Zimbra Security Overview

September 2022

zimbra®
A SYNACOR PRODUCT

AGENDA

- What is Email Security?
- Key Focus Areas
- Secure your Zimbra Environment

What is Email Security?

"Email security is the process of ensuring the availability, integrity and authenticity of email communications by protecting against the risk of email threats."

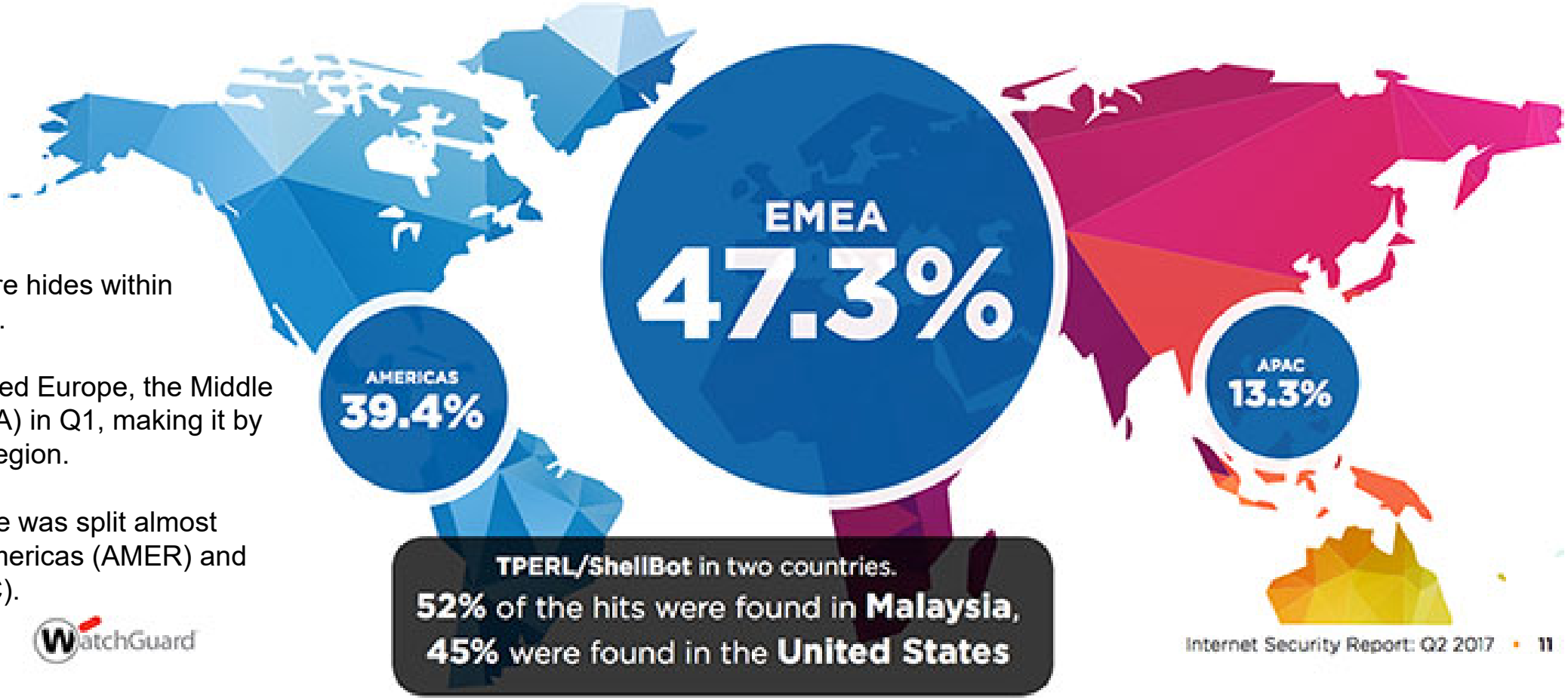
- Phishing Attempts
- Spoofing
- Spam Phishing
- Malware Delivery
- Business Email Compromise (BEC)
- Denial of Service (DoS) attacks

What can Malicious Email do?

60.1 percent of malware hides within encrypted connections.

57% of malware targeted Europe, the Middle East, and Africa (EMEA) in Q1, making it by far the most targeted region.

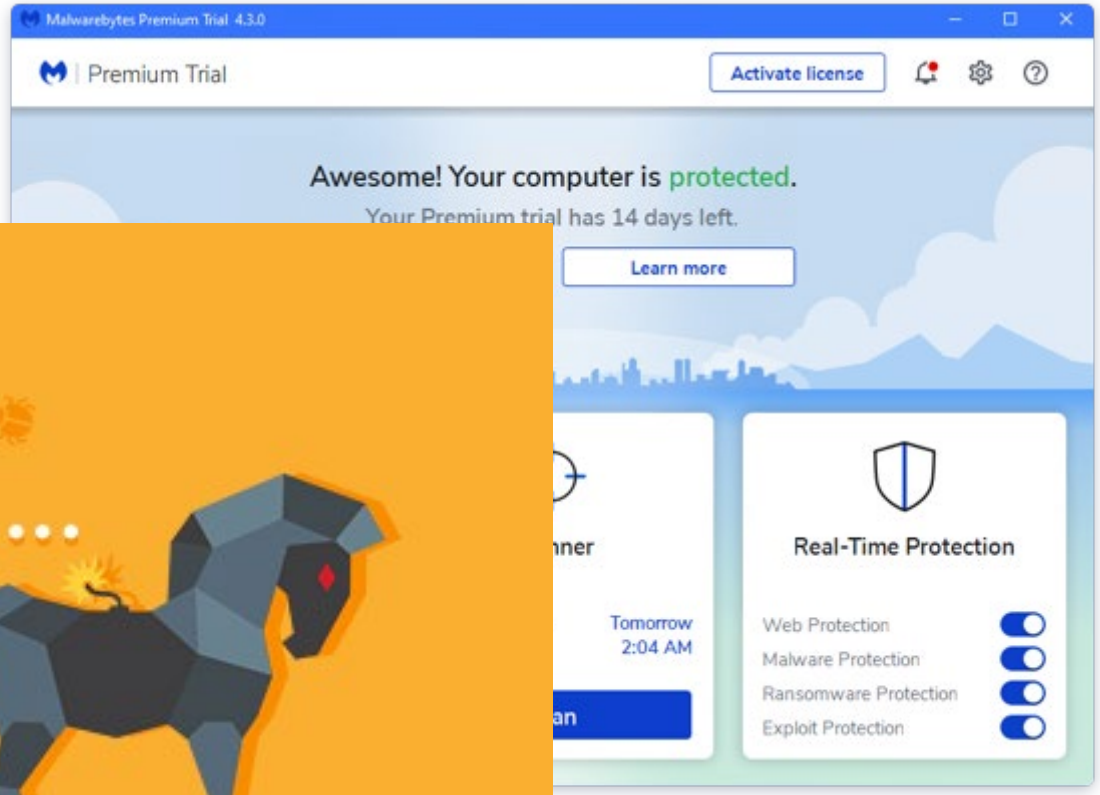
The remaining malware was split almost evenly between the Americas (AMER) and the Asia Pacific (APAC).



