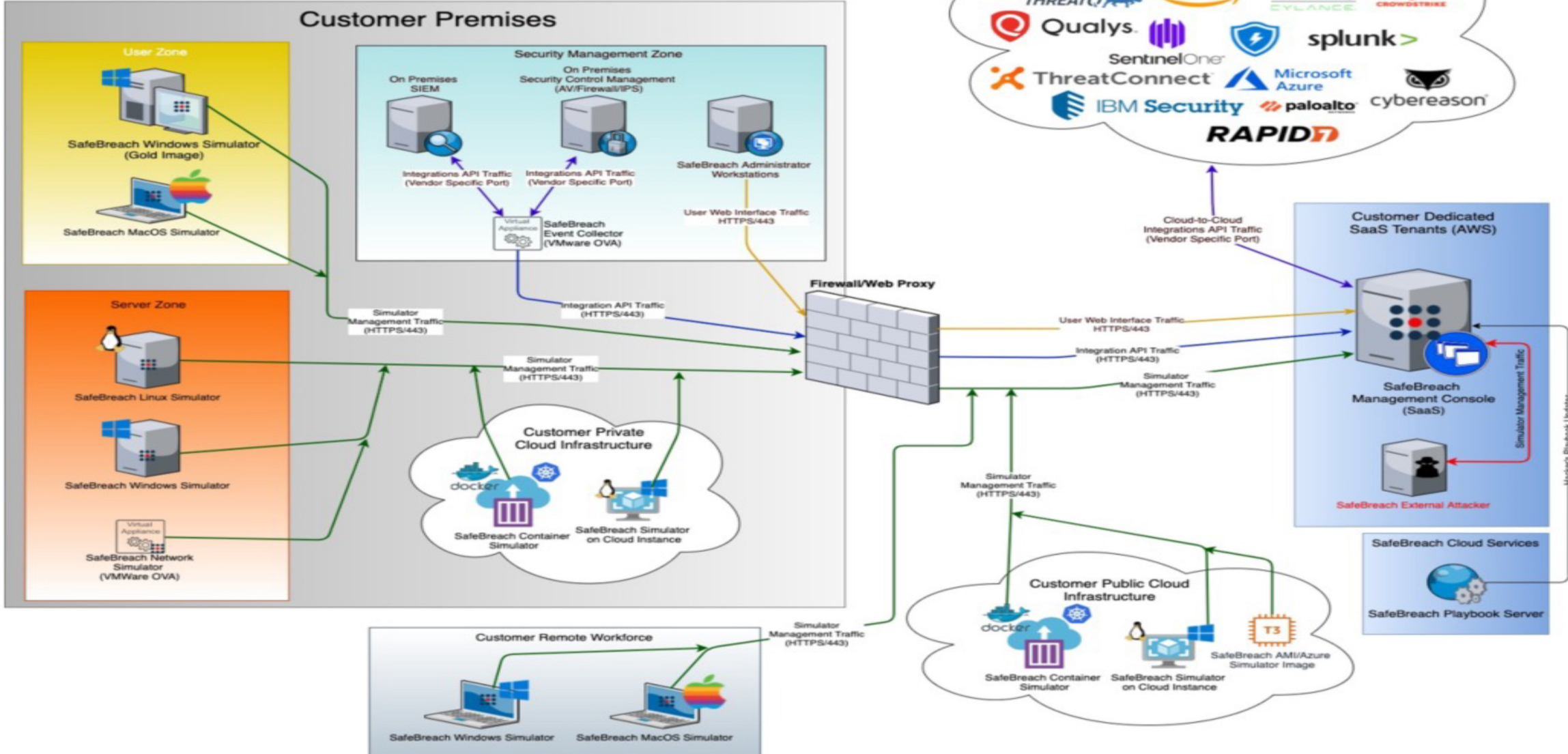
## RETAIL



## GOVERNMENT

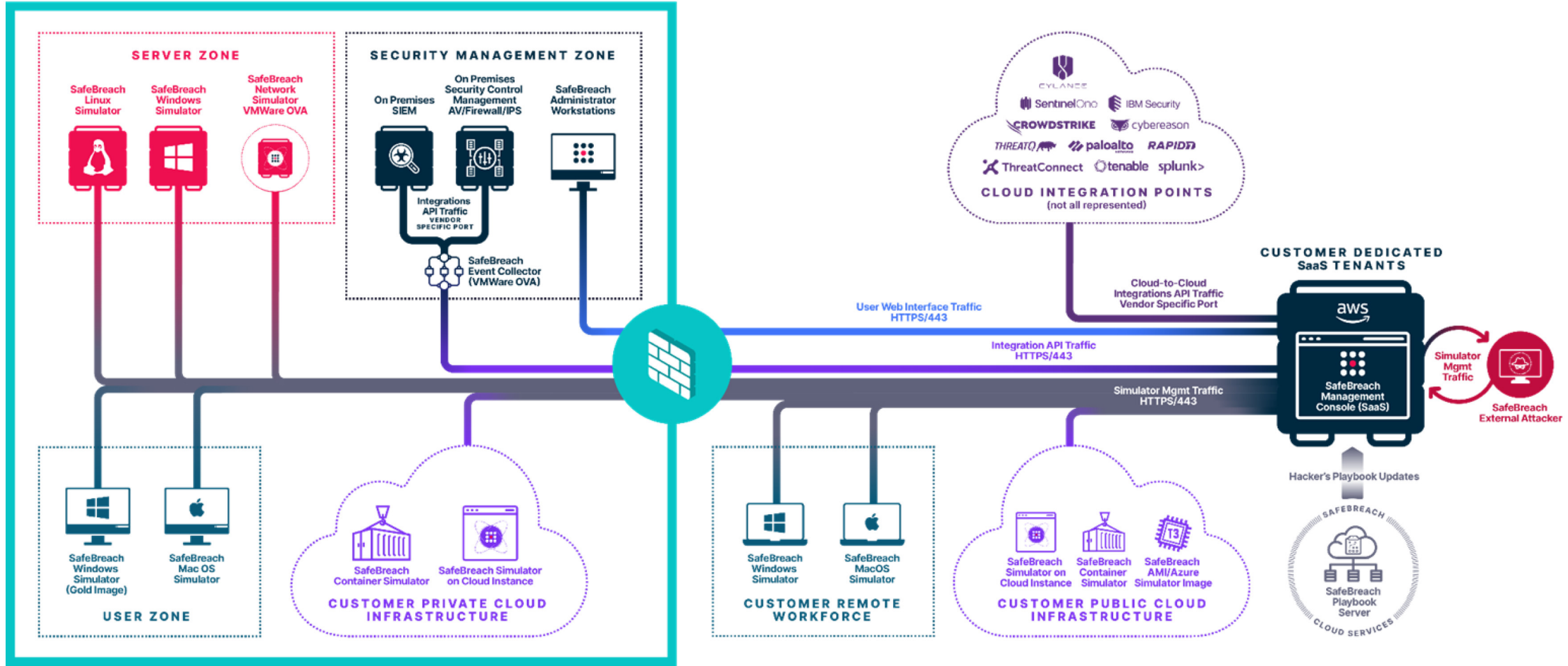


