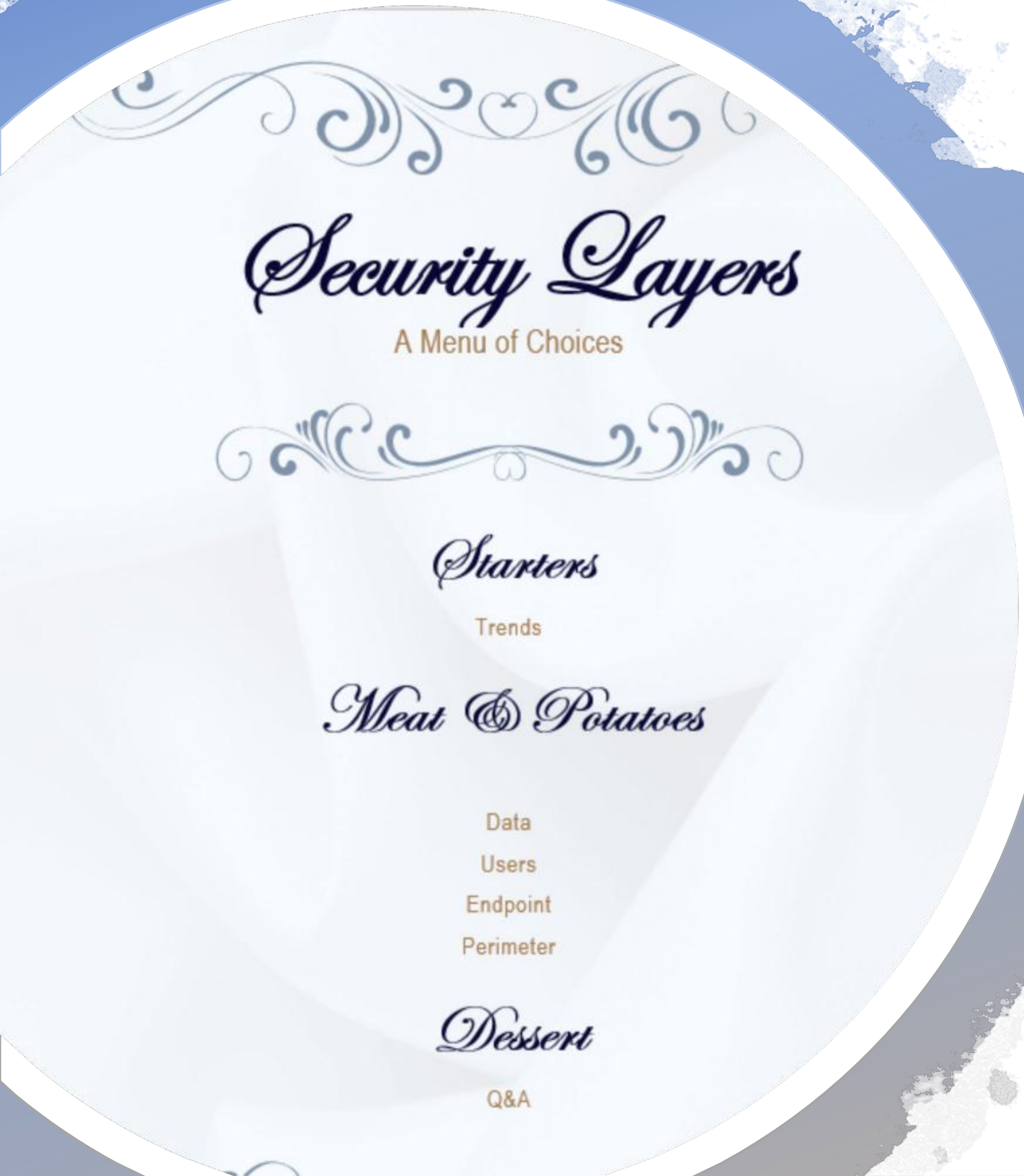
Security Layers
Peeling Back The Onion
A Menu of Choices



Security Layers

A Menu of Choices

Starters

Trends

Meat & Potatoes

Data

Users

Endpoint

Perimeter

Dessert

Q&A

john.dietle@ctcomp.com

ctcomp

Security is like an onion…

- As you peel the layers you get a better understanding!
- But sometimes it makes you cry!

Today’s Menu

Security Layers

A Menu of Choices

Starters

Trends

Meat & Potatoes

Data

Users

Endpoint

Perimeter

Dessert

Q&A

- ***Starters***
    - Trends today
- ***Meat & Potatoes***

    Highlight a few Solutions

    - Data
    - Users
    - Endpoint
    - Perimeter
- ***Dessert***
    - Q&A
    - Cocktails & Dinner

Security Layers

A Menu of Choices

Starters

Trends

Meat & Potatoes

Data

Users

Endpoint

Perimeter

Dessert

Q&A

Today's Menu

- ***Starters***
  - Trends today
- ***Meat & Potatoes***

  Highlight a few Solutions
    - Data
    - Users
    - Endpoint
    - Perimeter
- ***Dessert***
  - Q&A
  - Cocktails & Dinner

Starters

Today's Trends

Today’s Statistics

60% of SMBs will go out of business within 6 months of a cyber incident.

Ransomware is expected to attack a business every 14 seconds by end of 2019.

Source: Cybersecurity Ventures, 2017

Flip a coin once to see if your organization will be victimized by ransomware.

Flip it again to see if paying the ransom gets your data back.

Cybercriminal Ecosystem – For Sale on Dark Web

- Malware/ransomware – free-$20k Software to steal data
- Exploit Kits - $2k – Toolkits to exploit vulnerabilities
- Droppers – free-$10k Software to download malware/ransomware to a device
- Usernames/Passwords – Free - $8/name & password data to phish or hack.

PASSWORD:
QWERTY
80%
of hacking-related breaches leverage either stolen or weak passwords