Credential Theft: A phishing email can be designed to steal an employee's username and password. These credentials can be used to remotely access services both on-site and in the cloud to perform data theft or other actions.

https://www.watchguard.com/wgrd-resource-center/security-report-q1-2022

What can Malicious Email do?



Trojan Installation: Many malicious emails carry a Trojan designed to create a foothold on the target computer. This malicious file will then collect data and possibly download additional, specialized malware such as keyloggers or ransomware.

Zero-Day Malware: Many email security solutions rely upon signature-based detection of malware. This will not be able to identify and block zero-day attacks before they infect the corporate network.

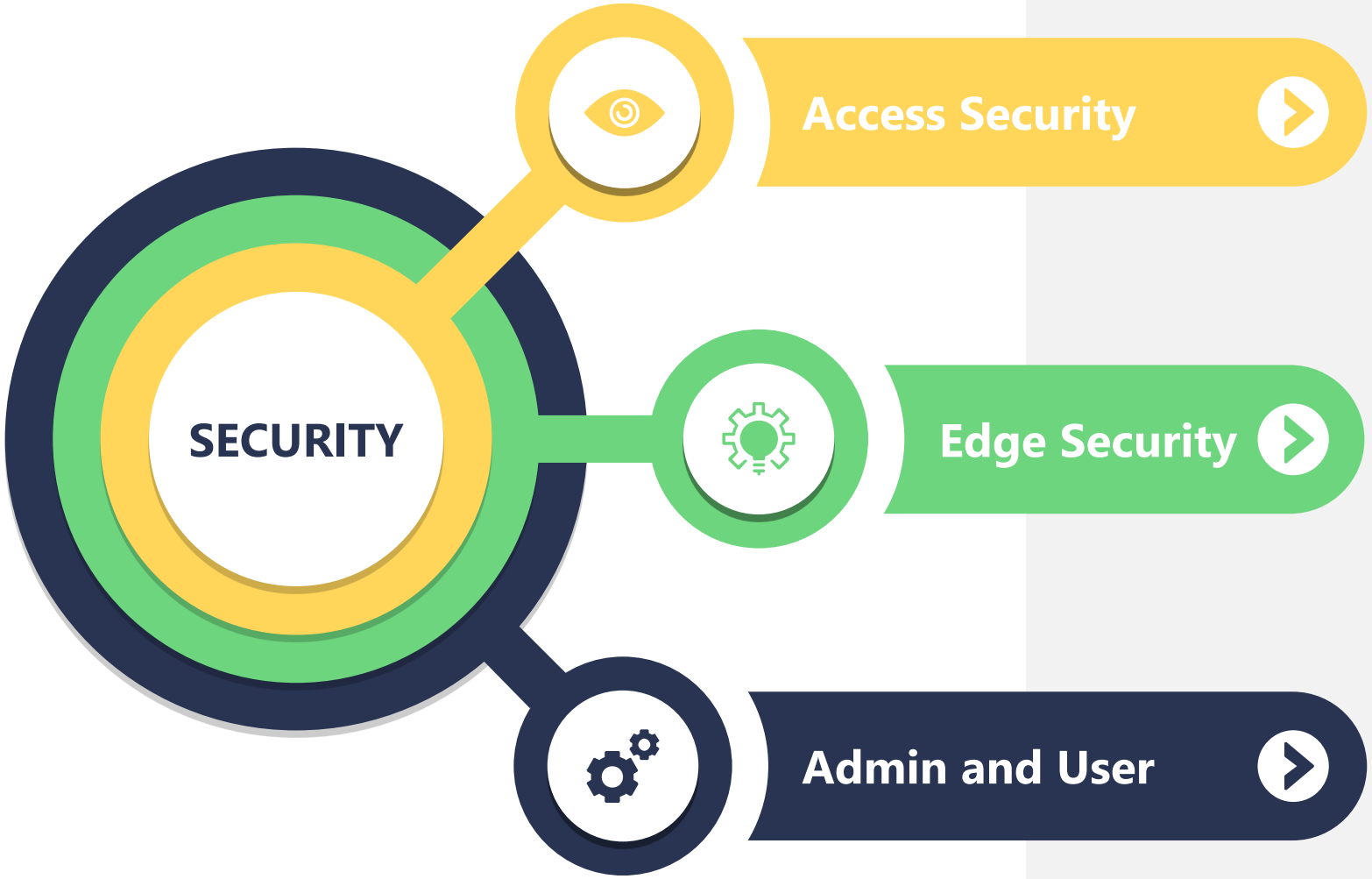
What can Malicious Email do?

