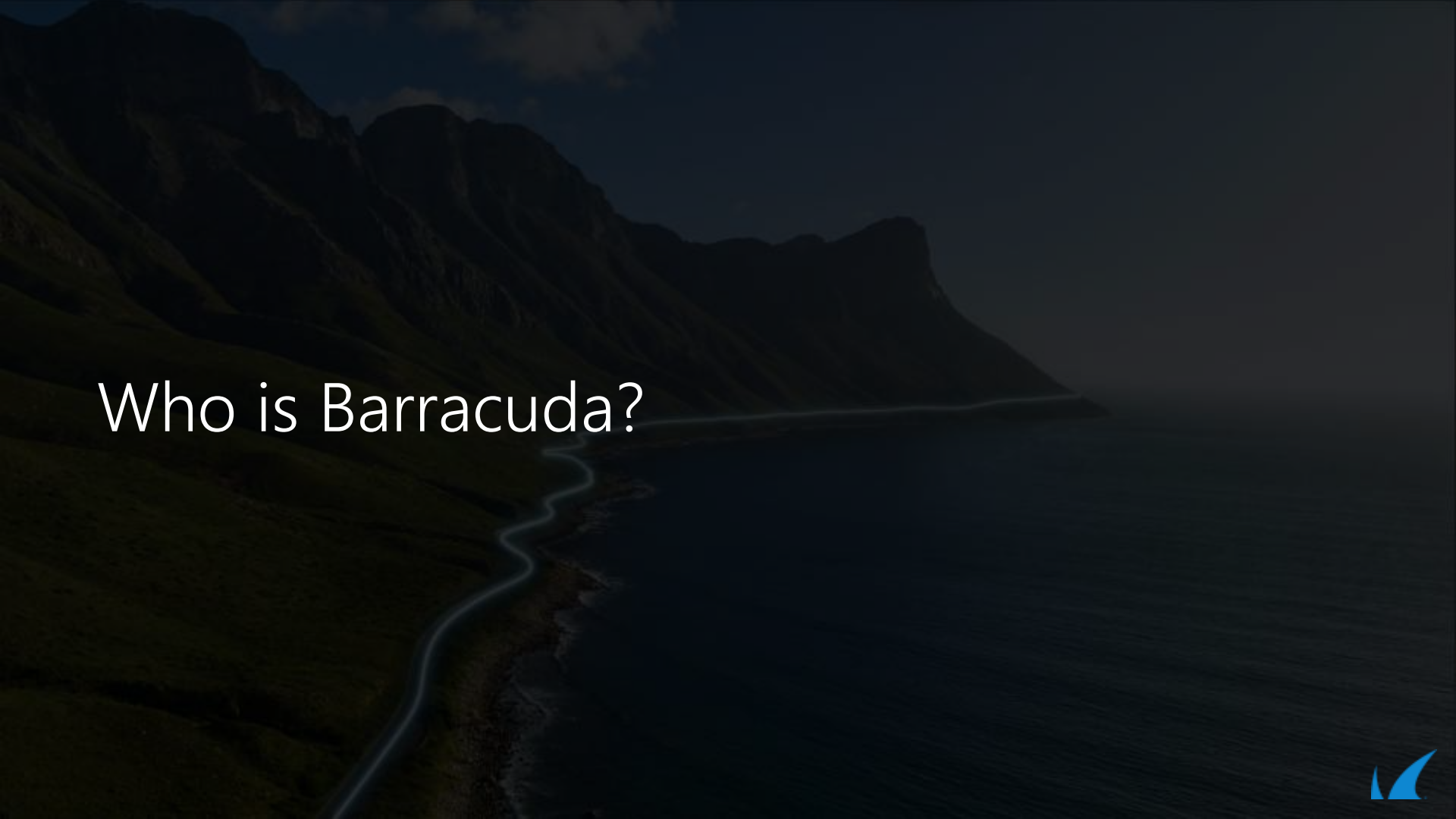
# Barracuda @ GELSEN-NET Security Day

## Services and Products

Florian Vojtech, Senior Manager Presales DACH

Barracuda
Your journey, secured.

# Who is Barracuda?



# We're a global company with massive scale

200,000
CUSTOMERS WORLDWIDE

32,000
CHANNEL PARTNERS

5,000
MSP PARTNERS

134
COUNTRIES SERVICED

Malicious emails blocked
(per week)

280M

Emails archived
(per week)

1.3B

Protected customer data

393PB

Zero-day network attacks blocked
(per day)

5M

# We're trusted by analysts and customers

FORRESTER®
Enterprise Email Security Wave

FORRESTER®
Web Application Firewalls Wave

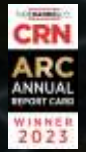
Gartner
Enterprise Network Firewall MQ

SC AWARDS 2022

Best Customer Service
Best Machine Learning/AI

Best Email Security

Product of the Year
Secure Connector




Best
Data
Protection
Software

Barracuda RMM
Managed &
Cloud Services
Winner

Finalist
Managed
Detection &
Response
category

Best WAF
& WaaP

Winner
CloudGen Access
for MSP

Winner
CyberSec Asia
Readers' Choice
Award 2023

# Barracuda Solution Framework ("Trust Platform")

Managed Services / XDR

Deployment Choices / Flexible Consumption

## Email Protection

- Spam, Malware, Threats
- Phishing & Impersonation
- Account Takeover
- Incident Response
- Security Awareness

## Data Protection

- Backup
- Archiving
- Data Classification

## Network Protection

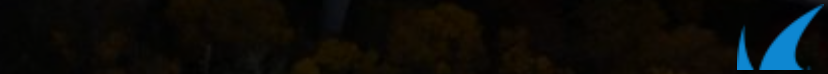
- Secure Access Service Edge
- Zero Trust Security
- Secure SD-WAN
- Network Firewalls
- IoT/OT Security