IN 2018, 43% OF BREACHES INVOLVED SMALL BUSINESS VICTIMS.
$
SOURCE: 2019 VERIZON DBIR

Security Layers

A Menu of Choices

Starters

Trends

Meat & Potatoes

Data

Users

Endpoint

Perimeter

Dessert

Q&A

Menu

Starters

- Trends today

- ***Meat & Potatoes***

  Highlighting Solutions

  - Data
  - Users
  - Endpoint
  - Perimeter

- ***Dessert***
  - Q&A
  - Dinner

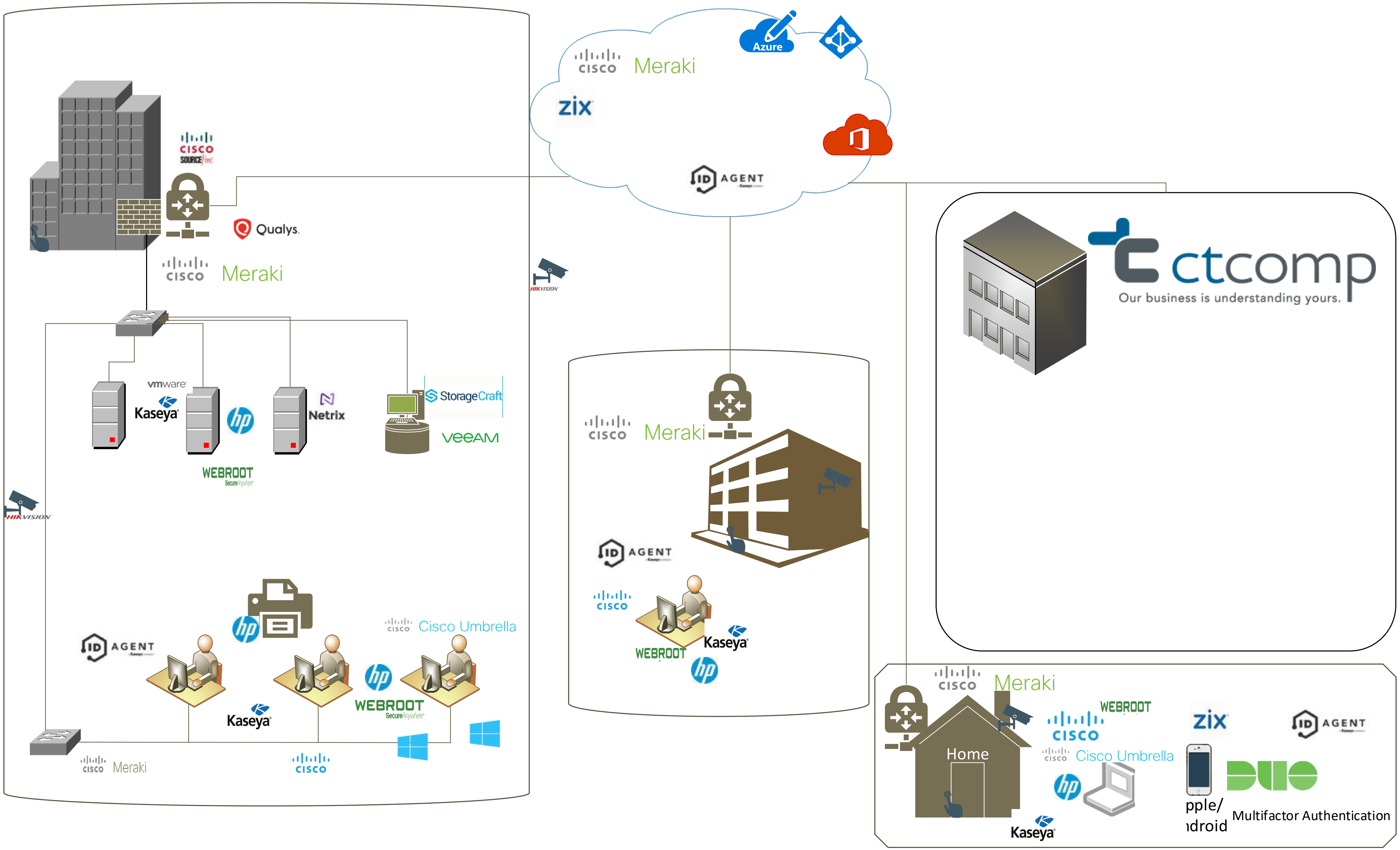
Meat & Potatoes

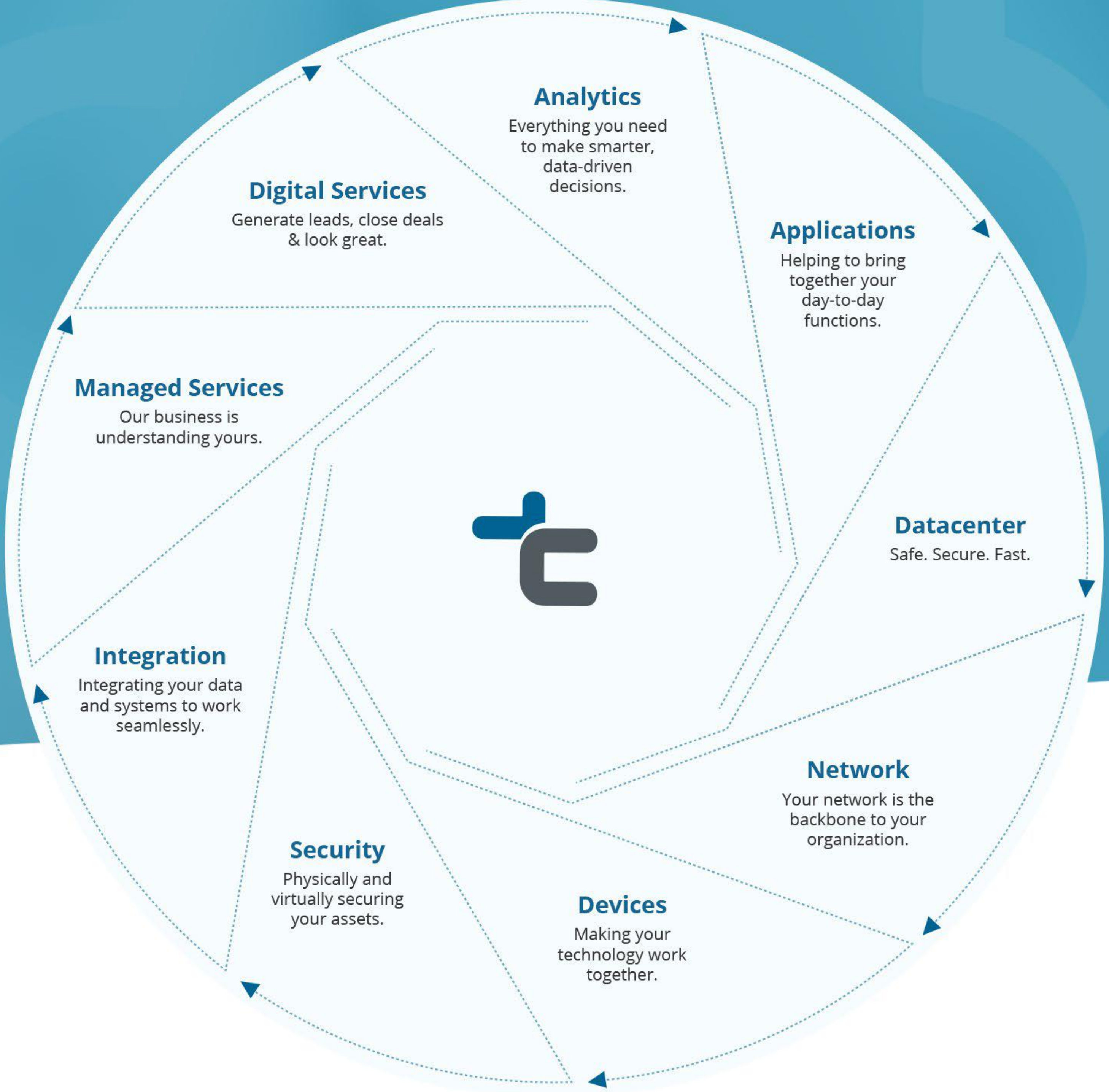
Highlighting Solutions

Why are we only Highlighting Solutions?

- ***Starters***
  - Trends today
- ***Meat & Potatoes***
  - ***Highlighting Solutions***
    - Data
    - Users
    - Endpoint
    - Perimeter
- ***Dessert***
  - Q&A
  - Dinner

CTComp’s Security Portfolio





Analytics
Everything you need to make smarter, data-driven decisions.

Applications
Helping to bring together your day-to-day functions.

Datacenter
Safe. Secure. Fast.

Network
Your network is the backbone to your organization.

Devices
Making your technology work together.

Security
Physically and virtually securing your assets.

Integration
Integrating your data and systems to work seamlessly.

Managed Services
Our business is understanding yours.

Digital Services
Generate leads, close deals & look great.

Menu

Security Layers

A Menu of Choices

Starters

Trends

Meat & Potatoes

Data

Users

Endpoint

Perimeter

Dessert

Q&A

Starters

- Trends today

Meat & Potatoes

- ***Highlighting Solutions***
  - Data
  - Users
  - Endpoint
  - Perimeter

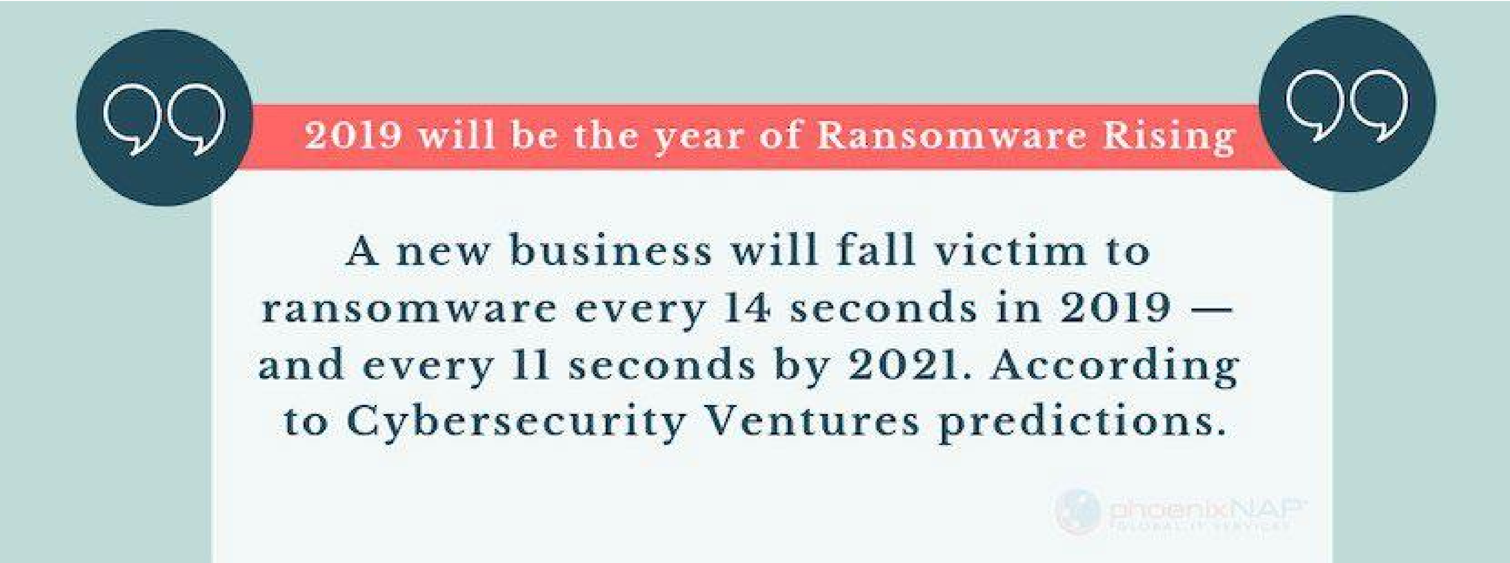
- ***Dessert***
  - Q&A
  - Dinner

Data Security

Backup & Email Security Highlights

- Backup
  - Managed Service On-Premise
  - Offsite Backup
  - Office 365 Backup
- Email Security
  - Advanced Threat Protection
  - Archiving/Compliance for Office 365
  - Zix Protection Suite for On-Premise or Office365

Backup



2019 will be the year of Ransomware Rising

A new business will fall victim to ransomware every 14 seconds in 2019 — and every 11 seconds by 2021. According to Cybersecurity Ventures predictions.

phoenixNAP

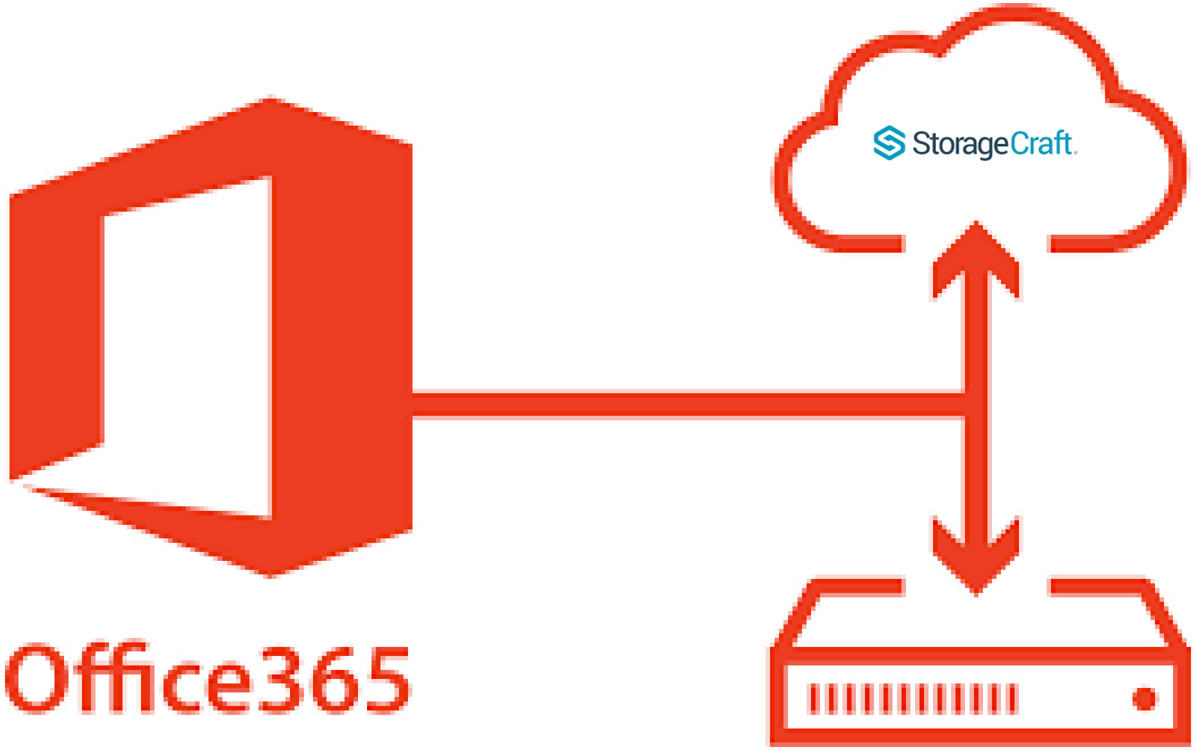
- Many of us use backup to protect from ransomware.
- What if Ransomware encrypts your backup?
- Are you still protected?
- 68% of Small/Medium sized business do not have a DR plan. Do you?

CTComp Managed Backup and Offsite Backup

- Managed Service
  - SSAE 18 - SOC II Type 2
- We install, configure AND MANAGE all aspects of your backup
- Our design minimizes a ransomware attack
- Call us to restore a file, folder, drive or a whole machine. Included in the service.
- Offsite storage at our SOC II Data Center Plantsville CT
  - You can visit your data anytime!
- Add Managed Service - DRaaS.