Fraudulent Payment: Business Email Compromise (BEC) and similar scams are designed to impersonate a high-level executive within a company. These emails instruct an employee to send a payment to a certain account, pretending that it is for closing a deal or paying a vendor invoice.

What can Malicious Email do?

Ransomware Delivery: Phishing emails are one of the primary delivery mechanisms for ransomware. A ransomware attack encrypts all of the files on infected computers and demands a payment to recover the files. Even if the ransom is paid, there is no guarantee of a complete recovery.

Focus Areas



TLS/SSL, HTTPS

SMTP Layer (SPF, DMARC)

Anti-Spam, Anti-Virus

2FA, SMIME

Password Policies, Mobile Policies, CBPolicyD, Encryption, DosFilter

TLS/SSL and HTTPS

- Configure strong ciphers for your environment
  - Encryption is always evolving - it is recommended to use Mozilla SSL Config generator and identify the right ciphers
  - Configure Zimbra to use the recommended ciphers, and enable TLSv1.2 and TLSv1.3
- Let's Encrypt offers free 90-day certificates – Wildcards are also supported
  - Configure the HTTP headers and use HTTP Strict Transport Security (HSTS)
- Configure the MTA to use only strong TLS ciphers
- Detailed settings is documented here - https://wiki.zimbra.com/wiki/Cipher_suites

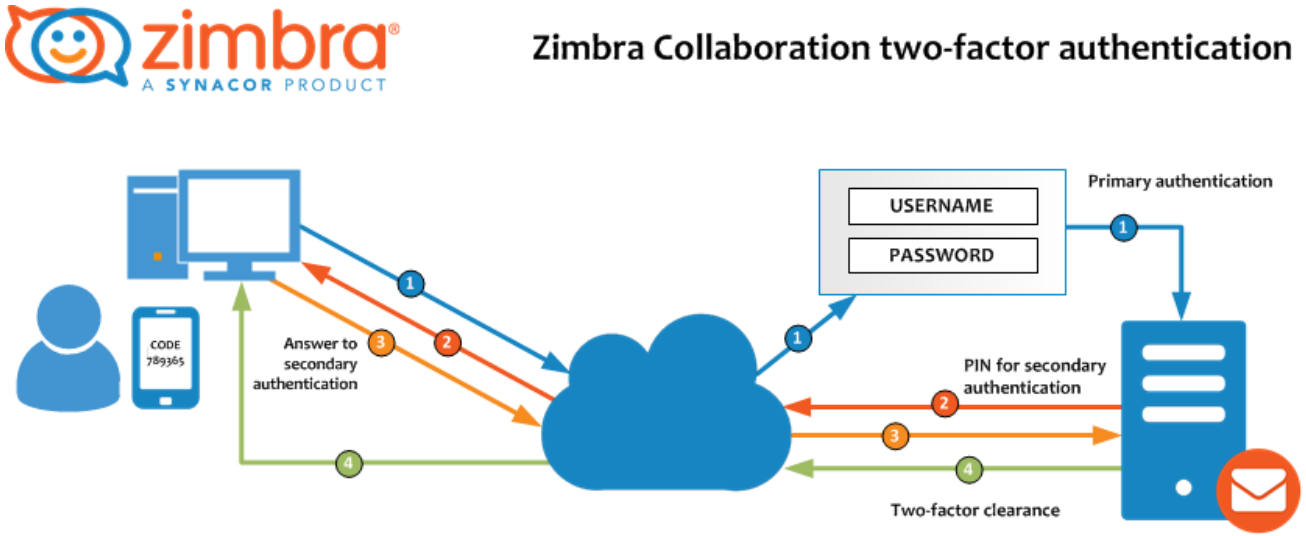
SSL/TLS

Multi-Factor Authentication

- **Strong Passwords:** For users, it is important that any passwords are complex and not easy to guess. It's often recommended that users have passwords with a combination of letter, numbers and symbols.
- **Two Factor Auth:** Zimbra 2FA provides identification of users with the combination of two different components.

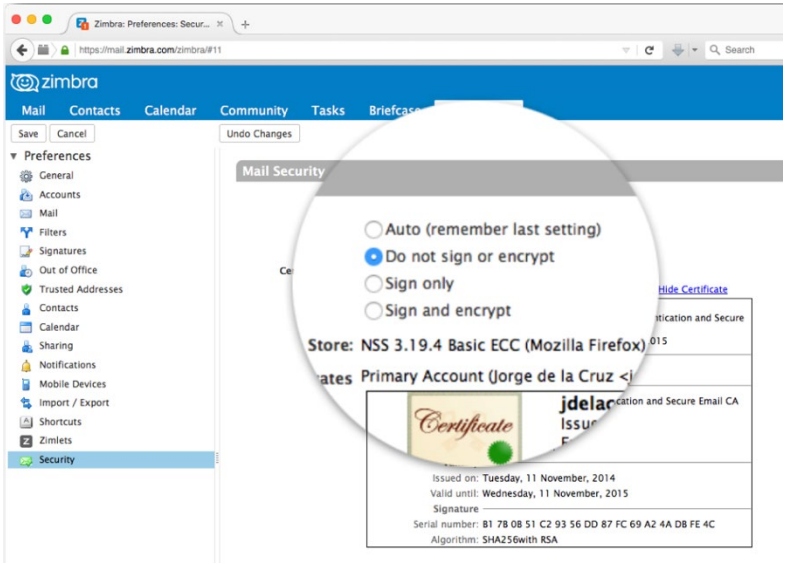
Key Benefits:

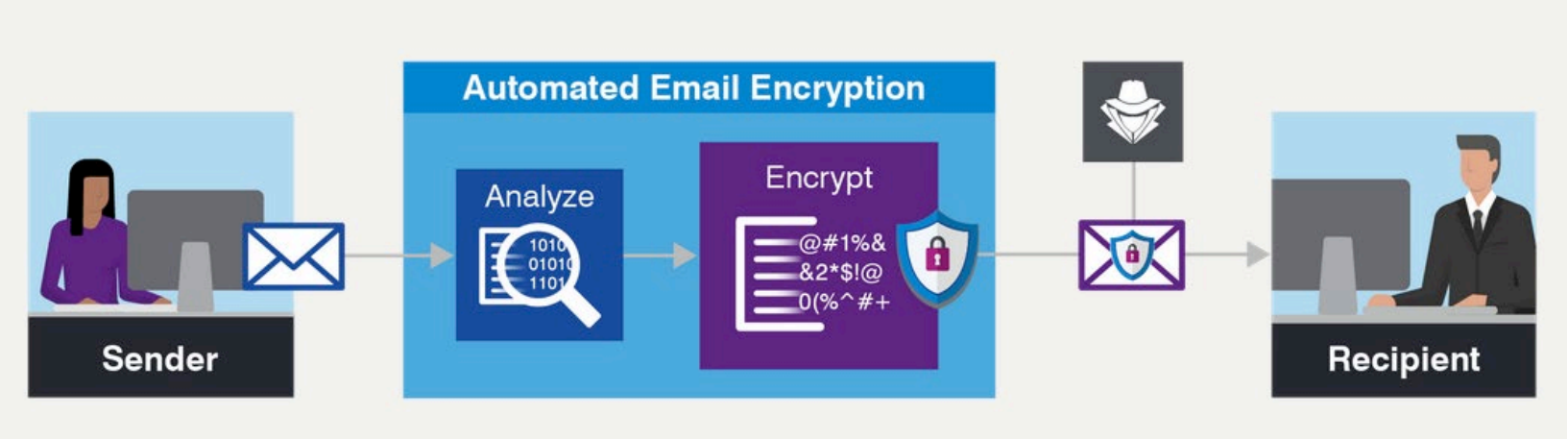
- Easy to setup, easy to be protected
- One-time codes, emergency codes for exceptional situations
- Application codes for legacy applications
- TOTP Applications for Android, iOS and Windows OS
- Zimbra 2FA for Zimbra Desktop & Outlook

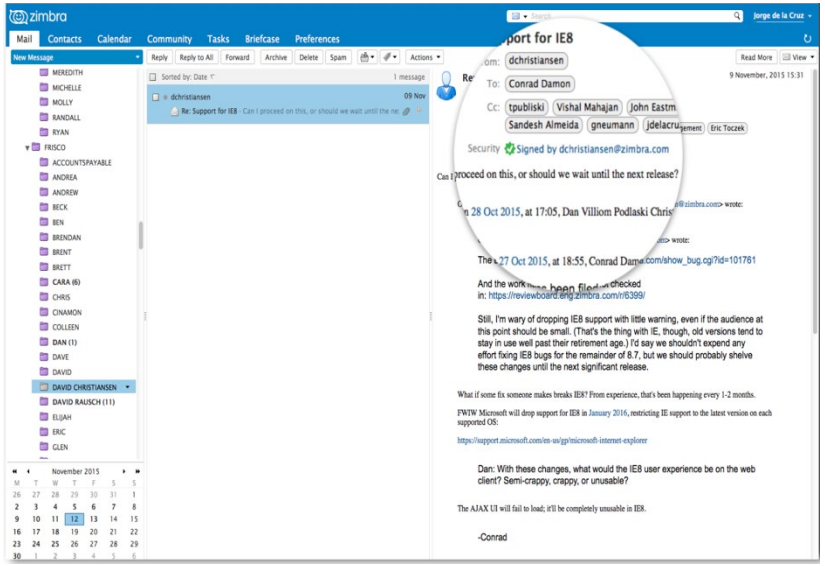


Support for S/MIME

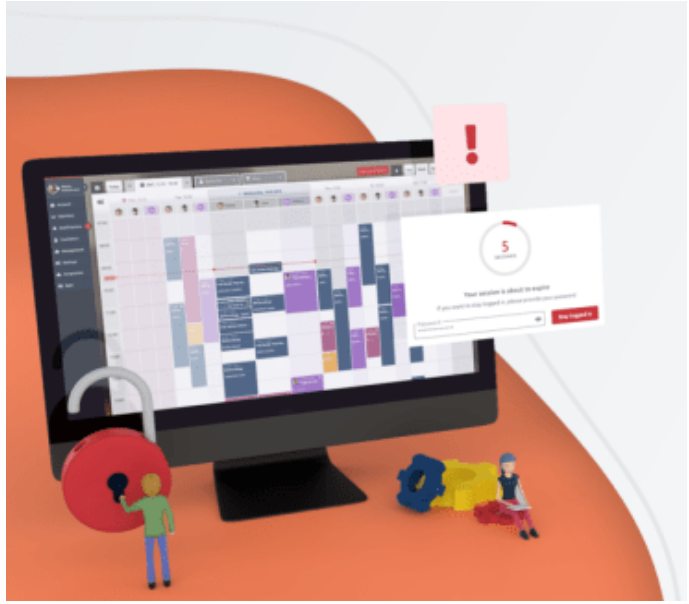
- Zimbra provides an easier way to work with S/MIME.
- Once S/MIME is enabled in the COS (Class-of-Service), the user can see a new option in Settings called Security.
- Users can *Sign Only*, *Sign and Encrypt*, or use the Auto mode, which will remember the latest used option.