## Application Protection

- OWASP Top 10
- Bot Protection
- DDoS Protection
- Client-side Protection
- API Security

Product Platforms

Threat Intelligence Platform



Barracuda Network Protection

# The evolution of network security challenges

Public cloud

SaaS adoption

Cyber physical systems

Work from anywhere

Shortage of networking and security experts

Challenging economic environment

# Provide easy-to-use & scalable solutions for

*Universal*

NextGen Firewall Security

Secure SD-WAN, SD-branch, and MPLS replacement

Secure cloud connectivity and security in the cloud

Work-from-anywhere and zero trust network access

*Service providers*

Managed security service provider

*Industrial*

Operational technology & factory floor security

Security & availability for internet connected devices (IIoT)

Edge compute & predictive maintenance

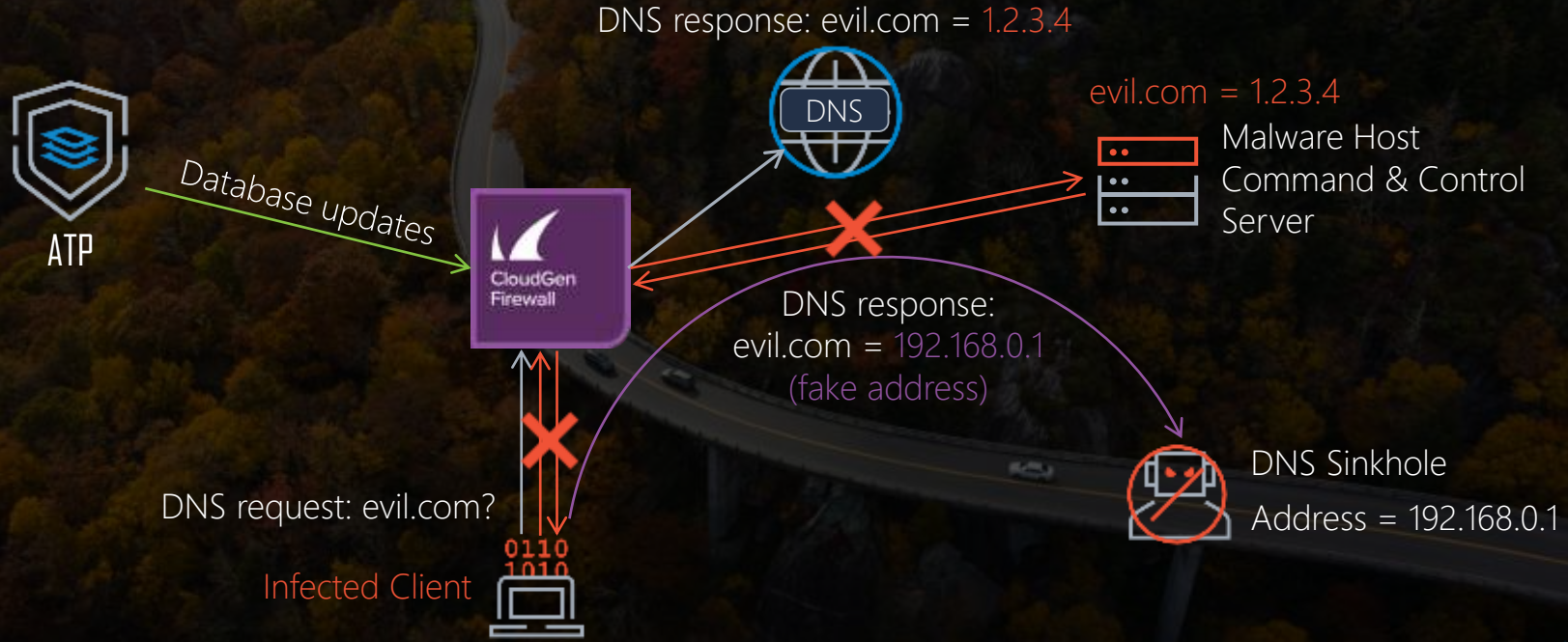
# Full next-generation security

# Barracuda Advanced Threat Protection

# ATP: Botnet & spyware protection

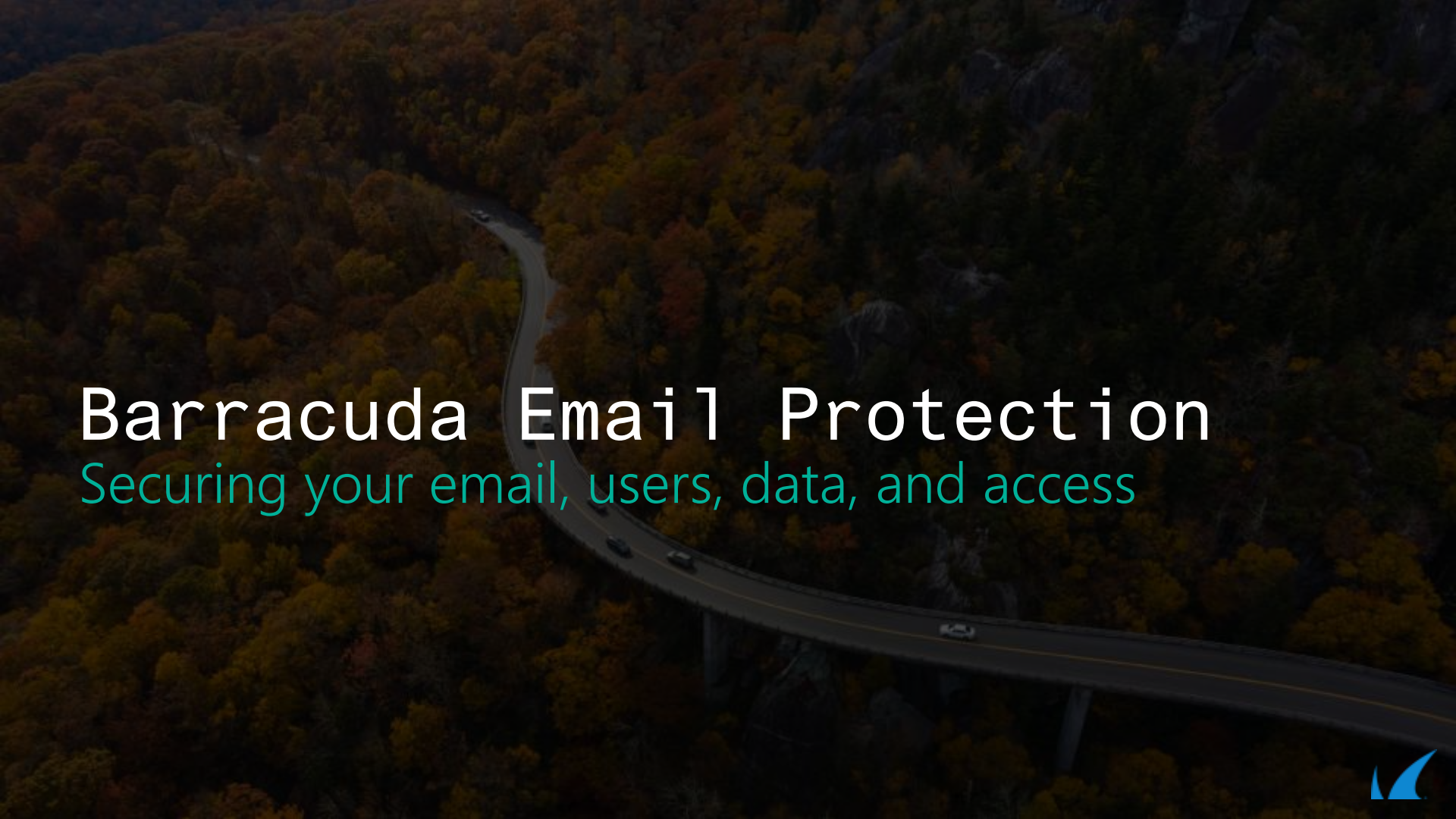
## DNS sinkhole using hostname reputation Database

(needs ATP subscription)



# Intelligent traffic routing

Application-based provider selection – Breakout to the internet


Barracuda Email Protection
Securing your email, users, data, and access

# Email attacks in 2024: what's the risk?

## 75%

Organizations experienced a successful email attack in 2023

## $1M

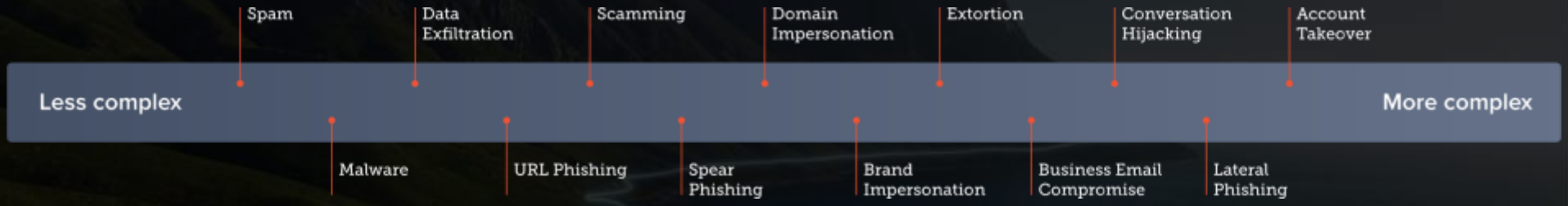
Serious attacks are expensive:

Downtime
Data loss
Reputation
Ransoms

## 98%

Organizations are not fully prepared to deal with email security risks

# Phishing is **STILL** the primary risk surface




99.8% of Email Attacks

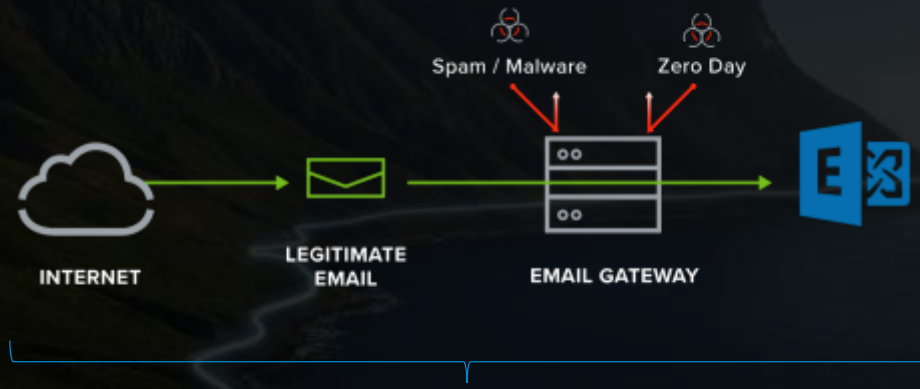
0.2% of Email Attacks

75% of organizations were victim of a successful email attack

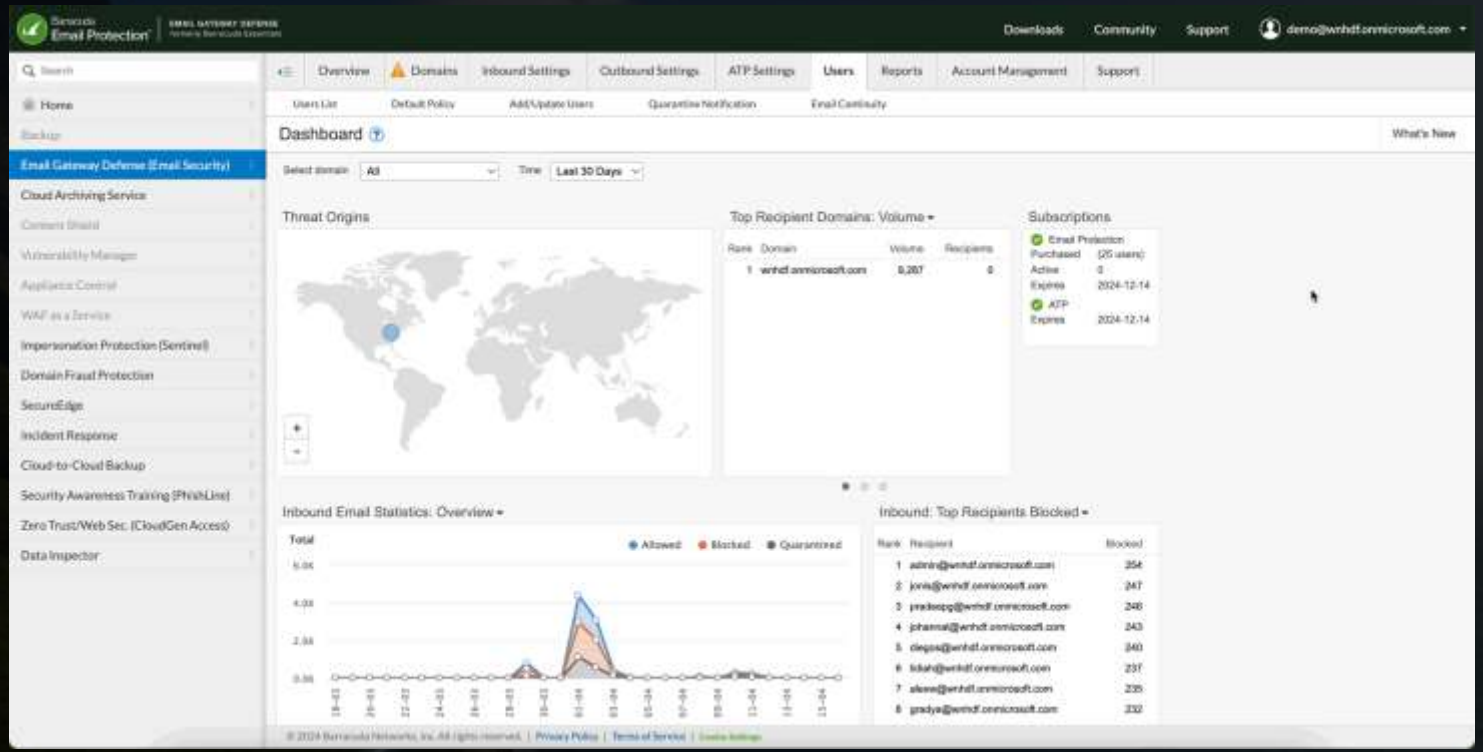
50% of organizations were victim of a successful spear phishing attack

# Secure your email, users, data, and access

# Gateway defense: stop volumetric attacks




- Blocks spam and malware
- Protects against bad links and attachments
- Intercepts sensitive data leaving your organization
- Encrypts outbound email



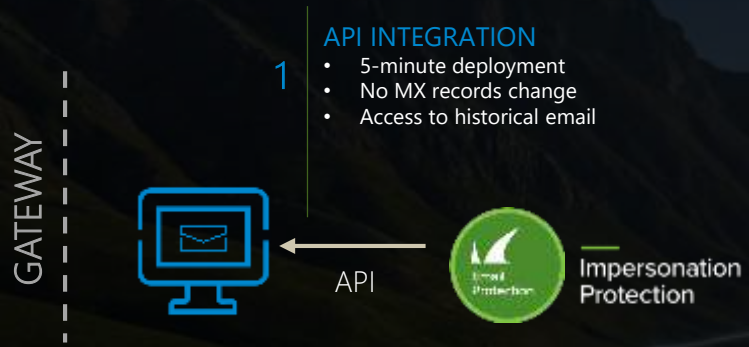

**"Our experience with Barracuda Email Protection has been absolutely positive.**

**The number of emails the gateway catches is fantastic, as well as the ease of configuring blocking criteria."** – System Administrator @ Civil Engineering Firm

“We’re seeing advanced spear phishing in our inboxes. We’re worried about account takeover and ransomware.

How can we prevent it?”