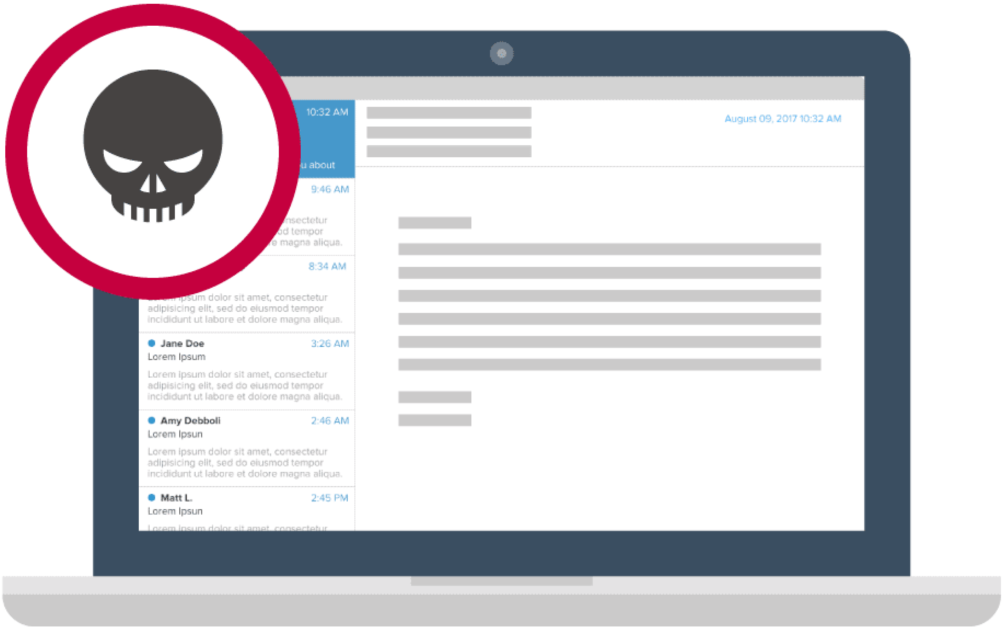
Office 365 Backup

  - Deletion
  - Ransomware
  - Corruption
- Managed CTComp Service



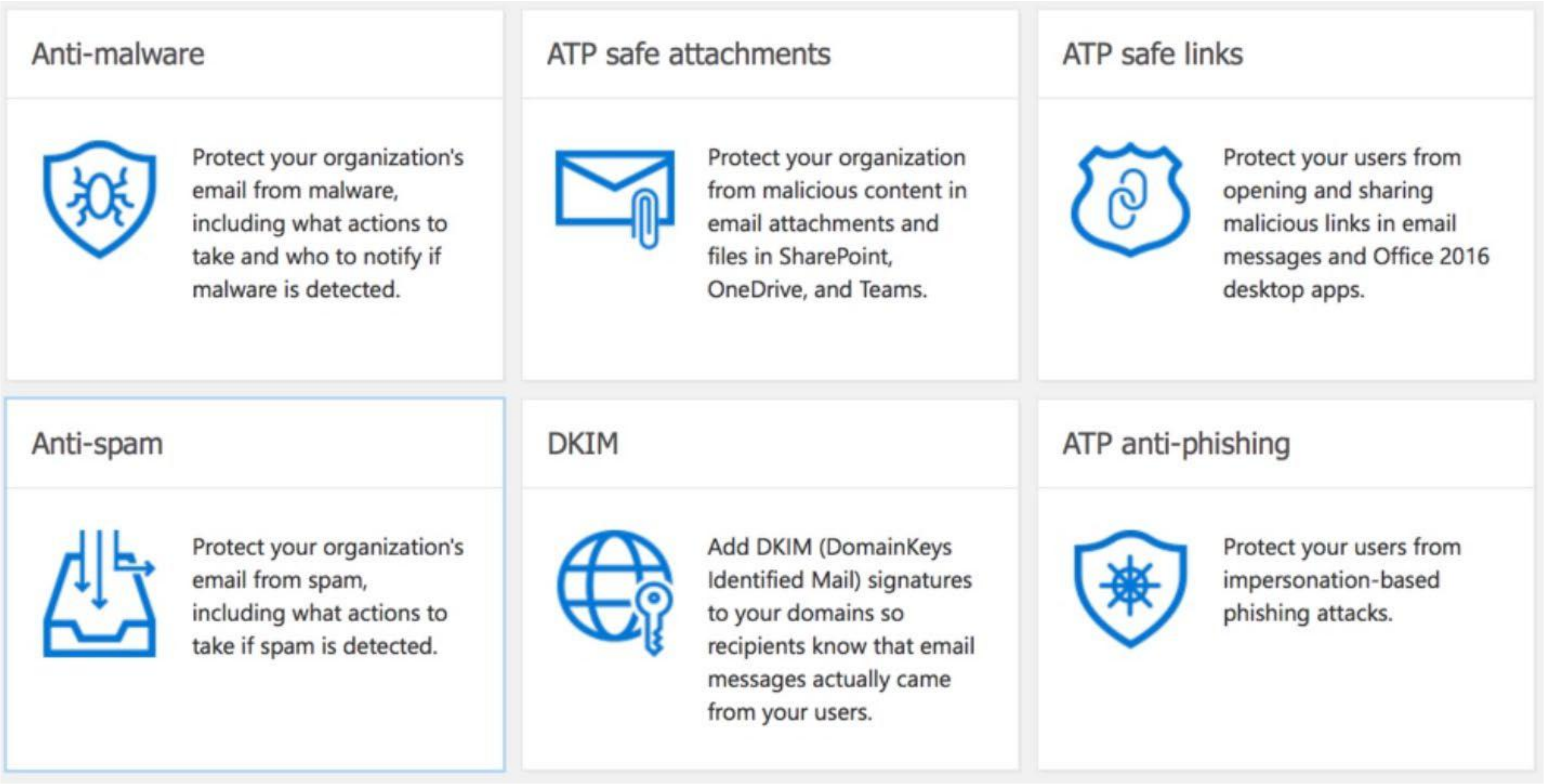
Email Security

- User behavior tops list of challenges
- Targeted phishing attacks make a comeback
- Account takeover is a gateway to more exploits



TOP EMAIL THREATS

Email Security – Advanced Threat Protection



Anti-malware

Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

ATP safe attachments

Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.

ATP safe links

Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.

Anti-spam

Protect your organization's email from spam, including what actions to take if spam is detected.

DKIM

Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.

ATP anti-phishing

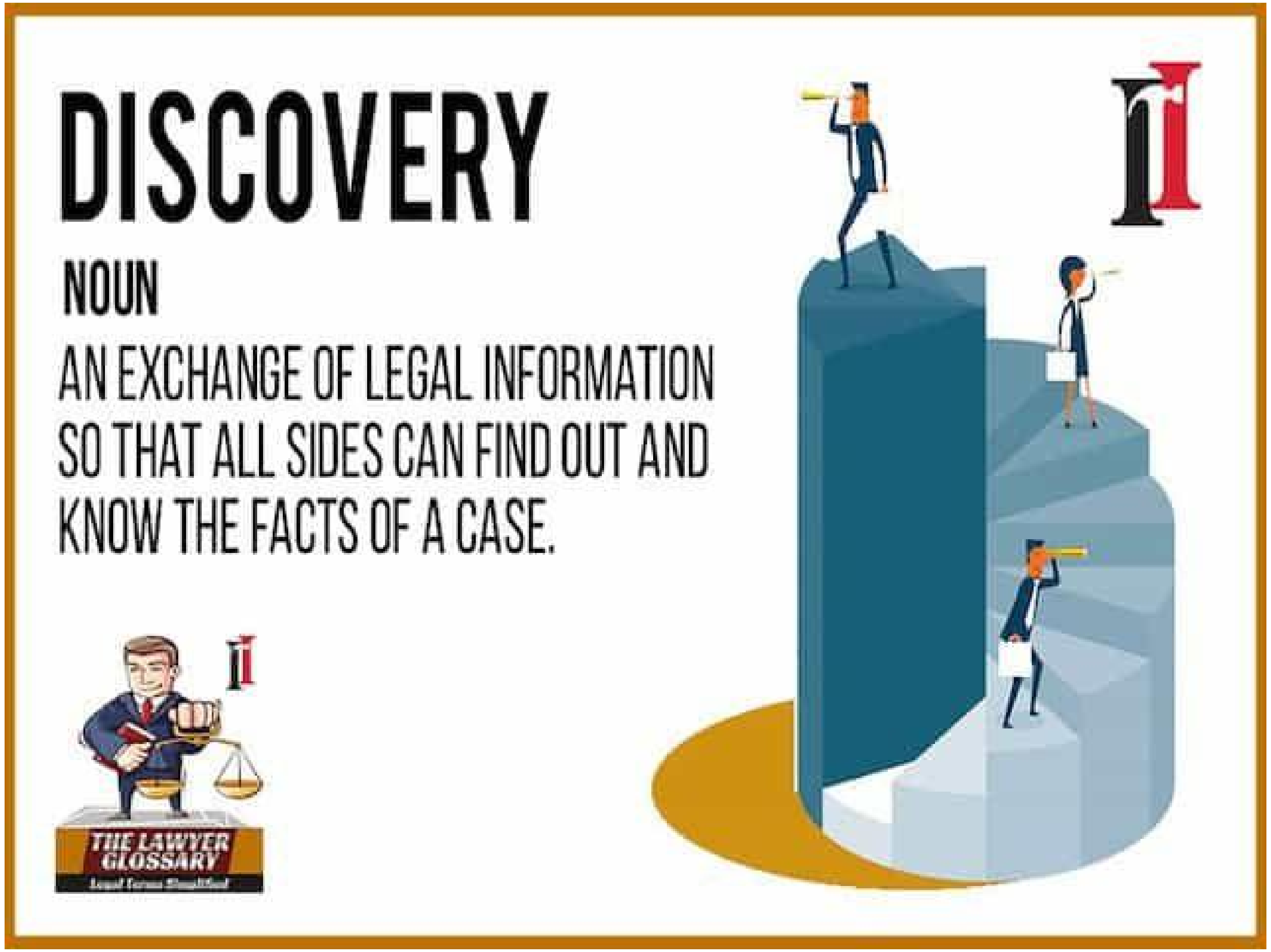
Protect your users from impersonation-based phishing attacks.

Add on to your office 365 subscription or comes with E5/A5 and Business Plans

I don’t need Archiving we are not subject to compliance.

Ever face a lawsuit?

The cost of 1 lawsuit will often pay for having an archival/E-discovery system.



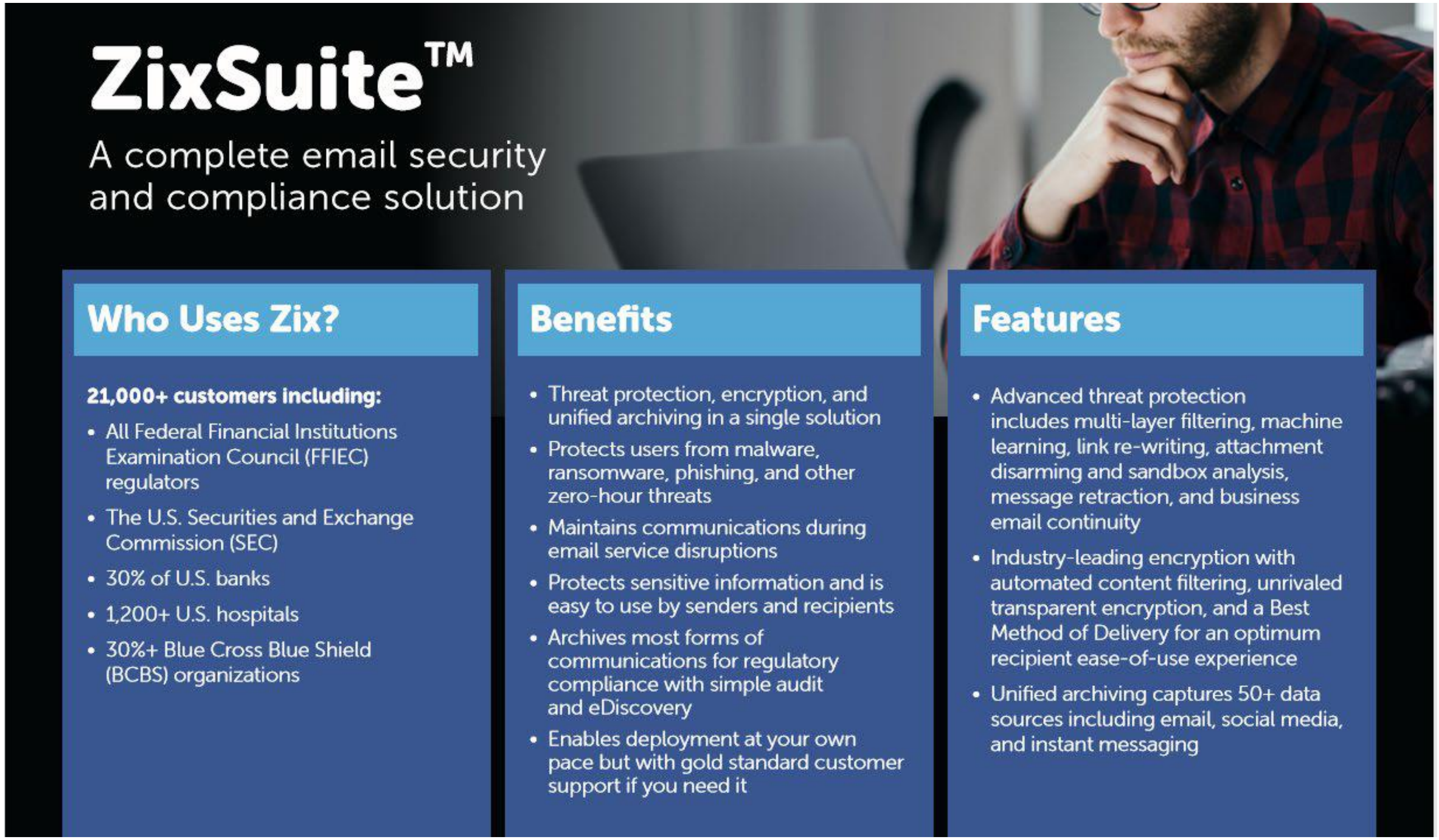
DISCOVERY

NOUN

AN EXCHANGE OF LEGAL INFORMATION SO THAT ALL SIDES CAN FIND OUT AND KNOW THE FACTS OF A CASE.