# Reference Management Traffic Flow for SaaS Deployments



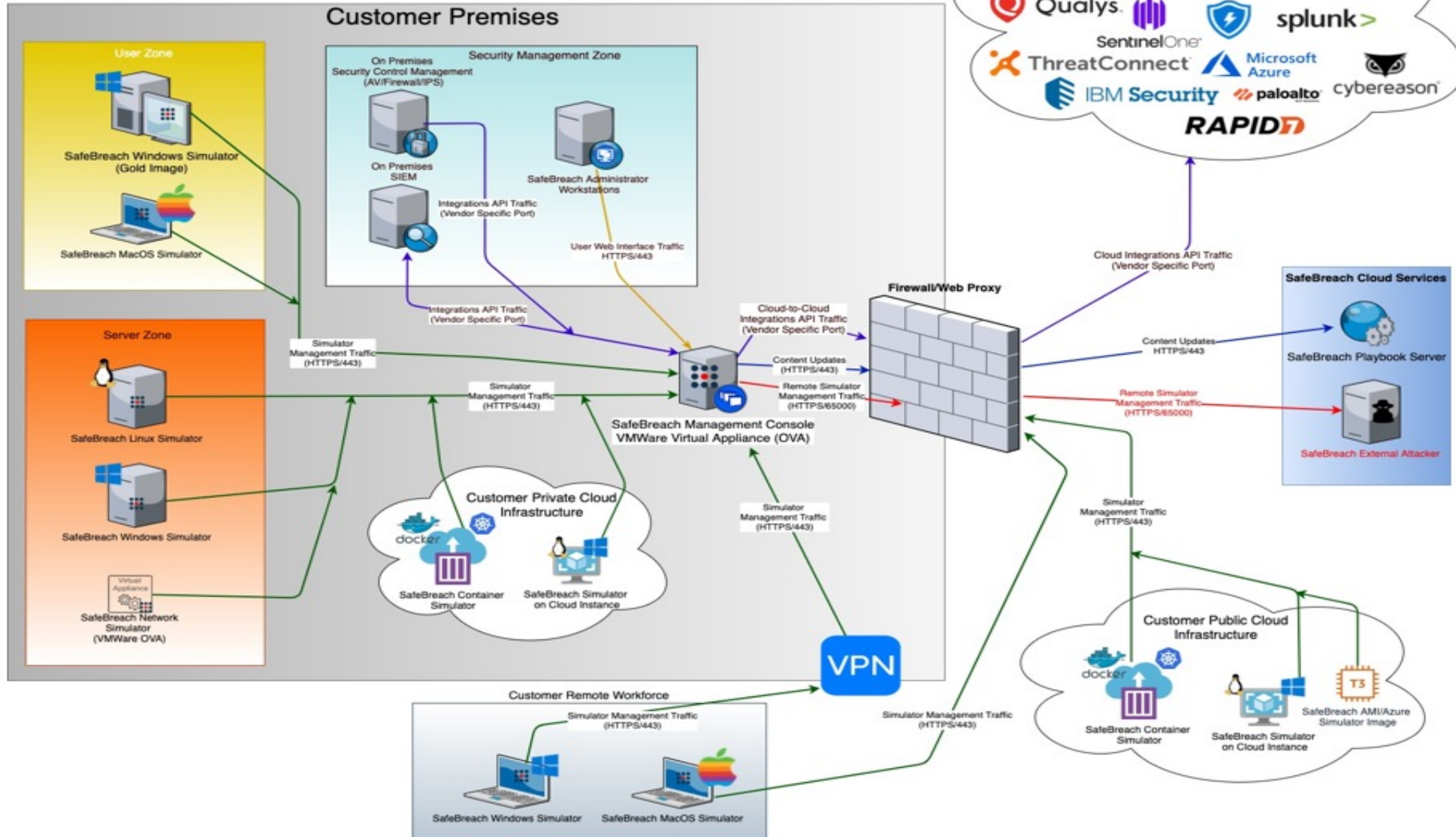
# Reference Management Traffic Flow for SaaS Deployments