Session Time Out



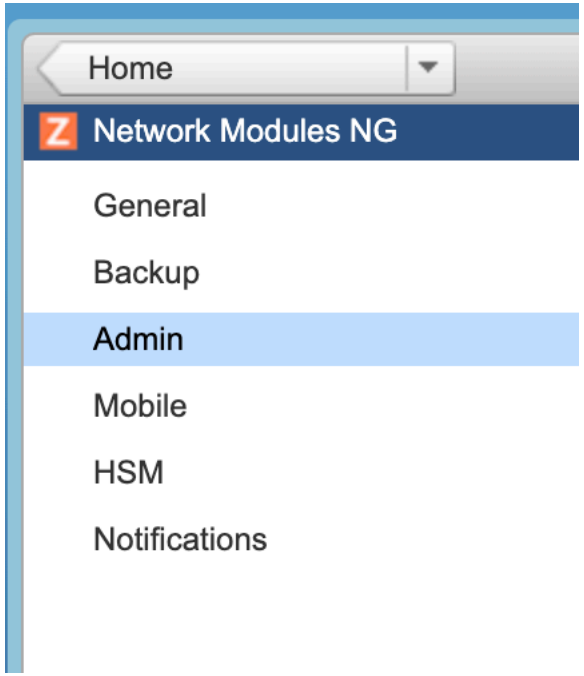
- User sessions should be set to expire if there is no activity
- Setting limits for auth token lifetime and session idle timeout limits exposure of information on shared machines. Applicable to API's also.
- The ***Session Idle Timeout*** determines how long a user session remains active if there is no activity on the Zimbra Web Client.
- If there is no activity within the configured time, the user is logged out of the Zimbra Web Client. The default is unlimited.

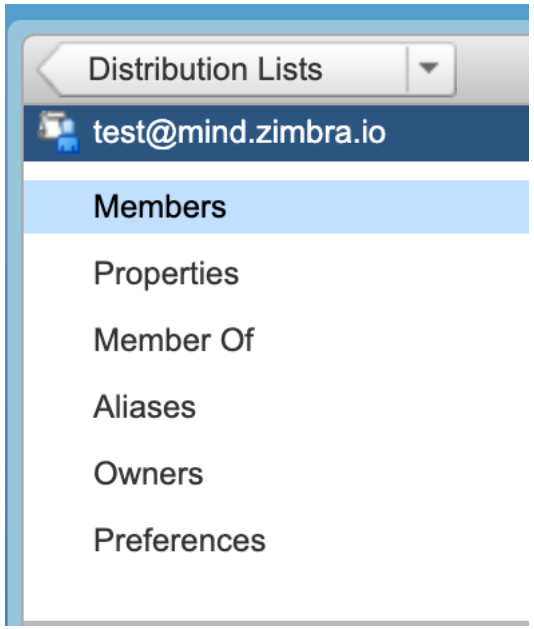
Admin Console→ **Configure** → **Class of Service** → **COS** → **Advanced** → **Timeout Policy**

Timeout Policy		
Admin console auth token lifetime:*	12	hours
Auth token lifetime:*	2	days
Session idle timeout:	never	days
Visibility lifetime in dumpster for end user:	30	days

Delegated Access

- The global administrator can create different delegated administrator roles e.g.
  - Rights to manage one or more distribution lists or
  - Reset forgotten passwords
  - To having domain administration rights on one or more domains.
  - Distribution list administrators