Archiving - Compliance for Office 365

- Add it to your plan or comes with E3 and above



ZixSuite™

A complete email security and compliance solution

Who Uses Zix?

21,000+ customers including:

- All Federal Financial Institutions Examination Council (FFIEC) regulators
- The U.S. Securities and Exchange Commission (SEC)
- 30% of U.S. banks
- 1,200+ U.S. hospitals
- 30%+ Blue Cross Blue Shield (BCBS) organizations

Benefits

- Threat protection, encryption, and unified archiving in a single solution
- Protects users from malware, ransomware, phishing, and other zero-hour threats
- Maintains communications during email service disruptions
- Protects sensitive information and is easy to use by senders and recipients
- Archives most forms of communications for regulatory compliance with simple audit and eDiscovery
- Enables deployment at your own pace but with gold standard customer support if you need it

Features

- Advanced threat protection includes multi-layer filtering, machine learning, link re-writing, attachment disarming and sandbox analysis, message retraction, and business email continuity
- Industry-leading encryption with automated content filtering, unrivaled transparent encryption, and a Best Method of Delivery for an optimum recipient ease-of-use experience
- Unified archiving captures 50+ data sources including email, social media, and instant messaging

Zix Protection Suite

- ADVANCED EMAIL THREAT PROTECTION
- INDUSTRY LEADING EMAIL ENCRYPTION
- UNIFIED BUSINESS COMMUNICATION ARCHIVING
- SINGLE MANAGEMENT INTERFACE
- BUSINESS EMAIL CONTINUITY DURING INTERRUPTIONS

Security Layers

A Menu of Choices

Starters

Trends

Meat & Potatoes

Data

Users

Endpoint

Perimeter

Dessert

Q&A

Menu

- ***Starters***
  - Trends today
- ***Meat & Potatoes***
  - ***Highlighting Solutions***
    - Data
    - Users
    - Endpoint
    - Perimeter
- ***Dessert***
  - Q&A
  - Dinner

PASSWORD:
QWERTY
80%
of hacking-related breaches leverage either stolen or weak passwords

Users Security
AD, Apps & Awareness Highlights

- Active Directory
  - New Password Guidance
  - Monitoring Dark Web for Username/Password
- Applications
  - 2 Factor Authentication
  - Audit & Data Classification
- Security Awareness Training
  - CTComp Managed Service

Active Directory Passwords – New Microsoft Guidance

"Microsoft now agrees that there is no point to forced password changes and will be removing that recommendation from its security recommendations."

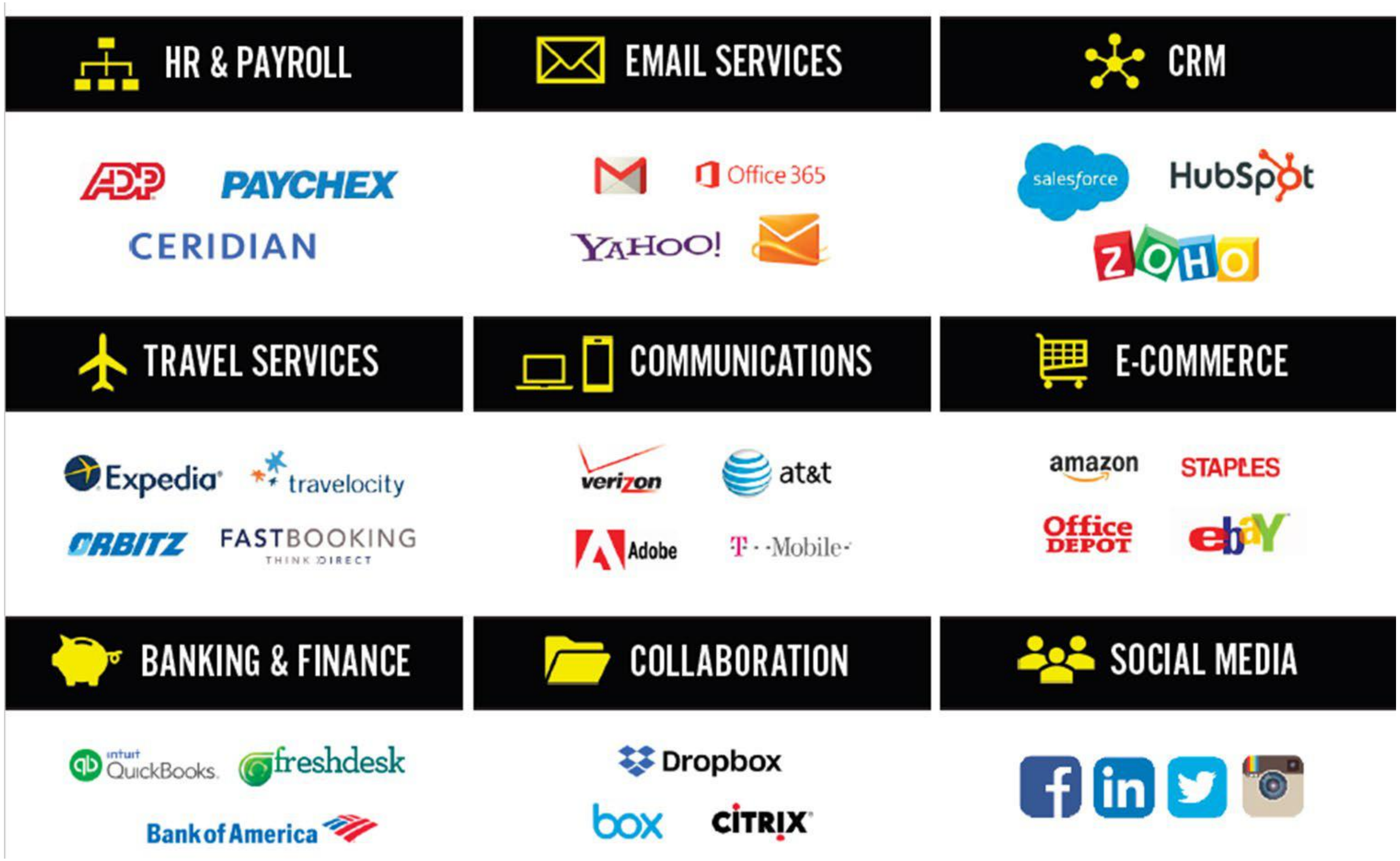
"If your users are the kind who are willing to answer surveys in the parking lot that exchange a candy bar for their passwords, no password expiration policy will help you,"

"If a password is never stolen, there's no need to expire it. And if you have evidence that a password has been stolen, you would presumably act immediately rather than wait for expiration to fix the problem."

The recommendation is change it when it is stolen,
or use 2 factor authentication (2FA or MFA)

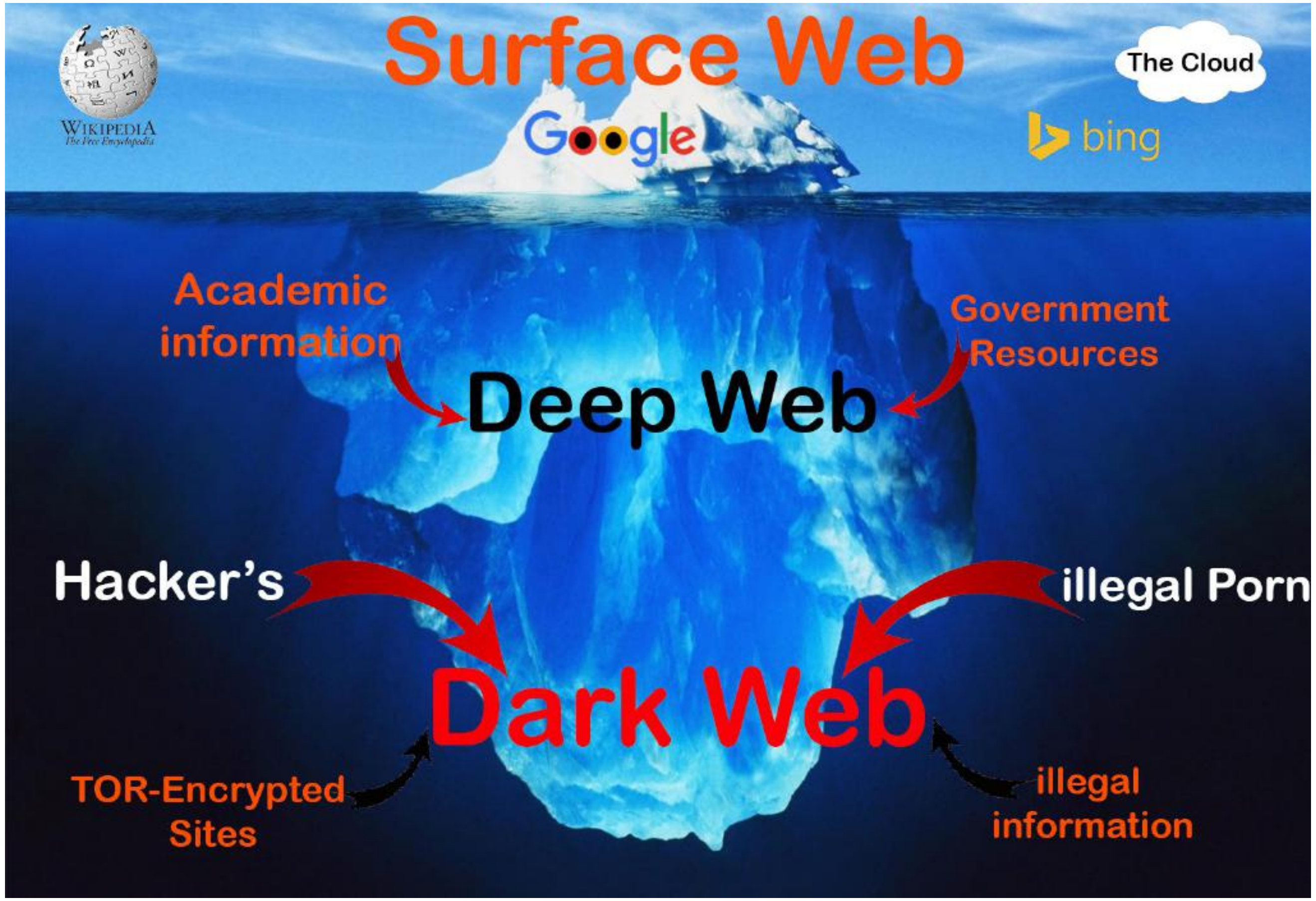
9 ways your employees work credentials can lead to a breach

39% of adults in the U.S. use the same or similar password on multiple sites



Credentials - For Sale on the Dark Web

- Surface web about 4% of Internet
- Deep Web 96% - Dark Web is part of deep web. Not Searchable websites.
- Dark Web it's on the internet
  - Access with VPN/Onion over VPN & a TOR browser
  - There are guides. BUT…
- Site names end in .onion
- Site names are often cryptic
  - Darkweb Marketplace 6ngvt5ueyjyo62zx.onion
- There are Chatrooms
  - chattorci7bcgygp.onion



For Sale: Guns, Porn, Drugs, Malware & Viruses, Exploits, Gift Cards, Usernames & Passwords and more! Pay with bitcoin.