## Customer Premises

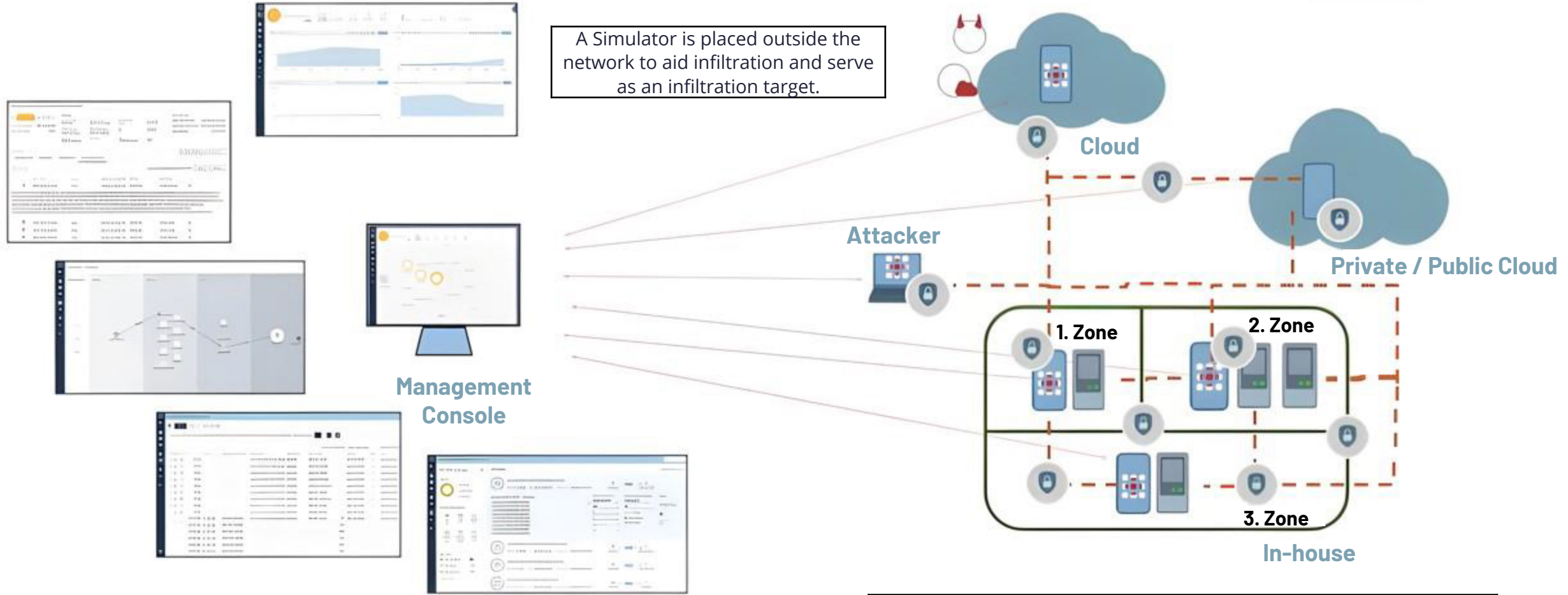




# Reference Management Traffic Flow for On Prem Deployments







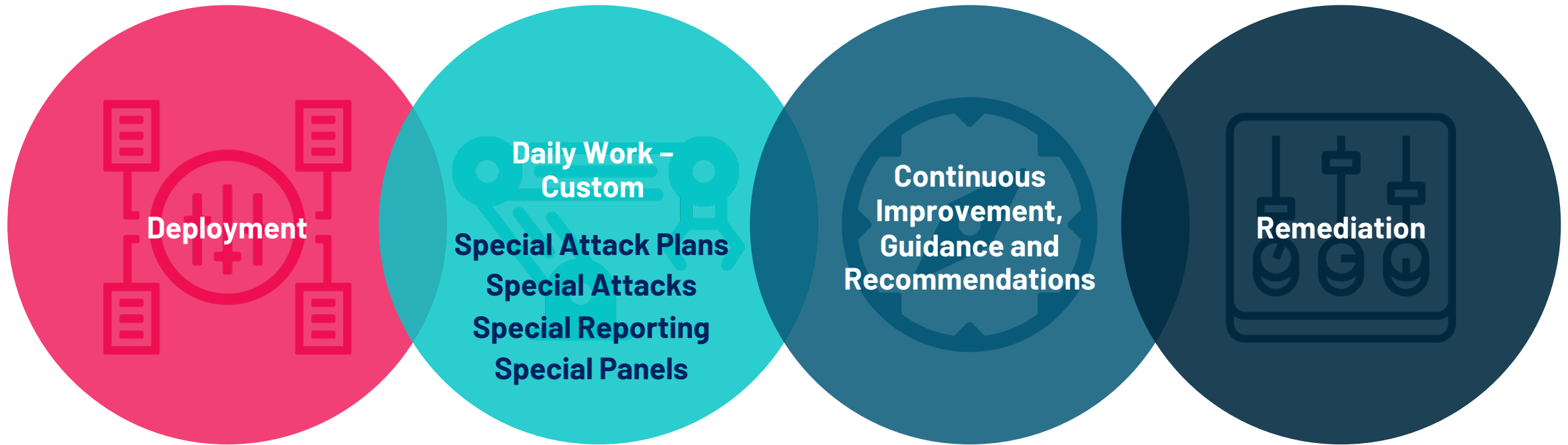
**Explanation**

	SafeBreach Simulator		Representational Systems		Communication Path from MC to Simulators		Identified Infiltration Target
	Security check		Remote User with Simulator		Potential Simulation Paths		Identified Infiltration Target
					Network Segmentation		



# Go from Defense to x with SafeBreach-as-a-Service: The Most Complete BAS Solution

All the advantages of SafeBreach in managing the platform



Enables you to focus on strategy, improvement, mitigation and standard setting and to strengthen your security posture