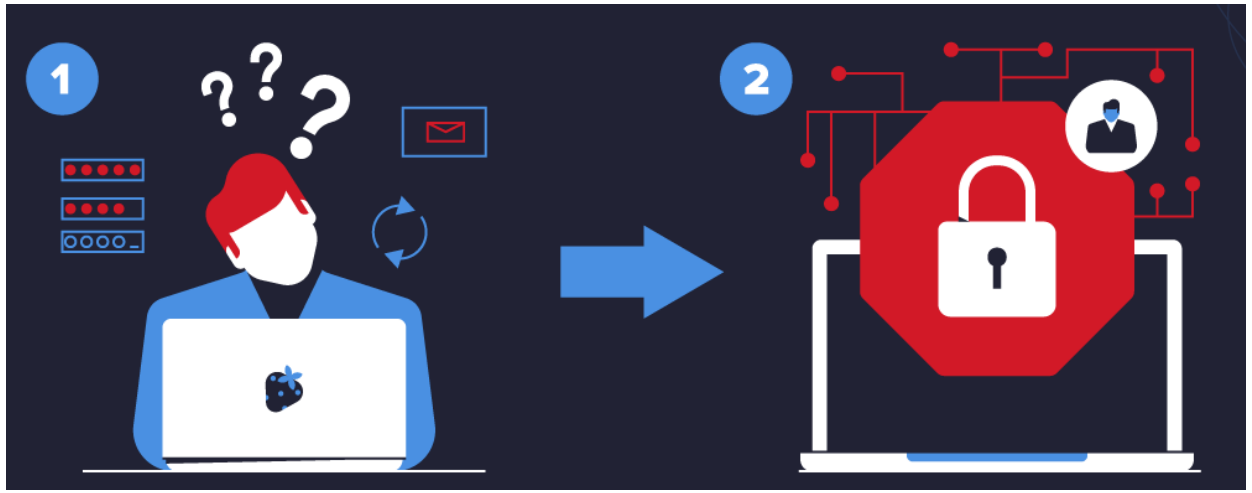


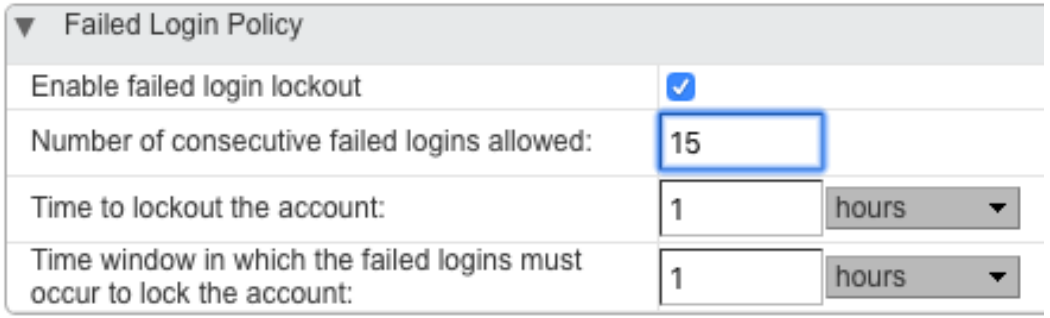
Mobile Policies - ActiveSync

- Zimbra provides the latest version of Exchange ActiveSync (EAS), so your users can sync their mailbox, calendar, contacts and tasks to their mobile devices. They can also connect to Microsoft Outlook using EAS.
- Improved Security Controls
  - The admin/user can remotely wipe out a mobile device in case the device is lost, or the user has left the organization
  - The new Allow/Block/Quarantine (ABQ) feature allows granular control of which mobile devices can connect to the server. This pre-emptive security feature lets the Zimbra admin keep track of all mobile devices in their network.

DoSFilter and Failed Login Lockout Policy

- **Denial of Service Filter** is a mechanism to throttle or block IP addresses that have a repeated number of failed logins to your Zimbra system.
- Natively supports Denial of Service filter to prevent throttling from clients sending large number of emails
- Configure the Failed Login Lockout policy that will put a mailbox in Locked Out mode, before a brute force attack is successful.
- The two together can improve system security and protect legitimate users, but only if configured appropriately.

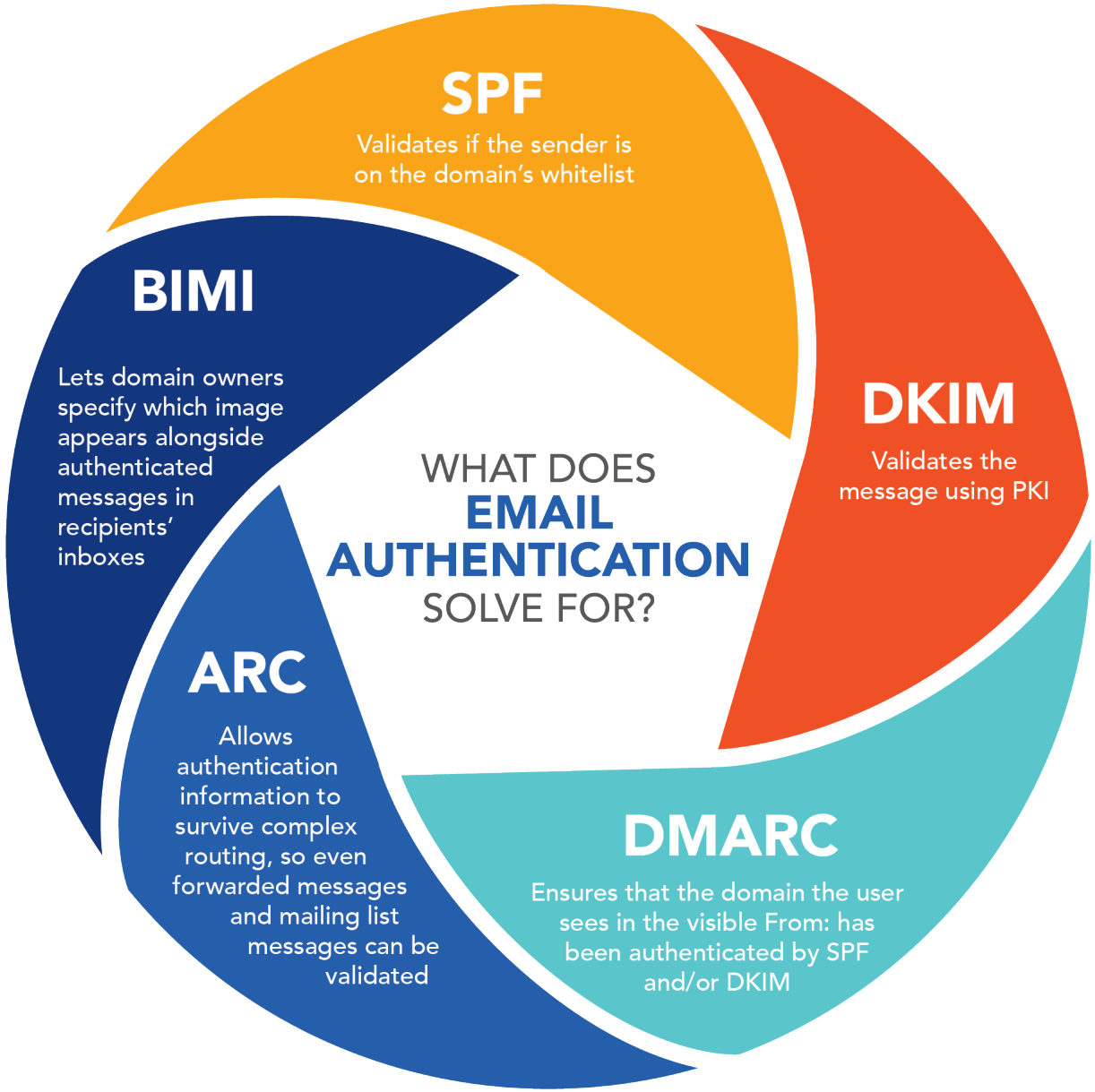




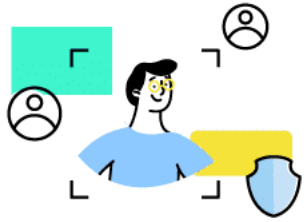
Zimbra will lock the account very quickly in order to prevent what looks like a brute force attack