We go into the Dark Web so you don't have to.

Are your credentials on the Dark Web?

Domain	Hits
@achievefinancialcu.com	13
@aefcu.com	145
@calcagni.com	344
@chelseagroton.com	65
@cmhacc.org	80
@duncaster.org	33
@durhammfg.com	59
@dutchpoint.org	20

Domain	Hits
@executiveag.com	44
@firstbristol.org	23
@hedgebay.com	12
@kbebuilding.com	115
@lcdone.com	7
@LenkowskiLoneranCPA.com	10
@livewell.org	2
@Lyons.com	105

Are your credentials on the Dark Web?

Domain	Hits
mdruben@...	1
@milfordbank.com	51
@newbritainct.gov	*
@newenglandcapital.com	5
@nsbonline.com	67
@npsmdit.com	0
@nuzzo-roberts.com	47

Domain	Hits
@richtercegan.com	20
@rjsassociates.com	135
sbjrealtyllc@	0
@southington.org	75
@stencilease.com	19
@superiornetwork.com	79
@sydell.net	2

*protected domain

Are your credentials on the Dark Web?

Domain	Hits
@thomastonsb.com	0
@townofcantonct.org	34
@TrinityHealthOfNE.org	*
@vna-commh.org	61

Domain	Hits
@wchn.org	138
@wctfcu.org	37
@wewlaw.net	3
@wiltonlibrary.org	38
@winnicklaw.com	11

*protected domain

Dark Web Monitoring

- Managed Service from CTComp
- Monitor the dark web for compromised credentials and sensitive data. We notify you and/or your users when problems arise.
- Monitors your domains for email/password attacks
- Monitor personal email addresses for key employees
- Monitors your public IP address(s) for botnet and other attacks
- Alerts you with a ticket when a password is compromised.

When alerted change your password on any site you use that combination of user/password.

First Domain $75/month. Additional domains, if needed, $35/domain/month!

We use complex passwords. We are safe, right?

Dictionary word passwords are cracked in seconds!

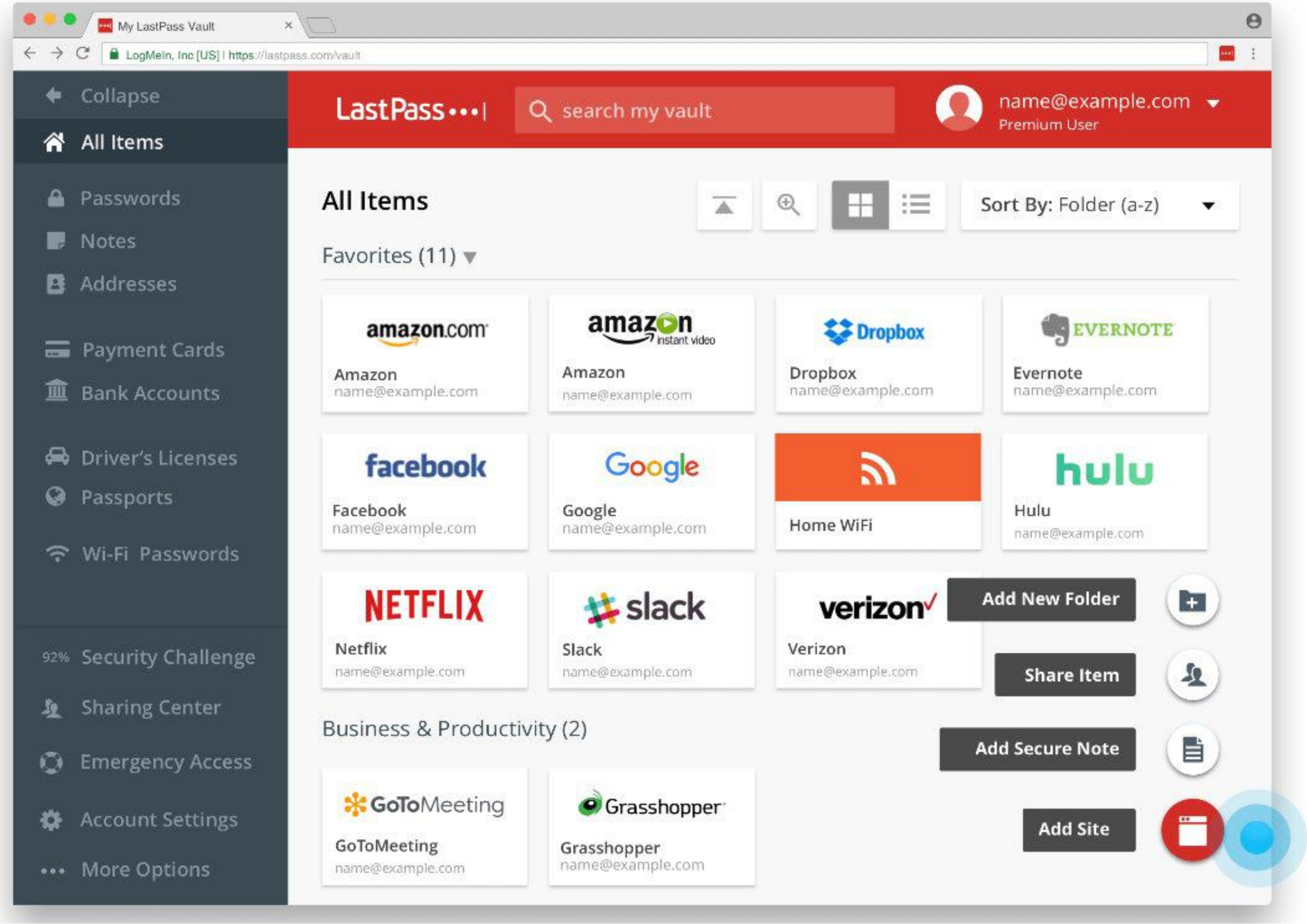
vacation	–	1.8 seconds	(8 char - lower)
VacAtion	–	7.6 minutes	(upper/lower)
VacAti0n	–	31 minutes	(+number)
V@c#ti0n	–	4 hrs	(+symbol)
% V@c#ti0n?	–	3 years	(+10 char)

Passwords should be fully complex (upper/lower/number/symbol)
10 char min

Use a different password for every site!

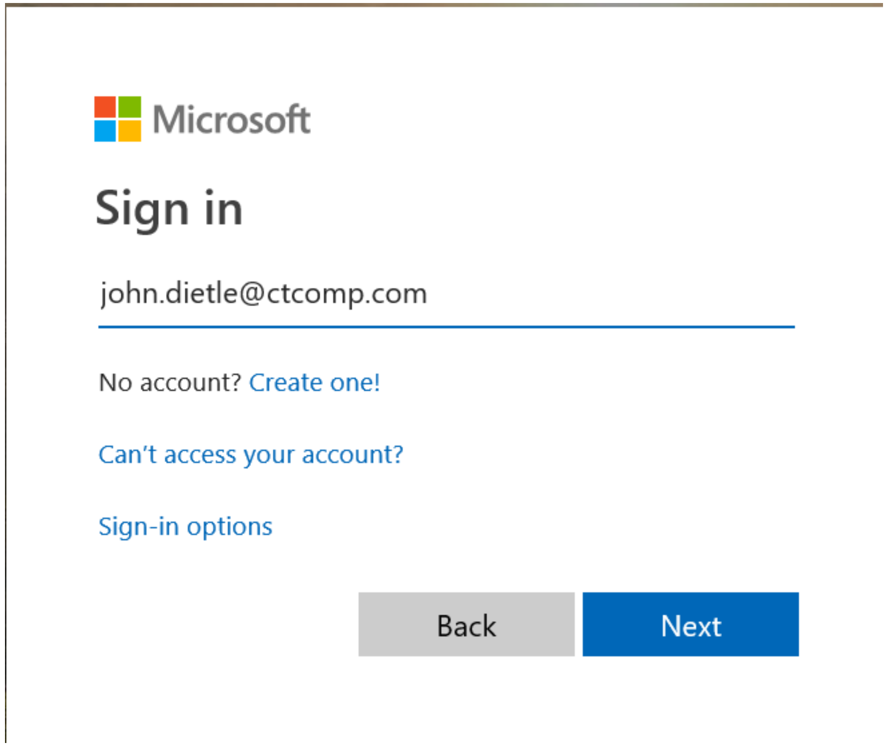
Use password managers
Use multifactor authentication!

Use a Password Manager



LastPass•••|

Cisco Duo Multi-Factor Authentication



Microsoft

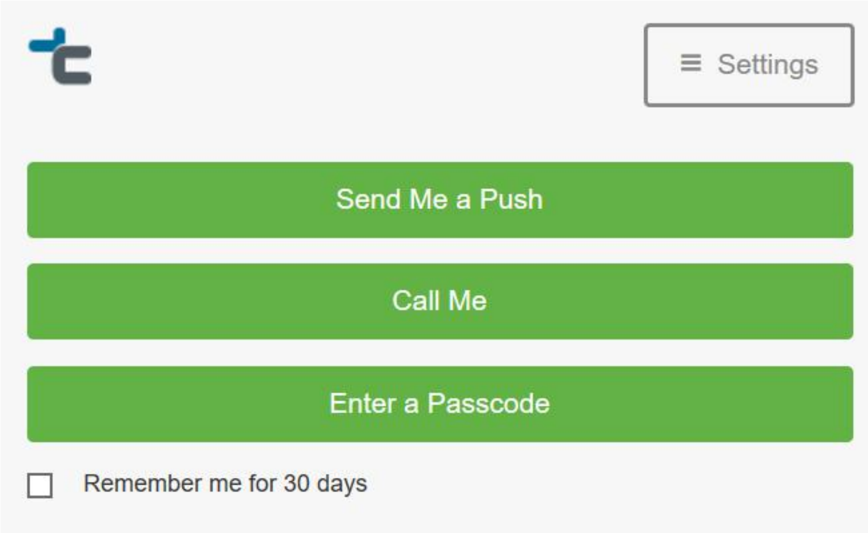
Sign in

john.dietle@ctcomp.com

No account? Create one!

Can't access your account?