# AI-based inbox defense: stop targeted attacks



# AI-based inbox defense: stop targeted attacks

GATEWAY

1 API INTEGRATION
- 5-minute deployment
- No MX records change
- Access to historical email

API

Impersonation Protection

2 BUILD AI MODELS
- Threat and behavior-based classifiers
- Communication graph

# AI-based inbox defense: stop targeted attacks

GATEWAY

1 API INTEGRATION
- 5-minute deployment
- No MX records change
- Access to historical email

2 BUILD AI MODELS
- Threat and behavior-based classifiers
- Communication graph

3 REAL-TIME ANALYSIS
- Content analysis
- Anomaly detection
- Pattern recognition
- Natural language processing

API

Impersonation Protection

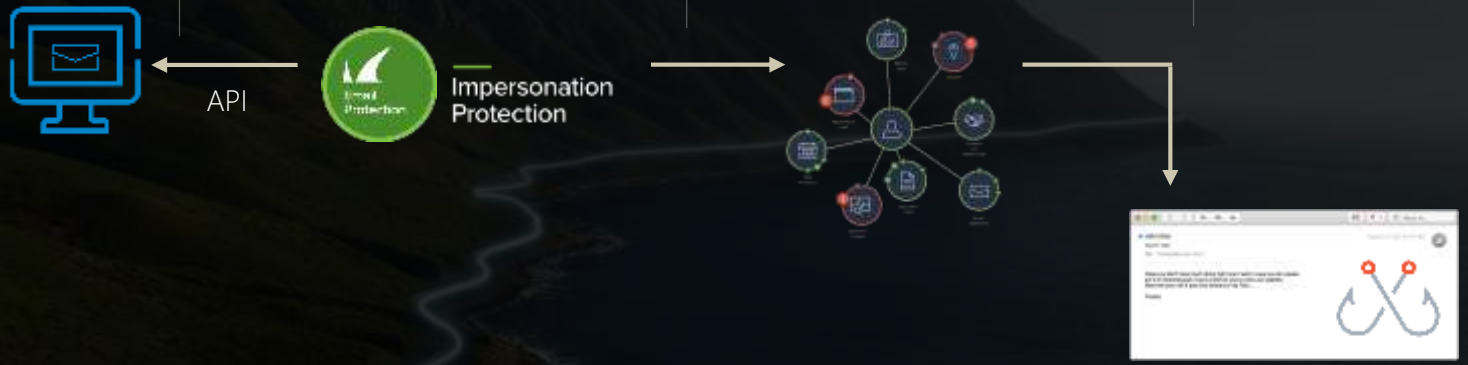
# AI-based inbox defense: stop targeted attacks

GATEWAY

1 API INTEGRATION
- 5-minute deployment
- No MX records change
- Access to historical email

2 BUILD AI MODELS
- Threat and behavior-based classifiers
- Communication graph

3 REAL-TIME ANALYSIS
- Content analysis
- Anomaly detection
- Pattern recognition
- Natural language processing




4 THREAT REMEDIATION
- Automated real-time remediation
- User / IT alerting

# AI-based inbox defense: stop targeted attacks

GATEWAY

1 API INTEGRATION
- 5-minute deployment
- No MX records change
- Access to historical email

2 BUILD AI MODELS
- Threat and behavior-based classifiers
- Communication graph

3 REAL-TIME ANALYSIS
- Content analysis
- Anomaly detection
- Pattern recognition
- Natural language processing

API

Impersonation Protection

4 THREAT REMEDIATION
- Automated real-time remediation
- User / IT alerting

5 CONTINUOUS LEARNING
- Feedback loop
- Continuous retraining
- Lower false positives/negatives

# Account Takeover Protection

## Infiltration

Prevent phishing and ATO attempts with AI

## Reconnaissance

Detect patterns of malicious behavior:

- Suspicious login
- Impossible travel
- Rule changes
- Sent messages
- And more

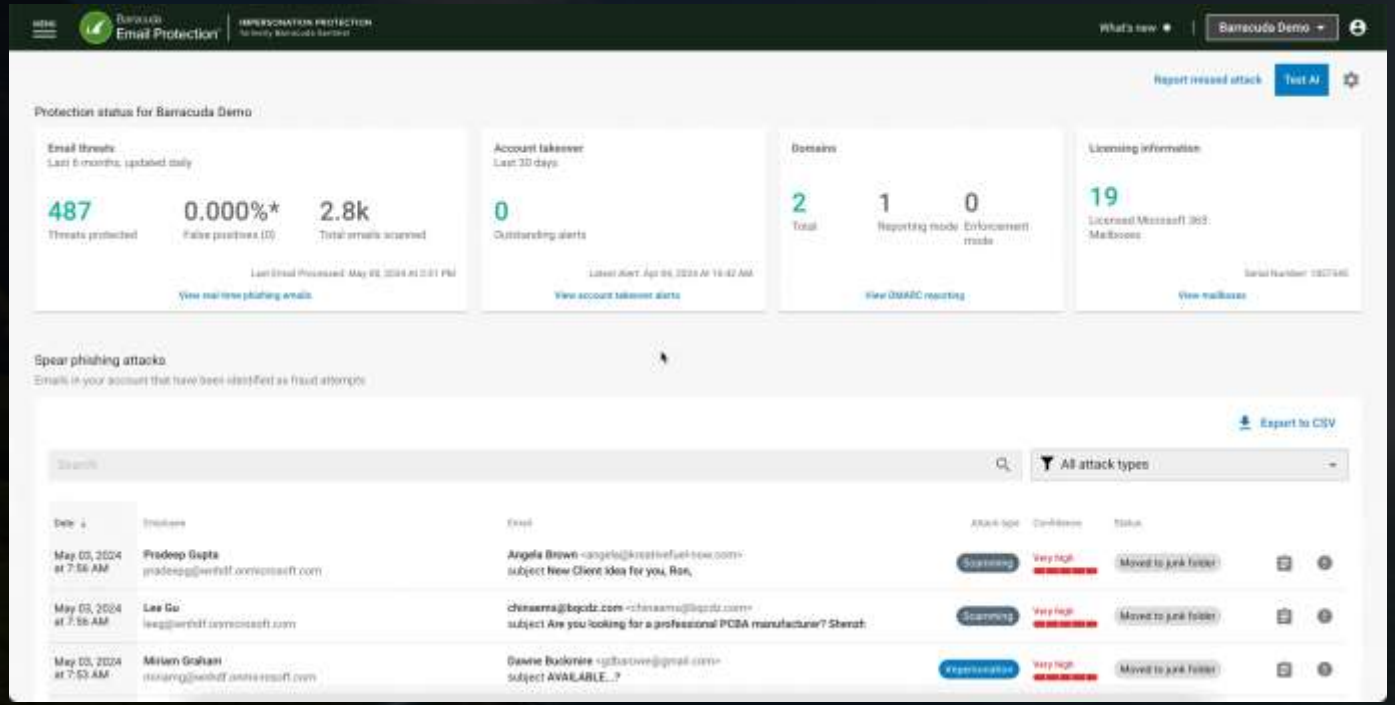
## Harvest Credentials

Prevent lateral movement by flagging malicious internal communications

## Monetization

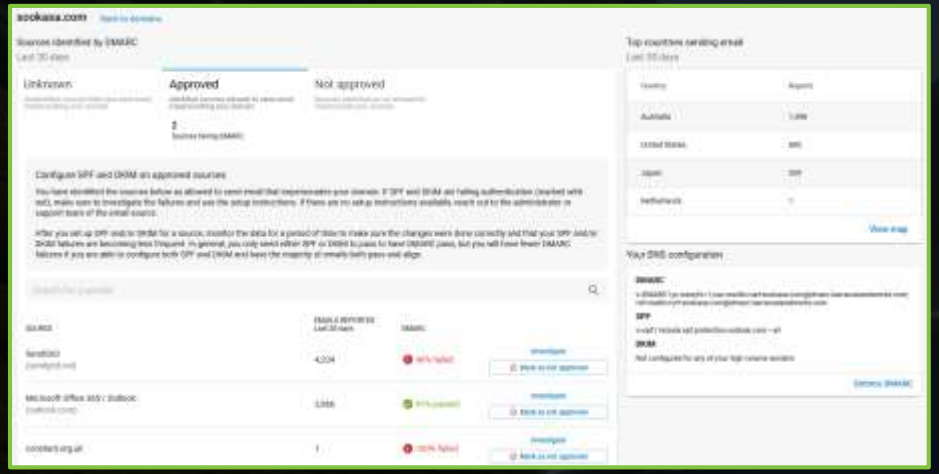
Remediation options:

- IT alerts
- Built-in playbooks
- Remediate malicious emails
- Alert external users
- And more




**"What made the biggest difference was the phishing and impersonation protection that uses AI to detect the kind of account-takeover threats that were our biggest immediate problem."** – IT Manager @ Restaurant Chain

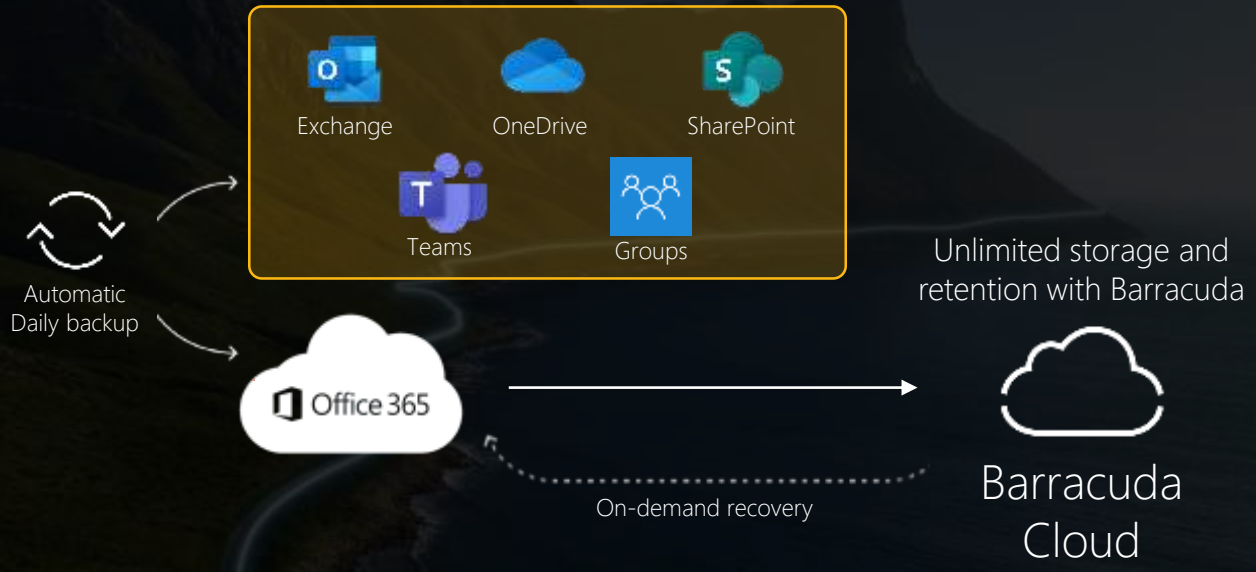
# Domain Fraud Protection: stop spoofing



