

Cloud Security Defined: The Required Safeguards for 2019



Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Today's Speakers



Mary Beth Hamilton

VP, Marketing
Eze Castle Integration



Bob Shaw

Director of Cloud Architecture
Eze Castle Integration

Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Today's Agenda



- How to approach a security-first strategy to cloud systems
- Defining the essential security layers from the outside in
- Security safeguards to protect your firm

Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Webinar Details



- ➔ How long? 45 minutes.
- ➔ Will the event be recorded? Yes.
- ➔ When will the recording/slides be available? 24-hours post-event.
- ➔ Where can I follow along?

Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

When to Consider a Cloud Move

Office Relocation

- Ideal time to review
- Don't invest in moving outdated technology
- Migrate to cloud prior to relocation

New Applications

- Easy to add new applications (in hours)
- Long-term planning no more
- Predictable cost structure

Technology Refresh

- Conduct a cost-feature comparison for on-prem refresh vs. cloud
- With cloud, transition process is simple

Follow Along

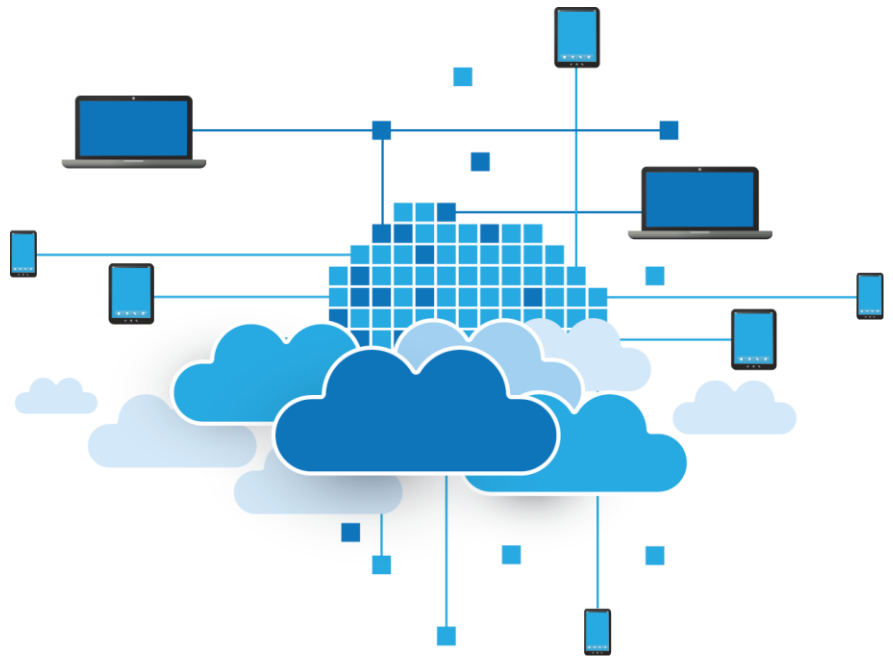
@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Security in the Multi-Cloud Era

- Cloud technology is transforming businesses
- Transition to ‘any’ cloud/multi-cloud mandates Security First Strategy

“By 2020 clouds will stop being referred to as ‘public’ and ‘private.’ It will simply be the way business is done and IT is provisioned.” – IDC



Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Threat Landscape

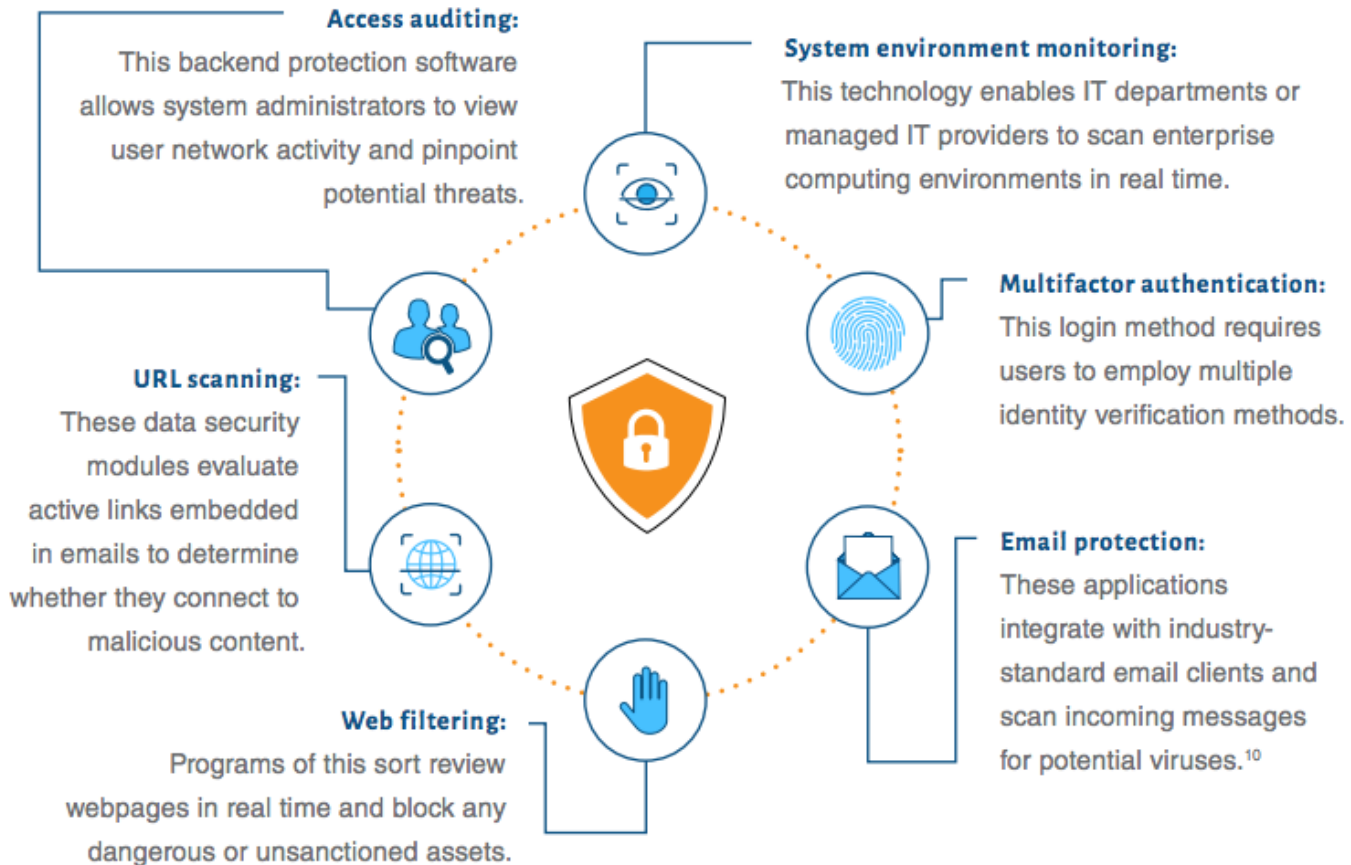


Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

What is a Security-First Approach?



Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Multi-factor Authentication

- Requirement in today's environment
- Enable MFA on all devices and applications:
 - Cloud platforms and remote access gateways
 - Social media sites
 - Web-based apps



Photo Credit: Duo

Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Email Security Components

Anti-Virus +
Malware Protection

- Protect desktops, laptops, servers

Encryption

- Encrypt private information (PII) leave your network

Targeted Attack
Protection

- Block and quarantine messages with malicious attachments or malicious URLs

URL Defense

- Continuously monitors and scans email URLs

Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Web Filtering

Providing a first line defense against threats on the Internet

Block ransomware,
malware and phishing
before it reaches
Endpoints

Protect users anywhere
they go, on and off the
corporate network

Stop malicious domain
requests and IP
responses at the DNS-
layer, over any port or
protocol

Enforce acceptable use
policies

Create custom
block/allow lists

Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Access Auditing

...Unauthorized access is widely considered one of the foremost public cloud security threats— and for good reason...

- Establish clear User Roles & Access Permissions
 - Follow the Principle of Least Privilege
- Monitor and Audit
 - Have an official user provisioning posture
 - Leverage data audit and provisioning software (example Varonis DatAdvantage)