**Unlock the full-kill chain through agentless web application security authentication**

## **SafeBreach for Web Application Security**

---

Full-kill chain verification

---

The scope includes the top ten security risks of the OWASP®  
Foundation

---

A contextualized view of web application security posture

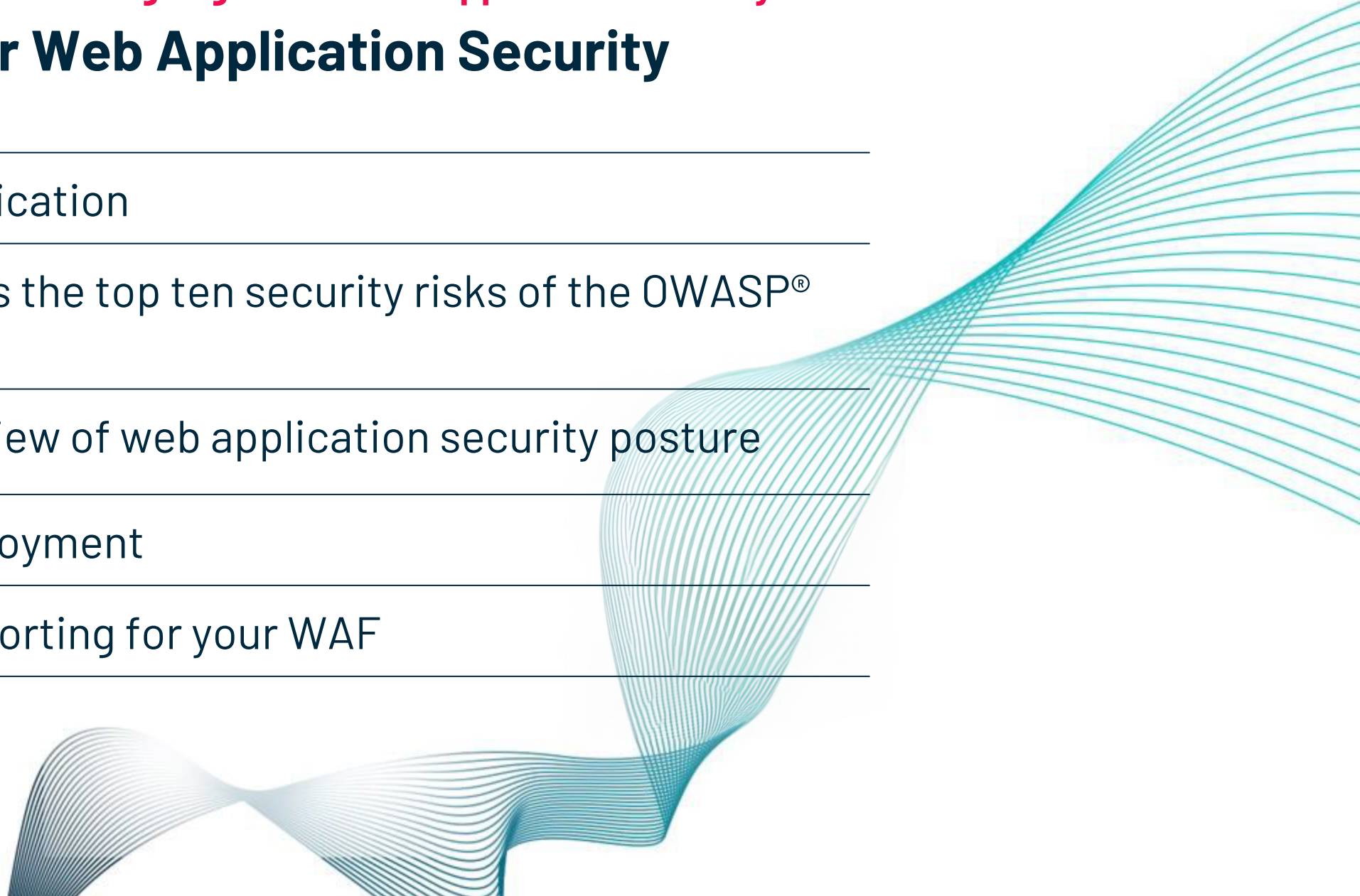
---

Fast and easy deployment

---

Actionable ROI reporting for your WAF

---





# Usage Examples

How does this fit into your security program?





## CUSTOMER CASE STUDY

# Top 3 US Insurers



### Challenge

---

Assess cyber risk and improve posture in OUs and non-integrated organizations



### Solution

---

SafeBreach is deployed in OUs and NIEs and continuously tests for infiltration, host-level, lateral movement and intrusion

---

SafeBreach Panels are reported quarterly to C-level and BoD



### Benefit / ROI (Return on Investment)

---

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

---

Ability to show improvement in posture over time

---

Ability to detect and fix thousands of gaps



## CUSTOMER CASE STUDY

# Top 3 US FIS



### Challenge

---

Assess segmentation controls on the most valuable segments

---

Assess resilience to imminent threats in a short time



### Solution

---

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

---

Used for SafeBreach SLA to test US-CERT security posture



### Benefit / ROI (Return on Investment)

---

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

---

Imminent threat resilience and the ability to communicate the mitigation plan within days

---



# PayPal



## Challenge

---

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



## Solution

---

The M&A team deploys and runs the SafeBreach baseline test during every DD process and assesses the cyber situation within days



## Benefit / ROI (Return on Investment)

---

Assesses acquired risk in a timely manner for impact

---

Evaluates the associated merger budget and impact

---

Efficient and fast assessment process



# Spear-phishing and “living-off-the-land” (LOTL) tools initiate OT attack reconnaissance

## Email, Endpoint & Network Control Validation

Attackers targeted Production employees with spear-phishing campaign. An embedded link pushed malware to create an unattributable communication path to a C&C server. Using LOTL tools, attackers extracted credentials and escalated privileges to begin mapping the extended network architecture and discovering OT targets of interest.

### Objective

Validate endpoint and network controls, visibility, and prevention of malicious host actions as part of the malware activity.

### Test

Ran attack simulations at different stages of the malware kill chain to test host controls including anomalous behavior detection, application whitelisting, and system lockdown policies.

Ran network infiltration/exfiltration simulations to validate filtering rules, lockdown policies, and whether network perimeter security controls are effective against indicators of compromise (IOC).