SPF, DKIM & DMARC

- SPF: Sender Policy Framework (SPF) is an email validation system, designed to prevent unwanted emails using a spoofing system. To check this common security problem, SPF going to verify the source IP of the email and compare it with a DNS TXT record with a SPF content.
- DKIM: DomainKeys Identified Mail (DKIM), is a method to associate the domain name and the email, allowing to a person or company assume the responsibility of the email.
- DMARC: Domain-based Message Authentication, Reporting & Conformance, is a technical specification created by a group of organizations that want to help reduce the potential for email-based abuse by solving a couple of long-standing operational, deployment, and reporting issues related to email authentication protocols. DMARC standardizes how email receivers perform email authentication using the well-known SPF and DKIM mechanisms. This means that senders will experience consistent authentication results for their messages at other email receiver implementing DMARC.



Support for DKIM, DMARC, SPF



SPF

- IP address authorization check

MUST-HAVE

USE IT TO:

- Secure yourself from spoofing and phishing

DKIM

- Message authenticity verification

MUST-HAVE

USE IT TO:

- Prevent possible message modifications
- Secure yourself from spam attacks

DMARC

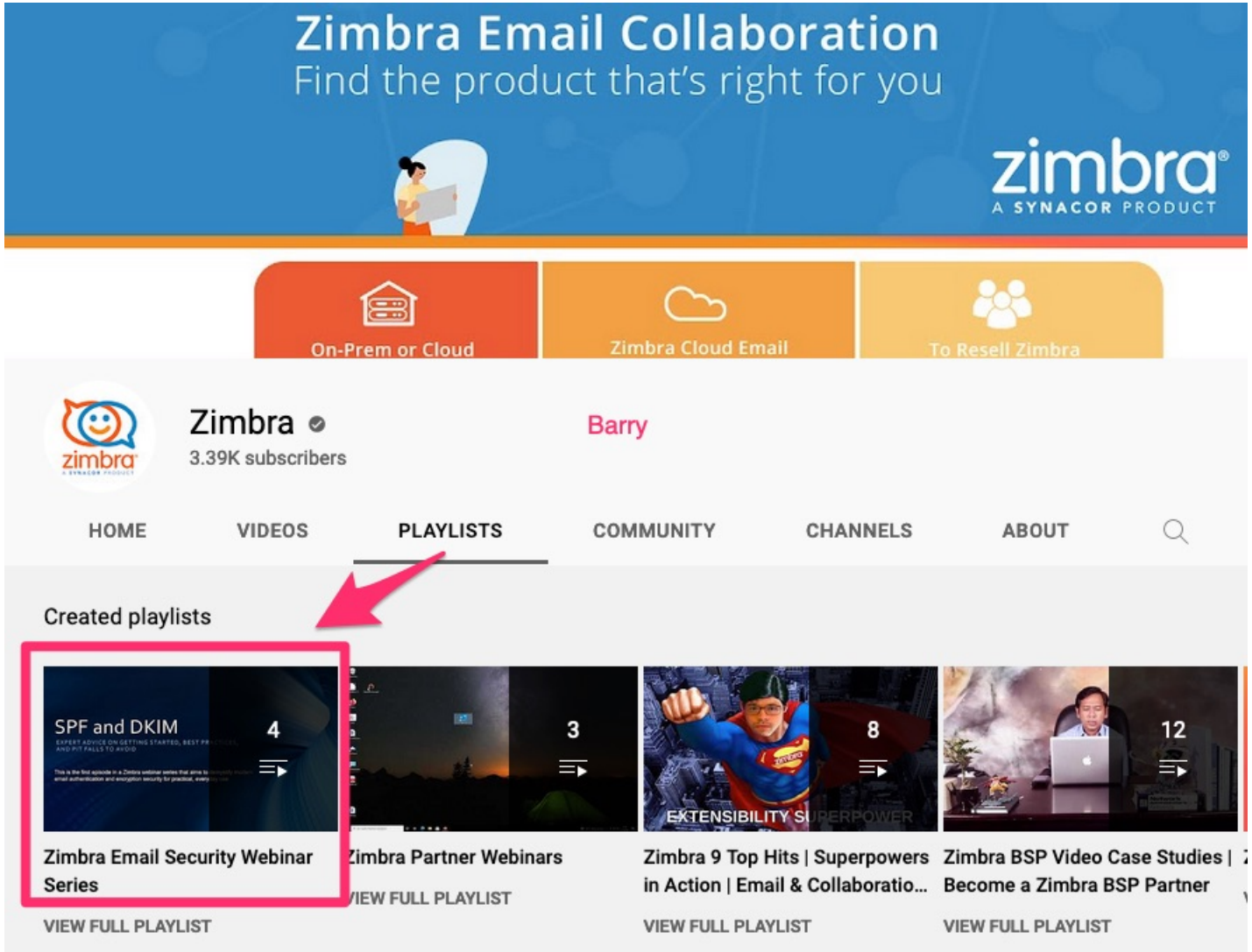
- Additional layers of security

HIGHLY RECOMMENDED

USE IT TO:

- Improve email fraud security
- Set up own domain authentication procedure

Email Security …



Zimbra's Barry de Graaff and Randy Leiker from Skyway Networks team up for this webinar series focused on Email Security.

Hands-on webinars includes practical how-to information and best practices to help you maximize Zimbra.