Visualize who can access sensitive and regulated information



Audit every single file and email touch on-premises and in the cloud



Simulate changes in a sandbox and safely commit them when ready



Eliminate repetitive clean-up projects and automate manual data protection tasks

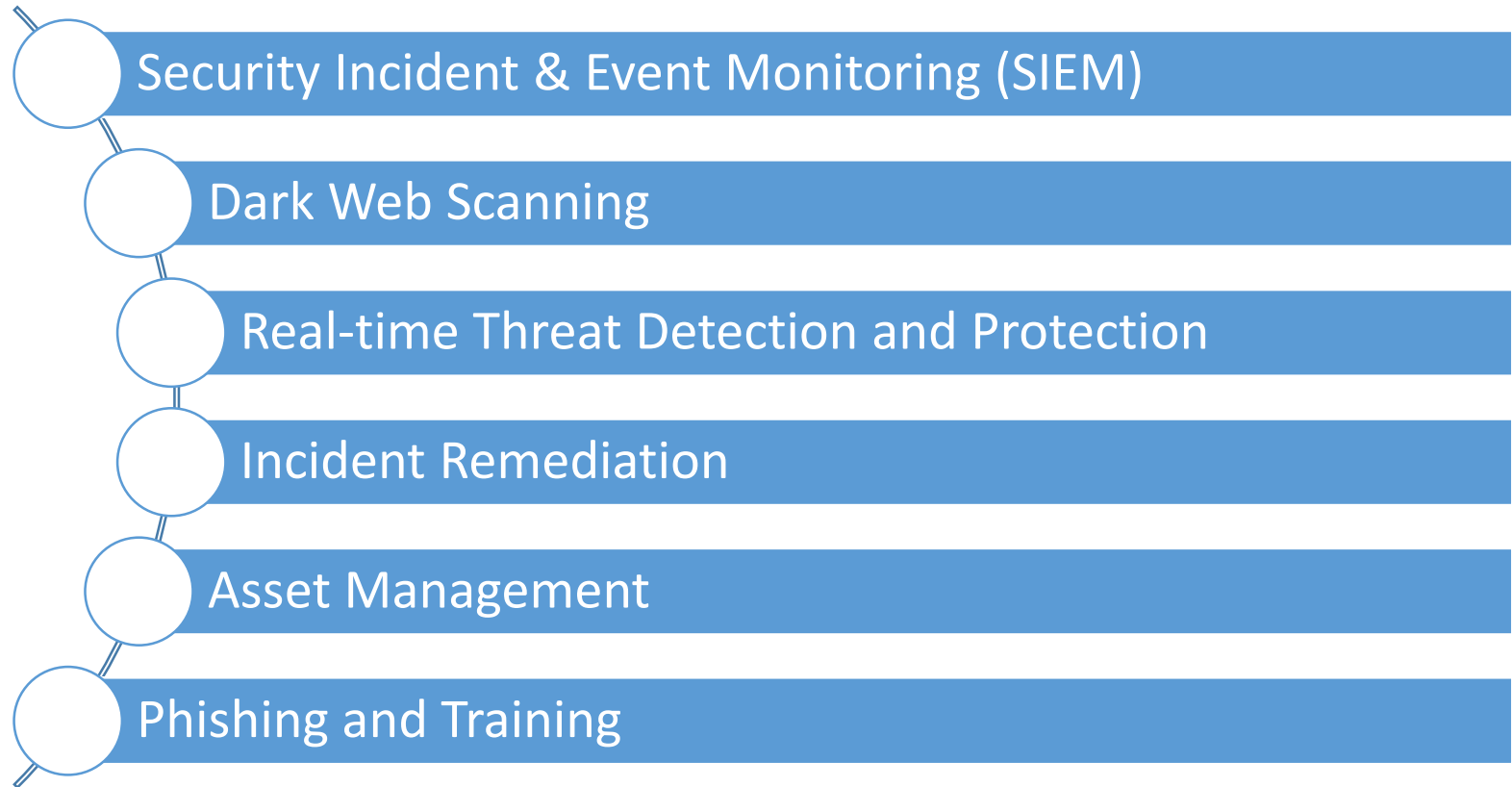
*Photo
Credit:
Varonis*

Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Cybersecurity/Advanced Security Measures



Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Employee Security Training



- Formal Staff training
 - Annual / bi-annual staff training
 - In person or computer based
 - Specify company policies/procedures

- Simulated Training
 - Train and test employees to recognize attacks via phishing simulations

Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Emphasize a Culture of Security

- Ensure top-down executive sponsorship to sustain a culture of security.
 - ✓ “Think before you click”
 - ✓ Validate the people you speak to
 - ✓ Recognize and manage vulnerabilities
 - ✓ Reinforce employee awareness



Acting securely should become second nature to employees!

Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION

Final Thoughts

- Security First Approach is Essential
- Strong Foundation Enables Evolution
- Train Your Weakest Link -> Employees
- Be Prepared to Respond

Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION 

Questions?



Mary Beth Hamilton
VP, Marketing



Bob Shaw
Director of Technical Architecture

Check Out Our Blog!
www.eci.com/blog

[Black Friday & Cyber Monday IT Security Scams to Be Aware Of](#)

[The Risks of Ineffective Patch Management](#)

[The Biggest Security Threat to Your Firm Might Be Sitting Next to You](#)

eci.com/blog

Follow Along

@EzeCastleECI
#Ezecloudsecurity

EzeCastle
INTEGRATION 