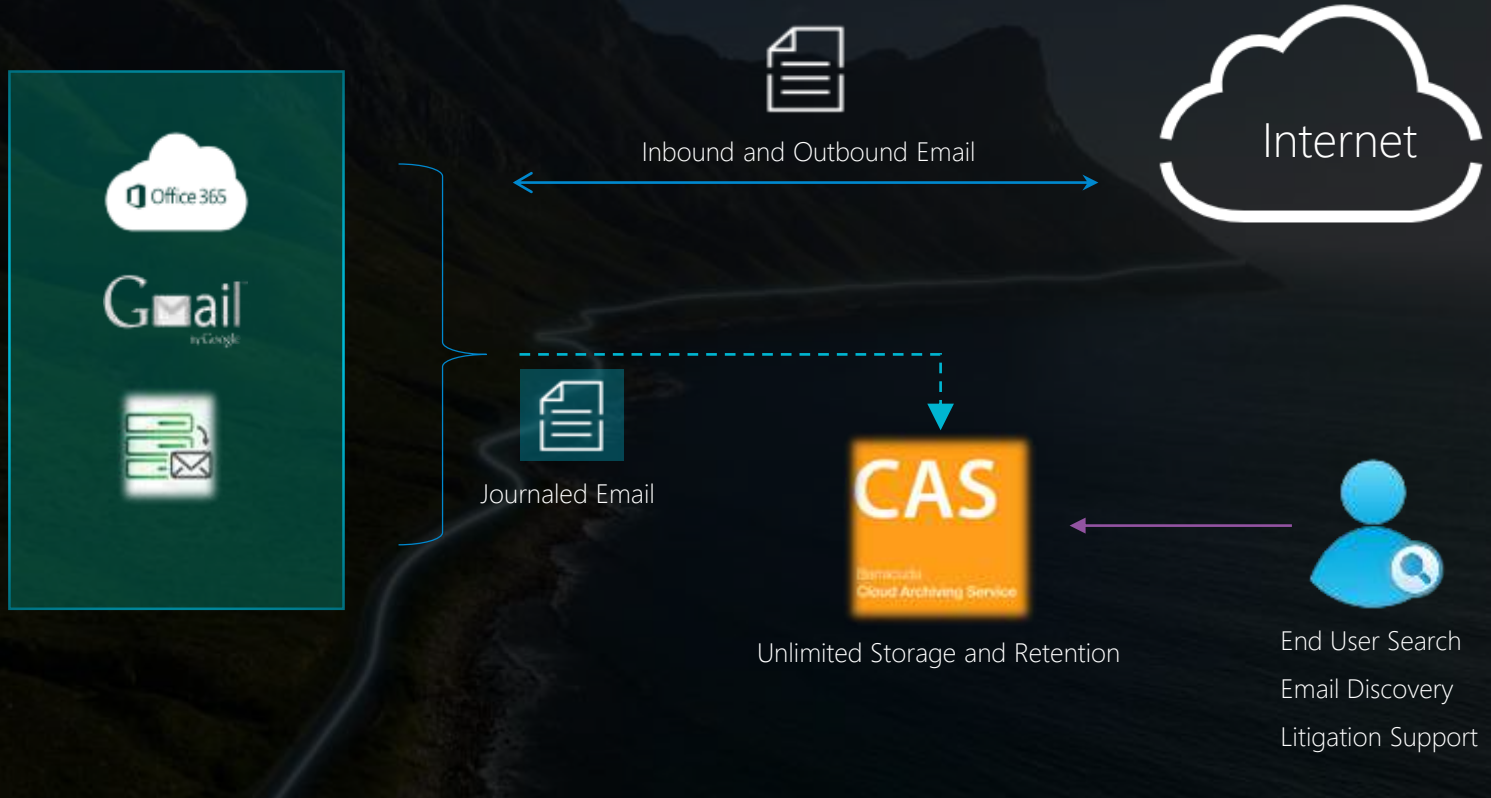
## Simplify email authentication and DMARC enforcement

- Automated DMARC reporting & visualization
- DKIM/SPF configuration and troubleshooting
- Report on misconfigured domains

# Cloud-to-Cloud Backup: set and forget

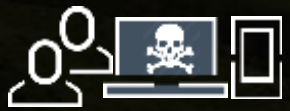


# Cloud Archiving: long-term retention

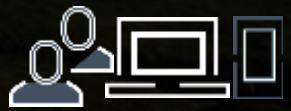


# Zero Trust Access for M365: secure access

In the office or Remote



Compromised Accounts

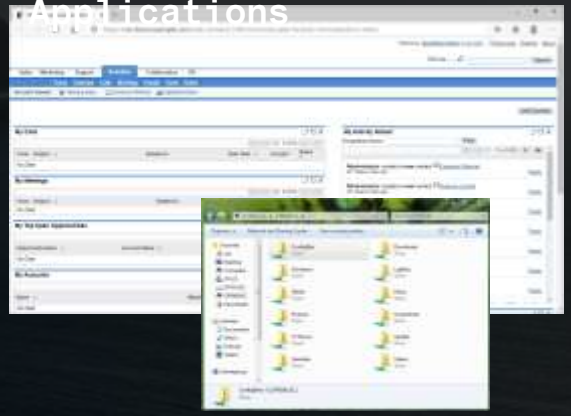


Insecure or Untrusted Devices

**Zero Trust Access**

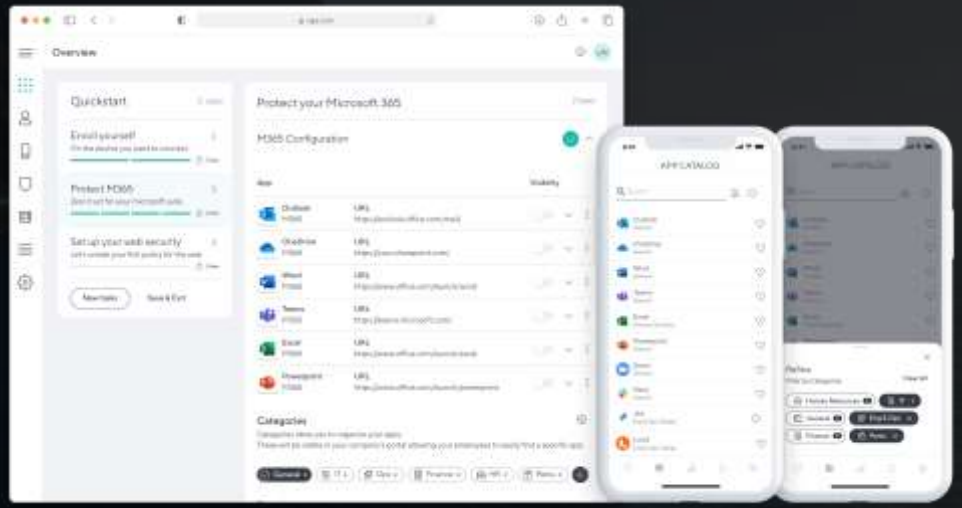
- Identity-Based User Authentication
- Device Authentication
- Device Health Checks (ongoing)
- Per-Application Permissions
- Central Management and Logging
- On-Demand Autoscaling
- Simple Always-On Connectivity