Zimbra – Fail2Ban and CBPolicyD

- Intrusion prevention software framework designed to prevent against brute-force attacks (especially on SMTP)
- Fail2ban operates by monitoring for selected entries
- Most commonly, this is used to block selected IP addresses that are trying to breach the system's security.
- It can ban any host IP address that makes too many login attempts or performs any other unwanted action within a time frame defined by the administrator
- Fail2ban can perform multiple actions whenever an abusive IP address is detected, update ***iptables*** or firewall rules, to reject an abuser's IP address; email notifications; or any user-defined action.

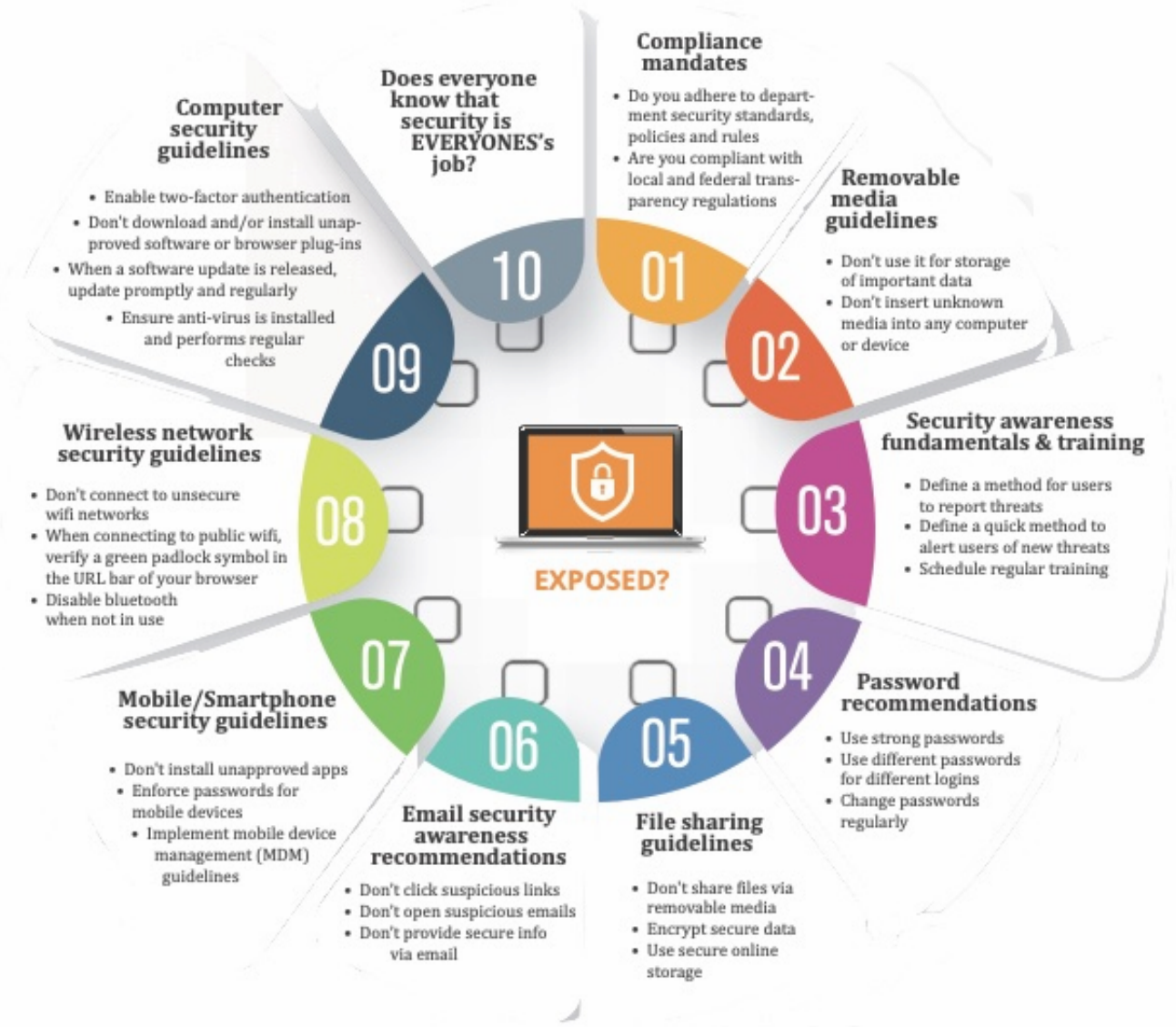
https://blog.zimbra.com/2022/08/configuring-fail2ban-on-zimbra/

- CBPolicyD is a policy daemon server integrated with Zimbra to enable restrictions
- Supported CBPolicyD features:
  - Access Control: Simple access control on email - includes holding, rejecting, discarding (dropping), filtering or redirecting.
  - HELO/EHLO Checks: SMTP transaction checks
  - SPF Checks: SPF based checks to verify that incoming messages
  - Greylisting: Anti-Spam technology that is used to detect if the sending server of a message is RFC compliant.
  - Quotas: message count and message cumulative size over a user-defined period of time.
  - Accounting: Message count and message cumulative size over fixed period of time - Counters can be based (Tracked) on sender, recipient or sender IP.

https://wiki.zimbra.com/wiki/CBPolicyD_Management

Conclusion

- Zimbra team strives to keep all the core and dependent packages upgraded to the latest versions -
  - OpenSSL
  - Apache and PHP
  - Open JDK
  - Nginx and other packages
- Keep a watch on the Zimbra Security Centre page (https://wiki.zimbra.com/wiki/Security_Center)
- Zimbra continues to work with 3rd party auditors and security organizations to validate the product on routine basis
- Use recommended 3rd party tools along with strict policies for password, mobiles and other access
- Educate end-users so they recognise phishing and other types of attacks



always try and keep your environment updated to the latest product release and patch

Thank You!

Piyush Mathur

Piyush.Mathur@synacor.com

zimbra®
A SYNACOR PRODUCT