### Outcomes

Identified network segmentation and filtering rules were not adequate with potential risk to exploit publicly known vulnerabilities and leverage multiple open-source tools to gain access to sensitive networks. Efficacy of EDR policy to detect and prevent malicious behaviors needs improvement.

Confirmed security controls can be strengthened applying the principle of least privilege. Also recommended disabling command-line scripting activities and permissions as threat actors will have difficulty escalating privileges and/or moving laterally.

Web filtering controls were strengthened against malicious C2 communication.



# Malware to disable critical infrastructure and render it inoperable

## Endpoint & Network Control Validation

Attackers targeted Windows-based HMIs within ICS network using WhisperGate and Hermetic malware. They attempted to manipulate the master boot record, to render the devices inoperable and shut down power generation.

### Objective

Validate network configuration and efficacy of network security controls, endpoint controls, and remediation response.

### Test

Validated SPAN port configuration.

Ran network attack simulation against level 2 and level 3 HMIs and Engineering workstations to verify OT security tools are functioning properly.

Test OT Network security controls with SafeBreach ICS attacks (Network Transfers).

### Outcomes

Lateral movement attacks identified improper configuration of network-based access control lists (ACLs) and system vulnerabilities allowing malware propagation.

The results highlighted that network segmentation and filtering rules were not adequate with potential risk to remove/modify configuration attributes, or destroy firmware or system binaries – which could isolate or degrade availability of critical network resources.





# Purpose-Built OT Ransomware

## IT/OT Security Validation

WannaCry and SNAKE ransomware attacks forced two top-10 automakers to shut-down production lines. Both attacks are thought to have originated with phishing, and successfully hijacked Windows-based ICS endpoints.

### Objective

Validate network configuration and efficacy of network security controls, endpoint controls, and remediation response.

### Test

Ran simulated attacks to validate system security controls in order to identify where to limit access to data involving production processes and identify weakness in security controls whereby malware could be introduced on the system.

Through our endpoint detection and response (EDR) integration tool, specific threat behaviors were simulated to validate the effectiveness of endpoint controls and validate those alerts generated by the EDR were prioritized correctly.

### Outcomes

Lateral movement simulations validated security controls and that network segmentation and filtering rules were minimally effective resulting in the implementation and enforcement of multi-layer network segmentation with the most critical communications and data resting on Whisper Gate the most secure and reliable layer.

Web filtering controls were strengthened for malicious remote monitoring and management software, and remote desktop software applications that aid in malicious exploits.



# Supply chain attack exploits weak network segmentation to infiltrate OT environment

## Network Perimeter & Segmentation Validation

Cyber criminals targeted an HVAC vendor to gain remote access to their client's OT network. Once inside the attackers moved laterally from the Facilities network to the OT network at the production plant.

### Objective

Gain visibility into effectiveness of compensating controls in OT environment.  
Validate the OT systems are adequately protected despite the patching lifecycle.

### Test

Ran attacks between critical process areas - validated segmentation policies, network inspection and threat prevention across critical segments, including within each process area and between process areas.  
Ran endpoint attacks to validate that local protections, such as application whitelisting and lockdown policies, were effective against specific attacker techniques.

### Outcomes

Simulation results confirmed security controls can be strengthened applying least access models and defense-in-depth to help prevent successful exploitation attempts.  
Lateral movement simulations validated need for enhanced network segmentation, separating OT networks into sub-zones based on roles and requirements.





## With Safe Breach for OT...

“ SafeBreach has really helped us look at our IT and OT networks more comprehensively. Testing our controls on likely entry points and critical connections between the two networks has enabled us to prioritize our remediation efforts much more efficiently. ”

– Global Pharmaceutical CISO





 SafeBreach

Thank you

OTD BİLİŞİM  
GLOBAL VAD

ICT  
OTD  
PREFER EXPERIENCE ONLINE  
Since 2011