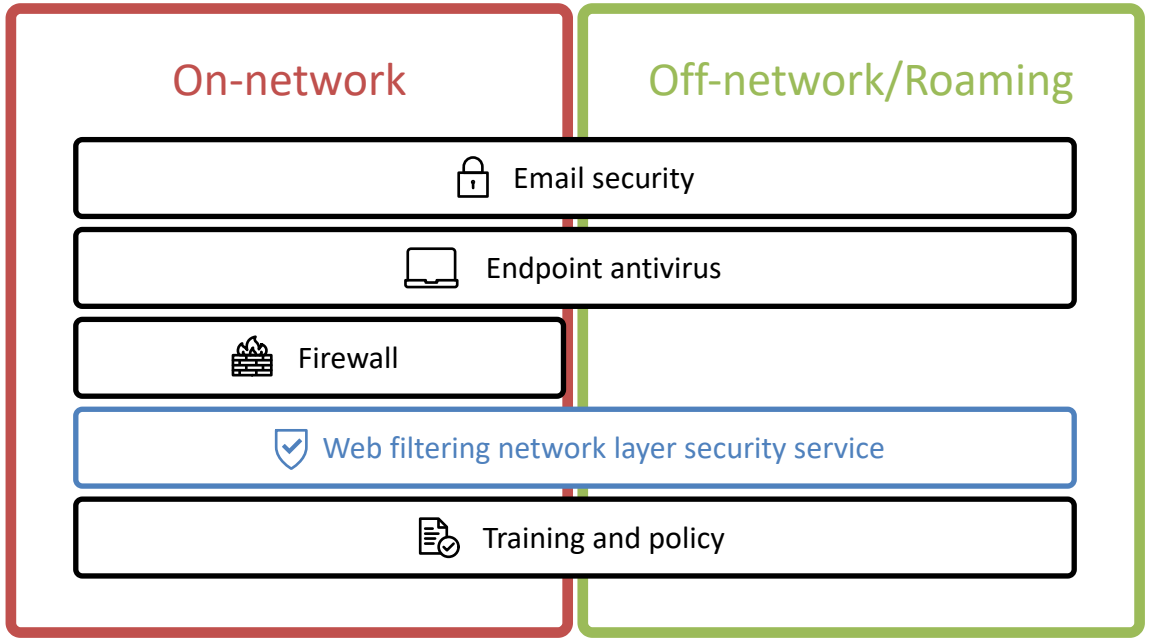
Security is about managing risk through layers



What are these layers?

- Webroot DNS web filtering
- Cisco AMP – Advanced Malware Detection
- Cisco IDS – Intrusion Detection System
- Webroot SecureAnywhere Endpoint protection
- Email Phishing attack awareness

Web Filtering

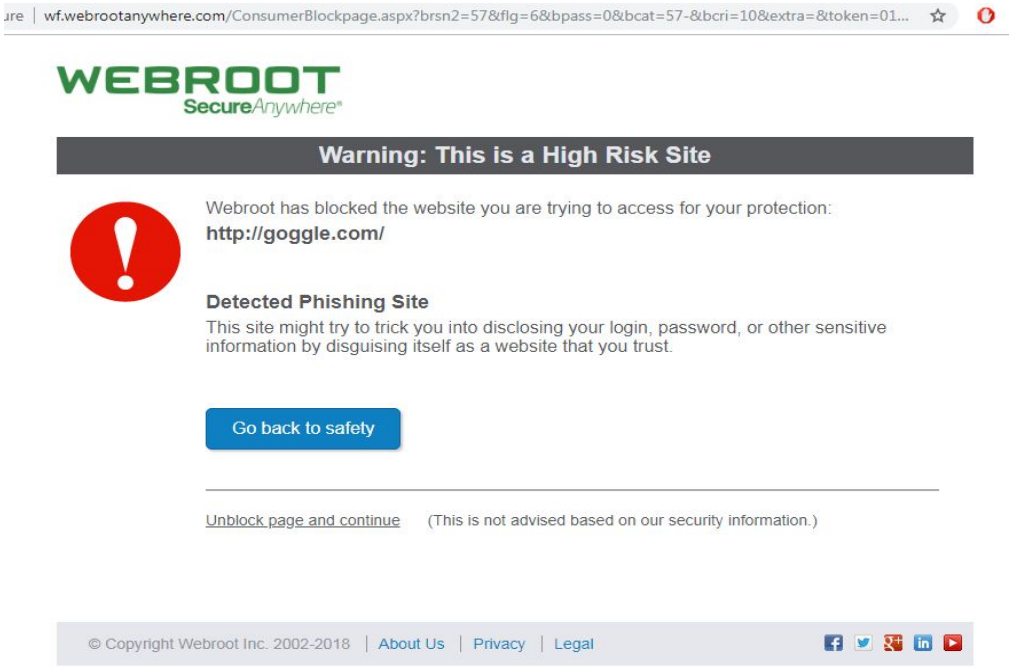
- The Internet is a dirty dangerous place
- How just browsing can cause problems
- How do we shape the Internet?