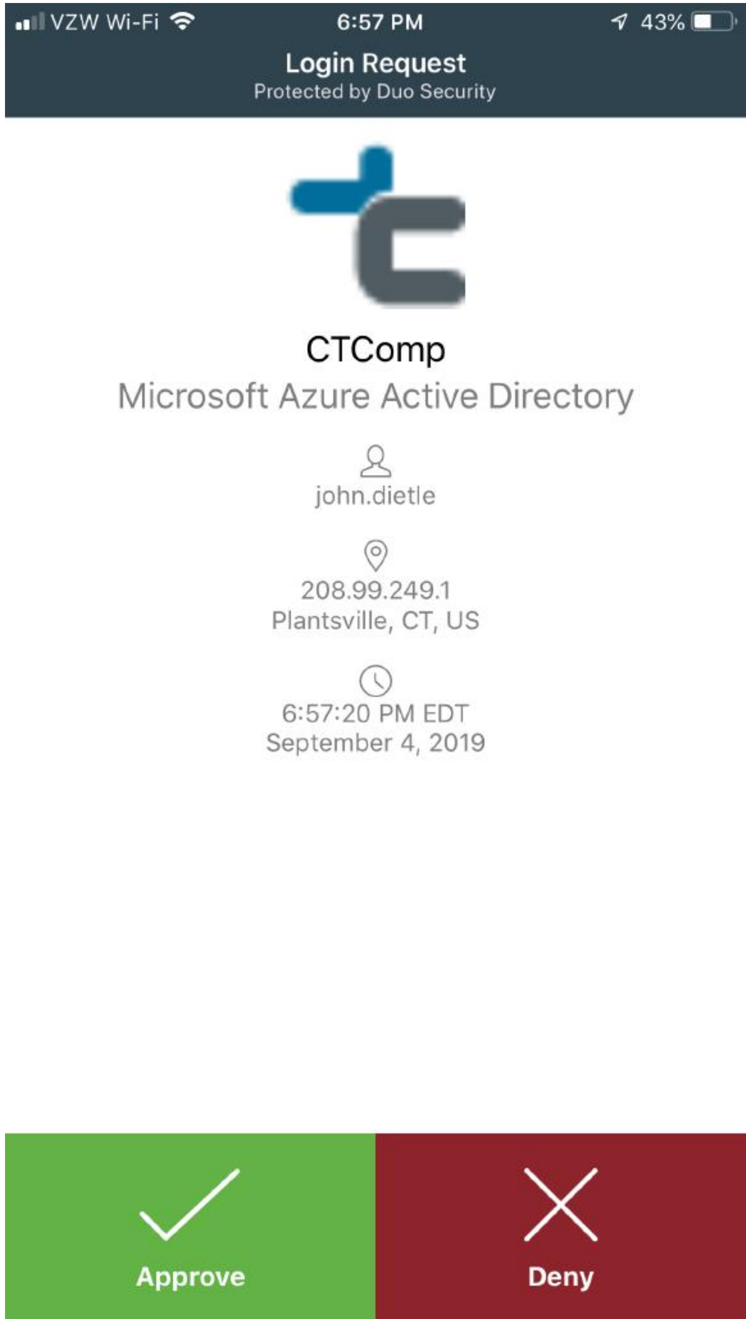
Sign-in options



□ Remember me for 30 days

- Verify users with strong two-factor authentication.

- Set policies to grant or block access attempts by identity or device and based on contextual factors such as user location, network address ranges, biometrics, device security and more.



Login Request

Protected by Duo Security

CTComp

Microsoft Azure Active Directory

john.dietle

208.99.249.1
Plantsville, CT, US

6:57:20 PM EDT
September 4, 2019

User Awareness Training

The 2018 Verizon Data Breach Investigations report revealed that 93% of successful security breaches start with phishing.

Managed Service

We Phish for you quarterly

You get results!

How do I get users from opening email and clicking links?

Do you need to make sure PII is secure?

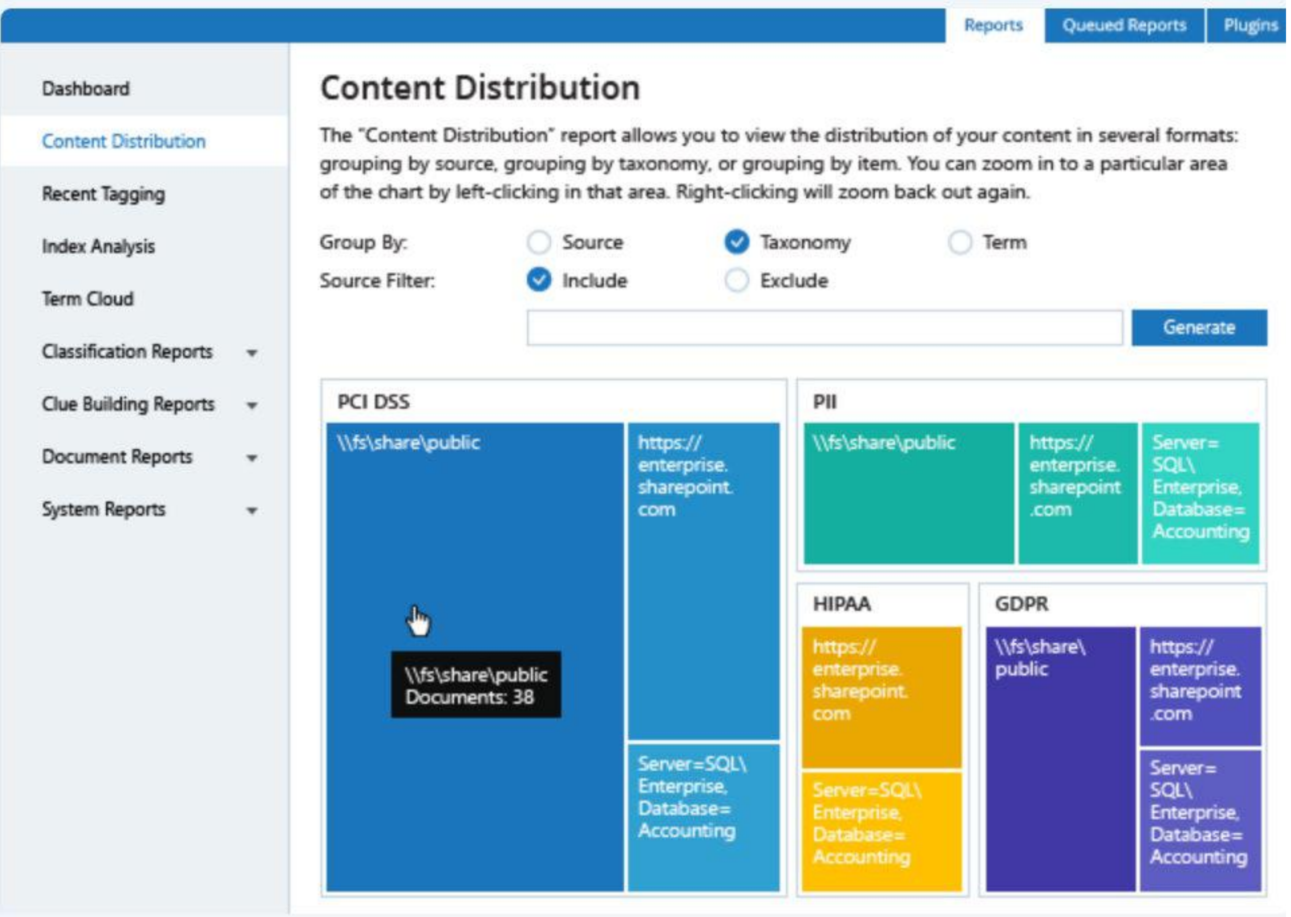
- **<u>Connecticut General Statutes § 36a-701b</u>**, anyone who conducts business in Connecticut and who– in the ordinary course of business– owns, licenses or maintains computerized data that includes personal information is required to disclose a security breach to state residents

- Losing employee or customer PII will impact your company's reputation = loss of sales.
- You must offer for no cost 24 months of credit monitoring for each impacted user.
- Plus Possible Fines and/or Law Suites.

ag.breach@ct.gov

Netwrix Data Classification

Do you know where on your network PII is?



Content Distribution

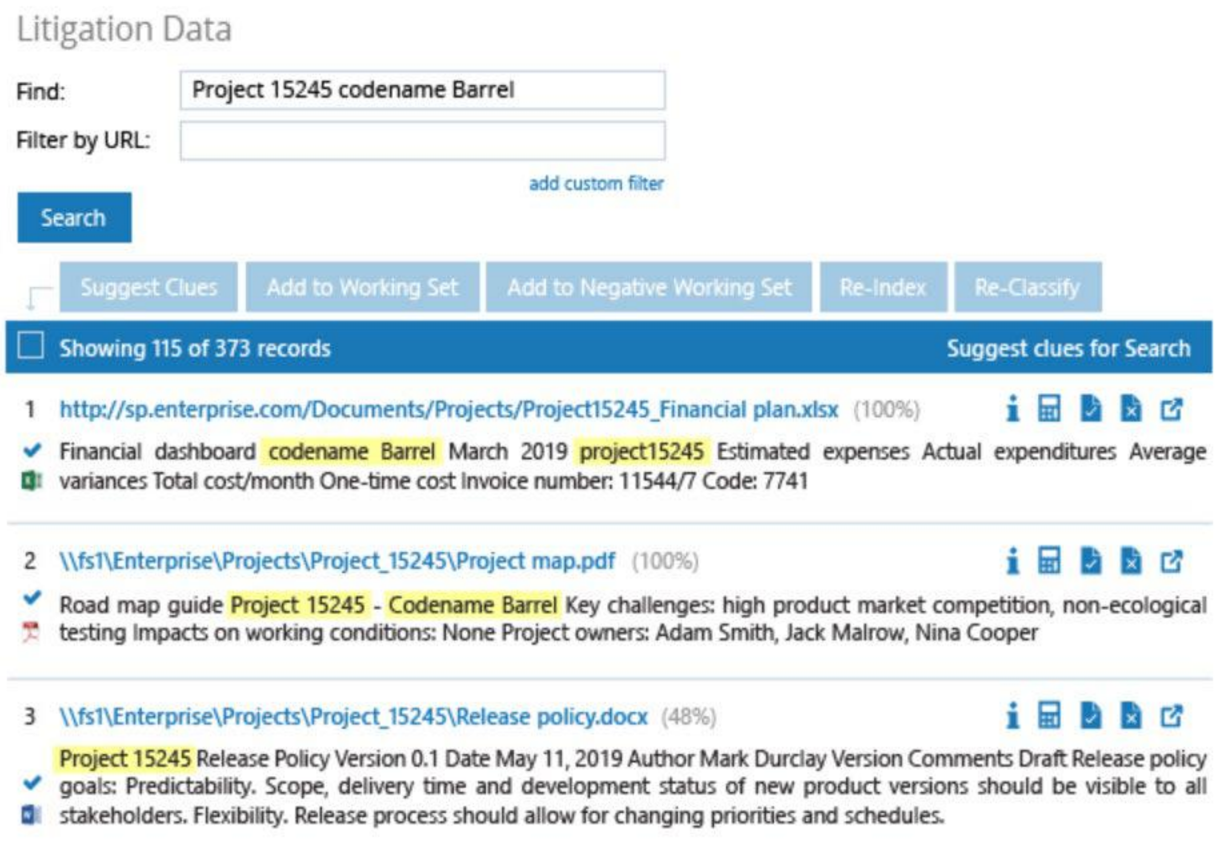
The "Content Distribution" report allows you to view the distribution of your content in several formats: grouping by source, grouping by taxonomy, or grouping by item. You can zoom in to a particular area of the chart by left-clicking in that area. Right-clicking will zoom back out again.