**Microsoft 365 Applications**



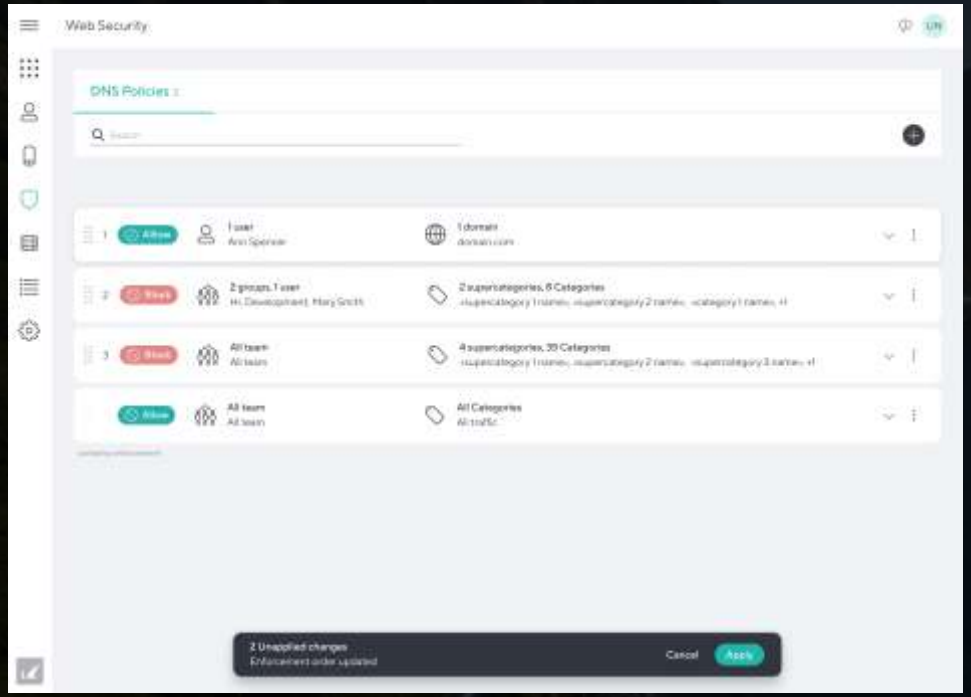
# Simple to deploy and use

- Deployment – including setting up user groups and policies – takes less than 1 hour
  - You can mass-provision devices or have self-enrollment via the major app stores
- End-user application is streamlined and easy to use



“What about web content? How can we protect our employees from visiting malicious or inappropriate websites?”

# Web Security: protect your browsing




Protect users from malicious or inappropriate web content no matter where they work

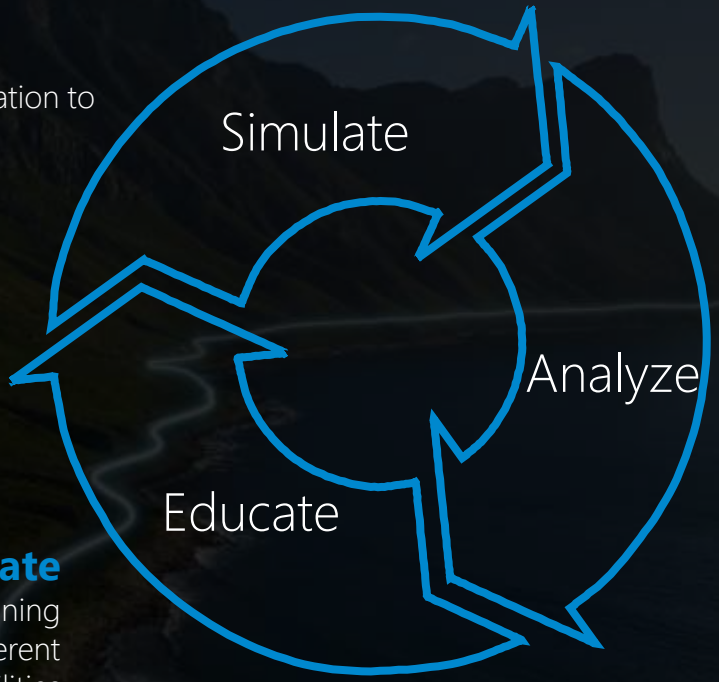
- Filter content at the DNS level
- Real-time threat intelligence
- Flexible enforcement by user-group and location
- Contractor and remote employee coverage
- Centralized management and granular reporting

“We also need to train our employees – for compliance, and so that they’re more vigilant.

We have some habitual clickers.”

# Security Awareness Training: the process

**Simulate**
Real-world threat simulation to assess user awareness




**Analyze**
Detailed reporting metrics to determine threat risk and inform the next campaign

**Educate**
Extensive library of training content tailored for different learning styles and abilities

# Multi-modal, multi-country content

Animated videos (3-5 mins)

Infographics

Threat spotting guides

Curriculums

**"With the advanced anti-phishing protection and security awareness training, we have built the best security against ransomware getting in. "** – Superintendent of Technology @ Texas-based Independent School District

# See for yourself with a free Email Threat Scan

Barracuda
Email Threat Scanner™

- Identify gaps in email security
- Find threats inside Microsoft 365 inboxes
- See threats visualized in multiple ways
- Get a shareable report about threats
- Start a free trial directly from the results!

21,000

Organizations already run the scan

20M

Mailboxes scanned for threats

21M

Spear-phishing attacks identified

Thank You
Barracuda
Your journey, secured.