Webroot DNS security

- Uses specific DNS servers that filter bad sites
- Policies are created for your company
- Can be set up to safeguard guest wireless access
- Agent based on network computers
- Will prevent access to bad sites and alert user

pcgit
Advanced IT Support

Webroot Alert!



Cisco AMP service

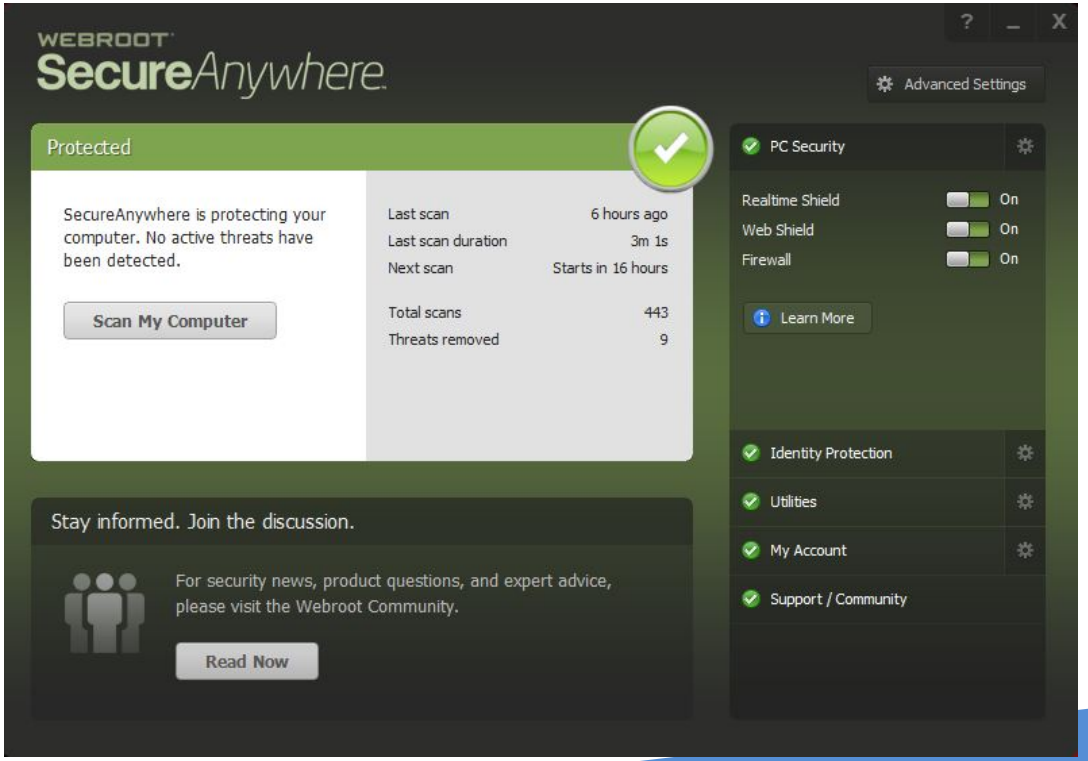
- Uses the Firepower service installed on Cisco Firewalls
- Connects to Cisco Talos Threat Intelligence Group
- Scans traffic through firewall for malware
- Policies can be set to allow or deny specific traffic
- Immediate edge detection using Cisco devices you already have

Cisco IDS service

- Also uses Firepower to leverage your existing Cisco device
- Scans traffic accessing your firewall for breach attempts
- Alerting can be set to warn us and you when your gateway is under attack
- Can shut down ports under attack until resources are hardened