Group By: ○ Source ● Taxonomy ○ Term

Source Filter: ● Include ○ Exclude

Generate

PCI DSS
\\fs\share\public
https://enterprise.sharepoint.com
Server=SQL\Enterprise, Database=Accounting
\\fs\share\public
Documents: 38
PII
\\fs\share\public
https://enterprise.sharepoint.com
Server=SQL\Enterprise, Database=Accounting
HIPAA
https://enterprise.sharepoint.com
Server=SQL\Enterprise, Database=Accounting
GDPR
\\fs\share\public
https://enterprise.sharepoint.com
Server=SQL\Enterprise, Database=Accounting



Litigation Data

Find: Project 15245 codename Barrel

Filter by URL:

add custom filter

Search

Suggest Clues
Add to Working Set
Add to Negative Working Set
Re-Index
Re-Classify

□ Showing 115 of 373 records Suggest clues for Search

1 http://sp.enterprise.com/Documents/Projects/Project15245_Financial plan.xlsx (100%)

✓ Financial dashboard codename Barrel March 2019 project15245 Estimated expenses Actual expenditures Average variances Total cost/month One-time cost Invoice number: 11544/7 Code: 7741

2 \\fs1\Enterprise\Projects\Project_15245\Project map.pdf (100%)

✓ Road map guide Project 15245 - Codename Barrel Key challenges: high product market competition, non-ecological testing Impacts on working conditions: None Project owners: Adam Smith, Jack Malrow, Nina Cooper

3 \\fs1\Enterprise\Projects\Project_15245\Release policy.docx (48%)

✓ Project 15245 Release Policy Version 0.1 Date May 11, 2019 Author Mark Durclay Version Comments Draft Release policy goals: Predictability. Scope, delivery time and development status of new product versions should be visible to all stakeholders. Flexibility. Release process should allow for changing priorities and schedules.

ctcomp

Netwrix Auditor for AD

How do you detect a possible breach?

DETECT INSIDER THREATS

Netwrix Auditor for Active Directory delivers visibility into all security and configuration changes in Active Directory and Group Policy, privilege escalation, anomalous administrator activity, suspicious user logon attempts, and more. This deep insight enables IT departments to more effectively detect security incidents caused by insider actions.

PASS COMPLIANCE AUDITS WITH LESS EFFORT

Netwrix Auditor for Active Directory provides out-of-the-box reports aligned with many compliance regulations, such as PCI DSS, HIPAA, SOX, GLBA, FISMA/NIST, CJIS, GDPR and others. The Interactive Search feature helps you generate custom reports and quickly answer auditors' questions.

INCREASE THE PRODUCTIVITY OF YOUR IT TEAMS

Netwrix Auditor for Active Directory helps minimize service downtime by enabling administrators to quickly uncover the root causes of problems and roll back unwanted changes to their previous states. Furthermore, Netwrix Auditor for Active Directory automates change control and reporting tasks, which increases operational efficiency and quality.

Security Layers

A Menu of Choices

Starters

Trends

Meat & Potatoes

Data

Users

Endpoint

Perimeter

Dessert

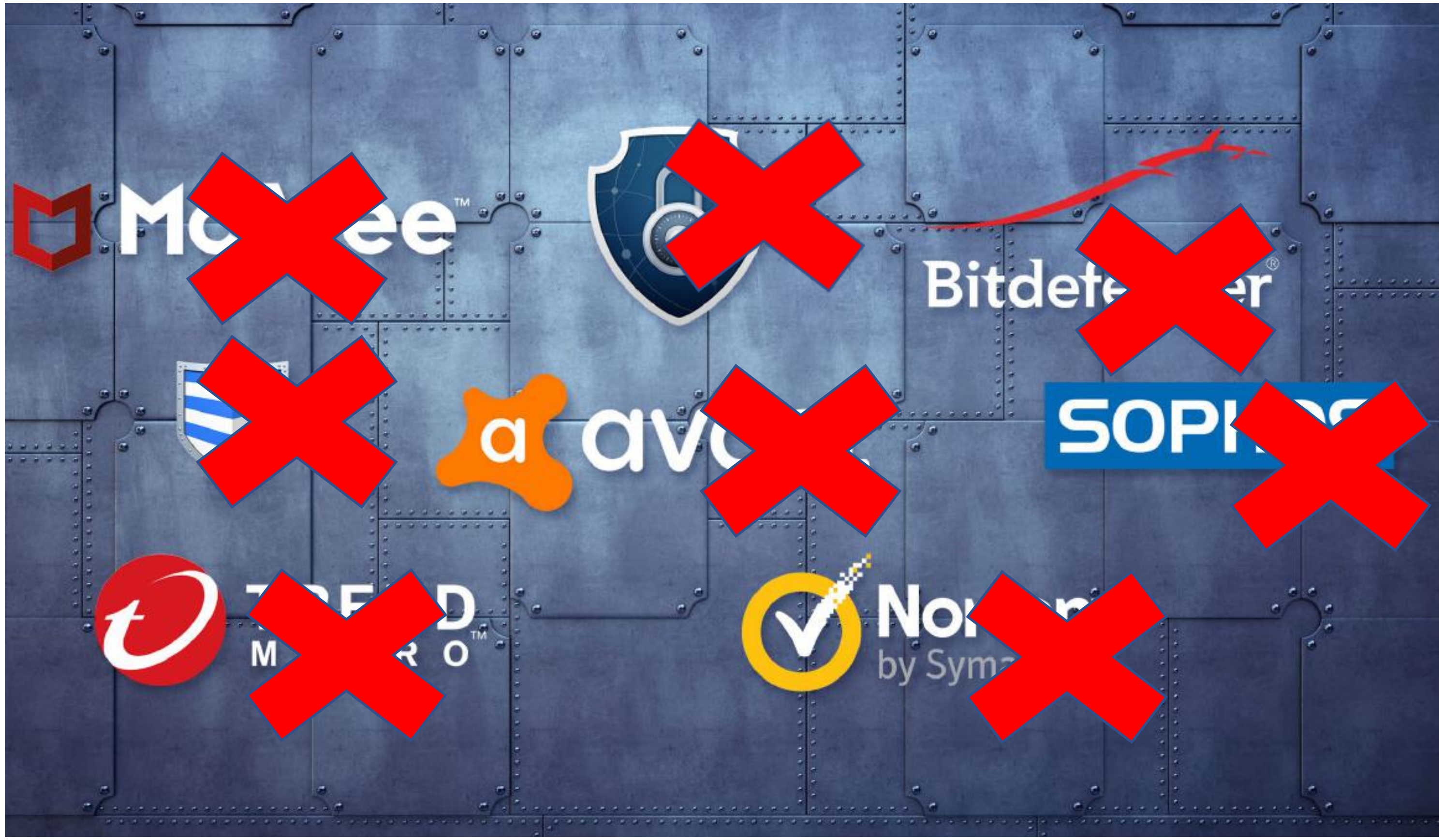
Q&A

Menu

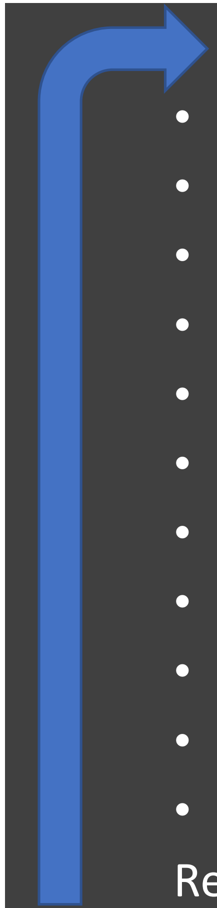
- ***Starters***
  - Trends today
- ***Meat & Potatoes***
  - ***Highlighting Solutions***
    - Data
    - Users
    - Endpoint
    - Perimeter
- ***Dessert***
  - Q&A
  - Dinner

Endpoint Security AV/AM, DNS Highlights

- AV/AM with Webroot
- DNS Security with Umbrella



I run AntiVirus/AntiMalware!



Download signatures

- Install/Update
- Scan device
- Monitor Logs
- Download signatures
- Install /Update
- Scan device
- Monitor Logs
- Download signatures
- Install /Update
- Scan device
- Monitor Logs

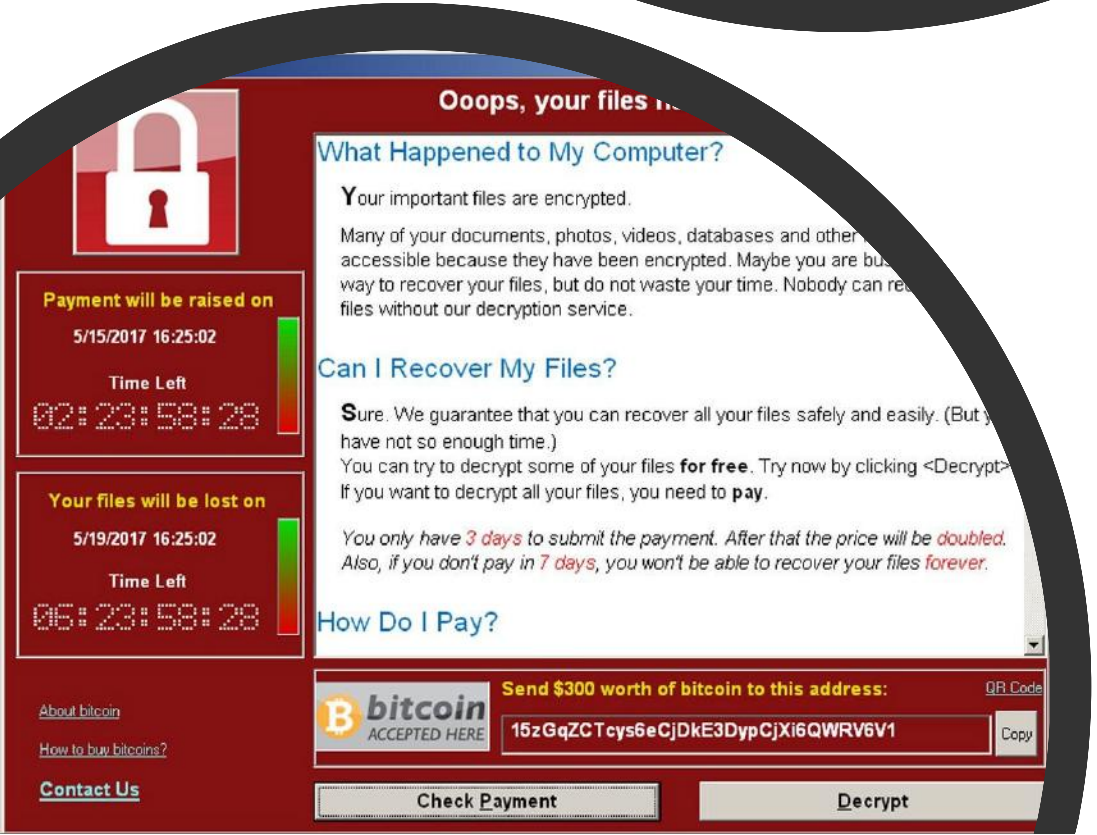
Repeat

Data/Bandwidth, processing repeat! Sometimes a gigabyte files moving to every pc!