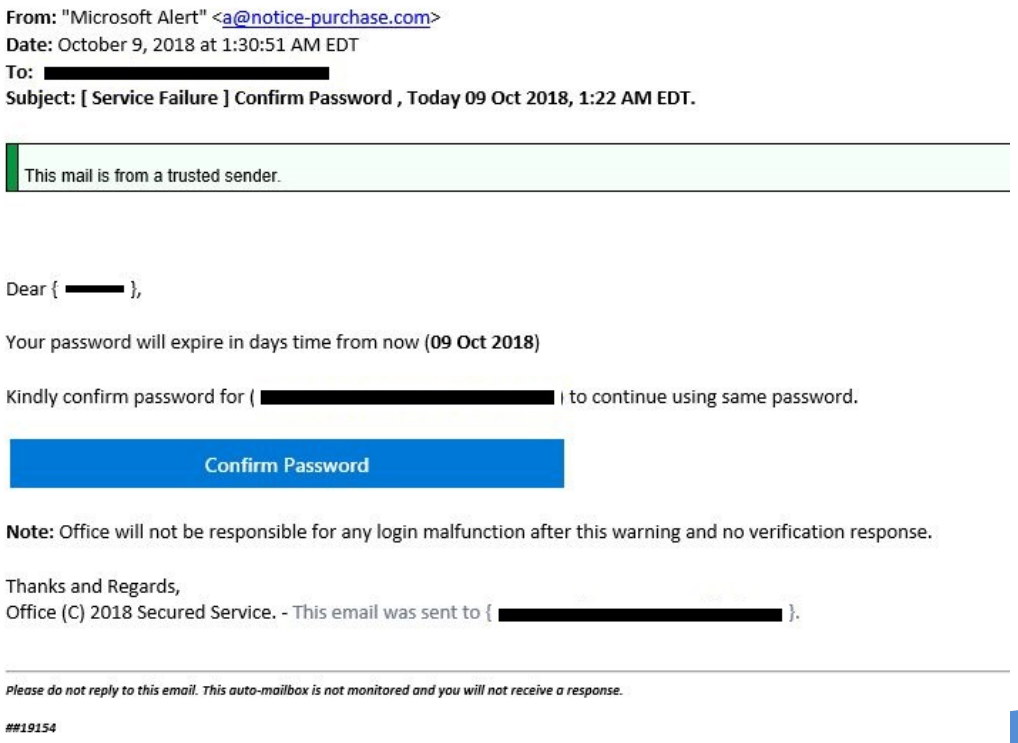
Webroot SecureAnywhere

- Agent installed on servers and desktops
- Centrally managed by Us
- Full suite of protections at the desktop level
- Viruses and Malware
- Web filtering
- Firewall
- Scans and alerting



Email Phishing example

- Email appears to be from Microsoft
- Is directly addressed to user
- They are aware the user has an account with the service referenced
- Button leads to a site that is not a Microsoft site but looks exactly like one
- Button can be “Hovered” to see its web address
- If the site is not of the service company – don’t go there!



From: "Microsoft Alert" <a@notice-purchase.com>
Date: October 9, 2018 at 1:30:51 AM EDT
To: [redacted]
Subject: [Service Failure] Confirm Password , Today 09 Oct 2018, 1:22 AM EDT.

This mail is from a trusted sender.

Dear { [redacted] },

Your password will expire in days time from now (**09 Oct 2018**)

Kindly confirm password for ([redacted]) to continue using same password.

Confirm Password

Note: Office will not be responsible for any login malfunction after this warning and no verification response.

Thanks and Regards,
Office (C) 2018 Secured Service. - This email was sent to { [redacted] }.

Please do not reply to this email. This auto-mailbox is not monitored and you will not receive a response.

##19154

Blackmail Phishing

- **Email appears to know details about you**
- **Describes illicit behavior by you**
- **Designed to scare you using technology terms that cause concern**
- **Attempts to leverage the seedier side of the internets overall metrics**
- **Threatens via blackmail that this information will be released unless a payment is made**

It seems that, marine, is your password. You may not know me and you are probably wondering why you are getting this e-mail, right?

Actually, I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. After that, my software program obtained all of your contacts from your Messenger, FB, as well as email.

What did I do?

I backuped phone. All the photo, video and contacts.
I created a double-screen video, 1st part shows the video you were watching (you've got a good taste haha ...), and 2nd part shows the recording of your web cam.

What exactly should you do?

Well, I think, $800 is a fair price for our little secret. You will make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address: 18sYDUVZ6kTkiNJrWTPFBZ7cCCxJR6TKae
(It is cAsE sensitive, so you should copy and paste it)

Important:
You have one day in order to make the payment. (I have a unique pixel in this e mail, and at this moment I know that you have read through this email message). If I do not get the BitCoins, I will certainly send out your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I receive the payment - I'll destroy the video immediately. If you need evidence, reply with "Yes!" and I'll send out your video recording to