Time to move to a next generation AV

- Small footprint 500meg
- PC or MAC
- No downloading signatures to any machines
- Fast Scans
- Cloud based, Instant updates
- Managed Service from CTComp
- We monitor and respond for you

Take a look next time your renewal comes for AV


Ooops, your files h

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other
accessible because they have been encrypted. Maybe you are bu
way to recover your files, but do not waste your time. Nobody can re
files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But y
have not so enough time.)
You can try to decrypt some of your files for free. Try now by clicking <Decrypt>
If you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

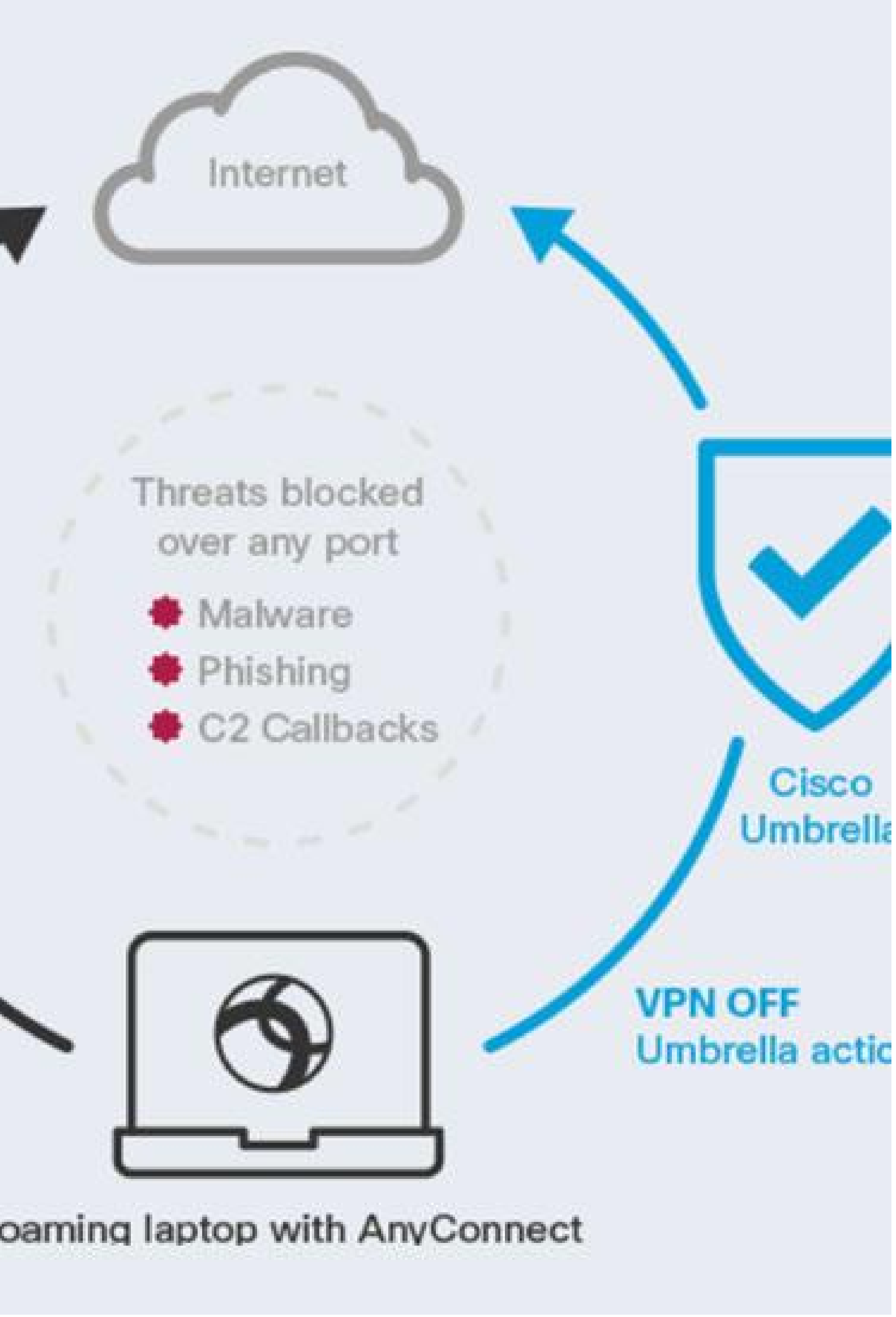
Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28

Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28

Send $300 worth of bitcoin to this address:
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

User clicks a link by mistake and malware!

You now have ransomware running. Then it phones home to get an encryption key and begins encrypting.



DNS Security – Cisco Umbrella

- Enforcement built into the foundation of the internet (DNS)
- Cisco Umbrella uses the internet's infrastructure to block malicious destinations before a connection is ever established.
- Umbrella uses DNS to stop threats over all ports and protocols — even direct-to-IP connections.
- Even if devices become infected in other ways, Umbrella prevents connections to attacker's servers.

ctcomp

Menu

Security Layers

A Menu of Choices

Starters

Trends

Meat & Potatoes

Data

Users

Endpoint

Perimeter

Dessert

Q&A

- ***Starters***
  - Trends today
- ***Meat & Potatoes***
  - ***Highlighting Solutions***
    - Data
    - Users
    - Endpoint
    - Perimeter
- ***Dessert***
  - Q&A
  - Dinner

Perimeter Security Highlights

- Firewall Management for Cisco NGFW and Meraki
- Switch Management and NAC
- Separation of WI-FI – Private/Public
- SIEM & SOC as a Service

Firewall Management
Do you do this?
If not, you are at risk!

CTCOMP Managed Service!

Cisco ASA Firewall

- Device provisioning and deployment
- Device upgrades and patch management
- Maintain policies and ACLs
- Site-to-site and remote access VPN management
- Policy-based control over applications, users and content
- Advanced Malware Protection and Detection
- IPS/IDS Policy and signature management
- Respond to severity 1 and 2 events
- Auditable and accurate change management
- Monthly health reporting
- Backup and recovery
- Manage license renewals

Cisco Meraki MX Firewall

- Checking appliance status and uptime
- Device upgrades and patches
- Check event logs and investigate suspicious activity
- Check Security Center
- Respond to alerts

Switch Management and NAC/ISE

CISCO NAC/Identity Services Engine

- **Policy lifecycle management**: Enforces policies for all operating scenarios without requiring separate products or additional modules.
- **Profiling and visibility**: Recognizes and profiles users and their devices before malicious code can cause damage.
- **Guest networking access**: Manage guests through a customizable, self-service portal that includes guest registration, guest authentication, guest sponsoring, and a guest management portal.
- **Security posture check**: Evaluates security-policy compliance by user type, device type, and operating system.
- **Incidence response**: Mitigates network threats by enforcing security policies that block, isolate, and repair noncompliant machines without administrator attention.
- **Bidirectional integration**: Integrate with other security and network solutions through the open/RESTful API.

Separation of WIFI –Private/Public(Guest)/BYOD
Guests on your network is so 2017! GET THEM OFF!

Can you proactively prevent security incidents?

SIEM & SOC as a Service

Threat hunting

Log ingestion

Intel agnosticism

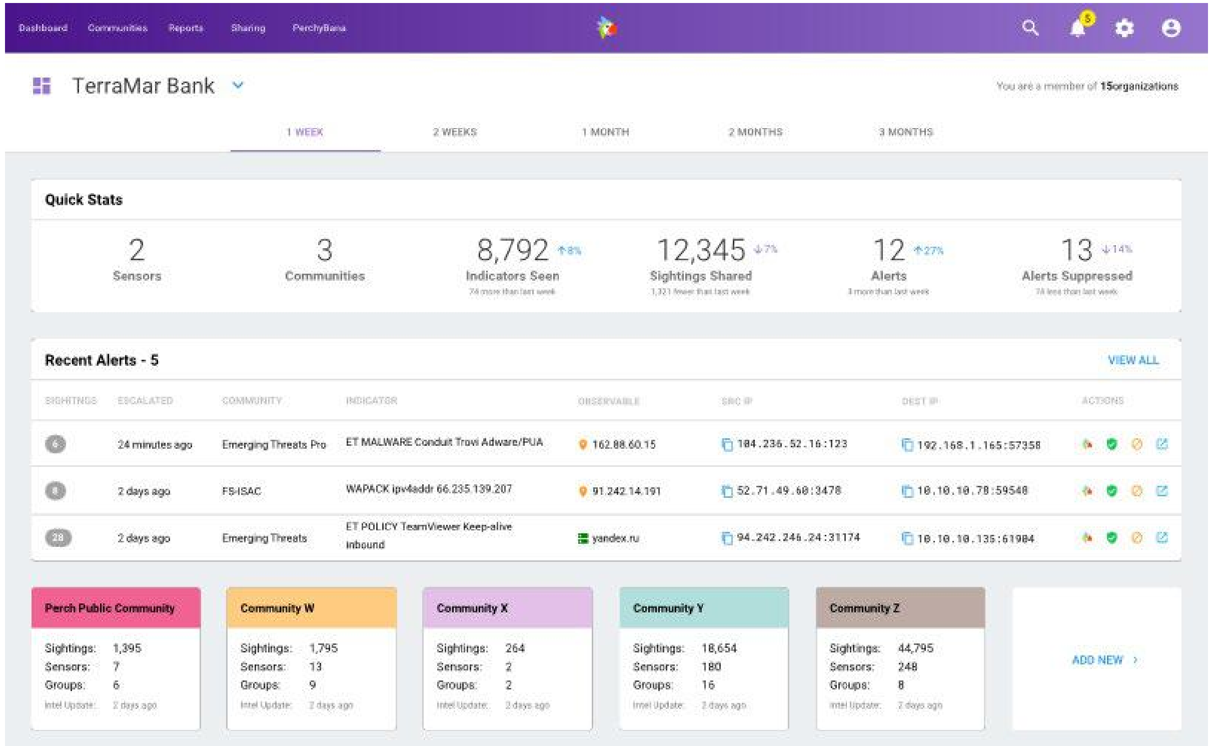
Threat management

Reports

Security Information and Event Management

Security Operations Center

CTComp Managed Service



TerraMar Bank

You are a member of 15organizations

1 WEEK | 2 WEEKS | 1 MONTH | 2 MONTHS | 3 MONTHS

Quick Stats

Sensors	Communities	Indicators Seen	Sightings Shared	Alerts	Alerts Suppressed
2	3	8,792 ↑8%	12,345 ↓7%	12 ↑27%	13 ↓14%
		74 more than last week	1,321 fewer than last week	3 more than last week	74 less than last week

Recent Alerts - 5 VIEW ALL

SIGHTINGS	ESCALATED	COMMUNITY	INDICATOR	OBSERVABLE	SRC IP	DEST IP	ACTIONS
6	24 minutes ago	Emerging Threats Pro	ET MALWARE Conduit Trovi Adware/PUA	162.88.60.15	184.236.52.16:123	192.168.1.165:57358	
8	2 days ago	FS-ISAC	WAPACK ipv4addr 66.235.139.207	91.242.14.191	52.71.49.60:3478	10.10.10.78:59548	
28	2 days ago	Emerging Threats	ET POLICY TeamViewer Keep-alive inbound	yandex.ru	94.242.246.24:31174	10.10.10.135:61984	

	Perch Public Community	Community W	Community X	Community Y	Community Z
Sightings:	1,395	1,795	264	18,654	44,795
Sensors:	7	13	2	180	248
Groups:	6	9	2	16	8
Intel Update:	2 days ago	2 days ago	2 days ago	2 days ago	2 days ago

PERCH

ctcomp

Security Layers

A Menu of Choices

Starters

Trends

Meat & Potatoes

Data

Users

Endpoint

Perimeter

Dessert

Q&A

Menu

- ***Starters***
  - Trends today
- ***Meat & Potatoes***
  - ***Highlighting Solutions***
    - Data
    - Users
    - Endpoint
    - Perimeter
- ***Dessert***
  - Q&A
  - Cocktails & Dinner

Dessert

Q&A

Data

- Backup OnPrem, Offsite, Office365
- Email Security
- ATP, Archiving, Zix

Users

- Monitoring Dark Web - Username/Password
- LastPass
- DUO 2 Factor Authentication
- Netrix Audit & Data Classification
- Security Awareness Training

Endpoint

- AV/AM with Webroot
- DNS Security with Cisco Umbrella

Perimeter Security

- Firewall Management
- Cisco NAC/ISE
- Separation of WIFI –Private/Public/BYOD
- SIEM & SOC as a Service

Hewlett Packard Enterprise

Special thanks to our presenting partners, HP & HPE!

Our partners represented in this seminar!

Microsoft · CISCO · hp · PERCH · veeam · Hewlett Packard Enterprise

WEBROOT Smarter Cybersecurity · zixcorp PREMIER PARTNER · netwrix · StorageCraft · ID AGENT

Thank You for Attending!

Don’t forget your compromise packet!

See your AM tonight.

ctcomp

Starters

- Trends today

Meat & Potatoes

- ***Highlighting Solutions***
  - Data
  - Users
  - Endpoint
  - Perimeter

Dessert

- Q&A

- Cocktails & Dinner!!!