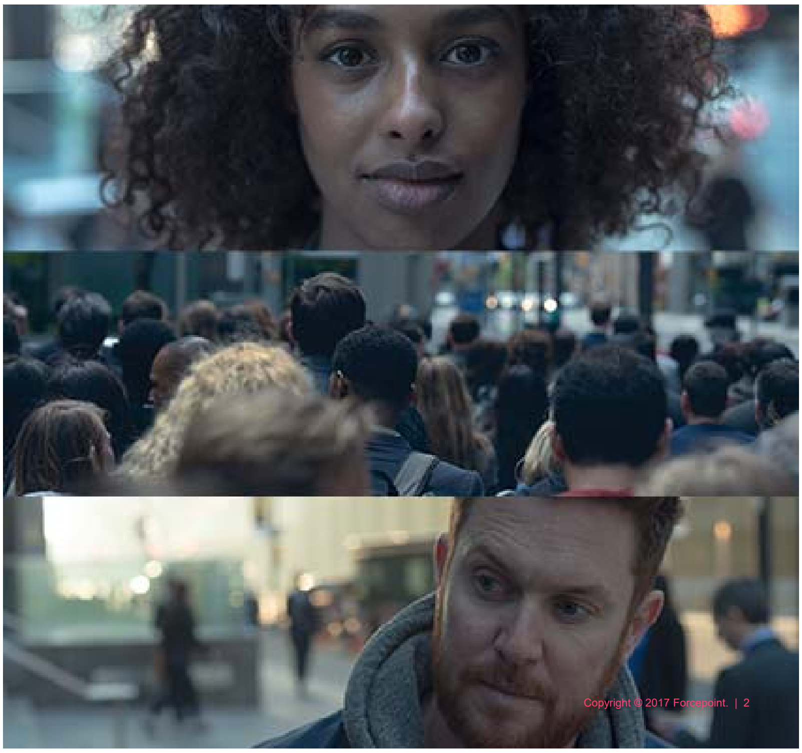
January 2019

SECURITY TREND and Awareness in 2019 for EDUCATION

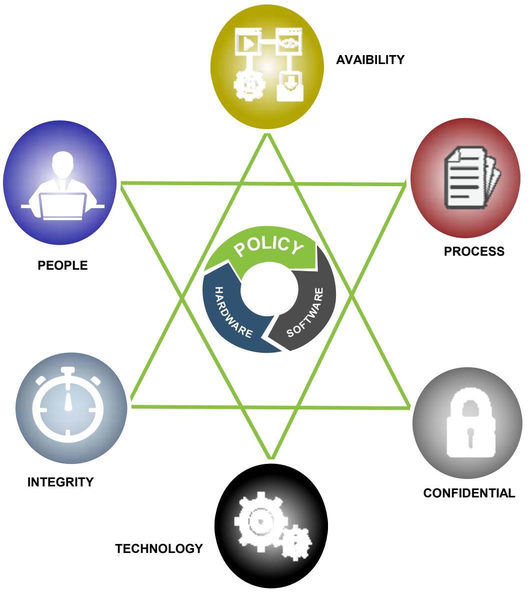
Saksit Nuchjirasuwan, SE

FORCEPOINT

Security Awareness and Principle



THE FUNDAMENTAL PRINCIPLES OF SECURITY



Importance of Cybersecurity

- The internet allows an attacker to work from anywhere on the planet.
- Risks caused by poor security knowledge and practice:
  - Identity Theft
  - Monetary Theft
  - Legal Ramifications (for yourself and your organization)
  - Sanctions or termination if policies are not followed
- According to the SANS Institute, the top vectors for vulnerabilities available to a cyber criminal are:
  - Web Browser
  - IM Clients
  - Web Applications
  - Excessive User Rights

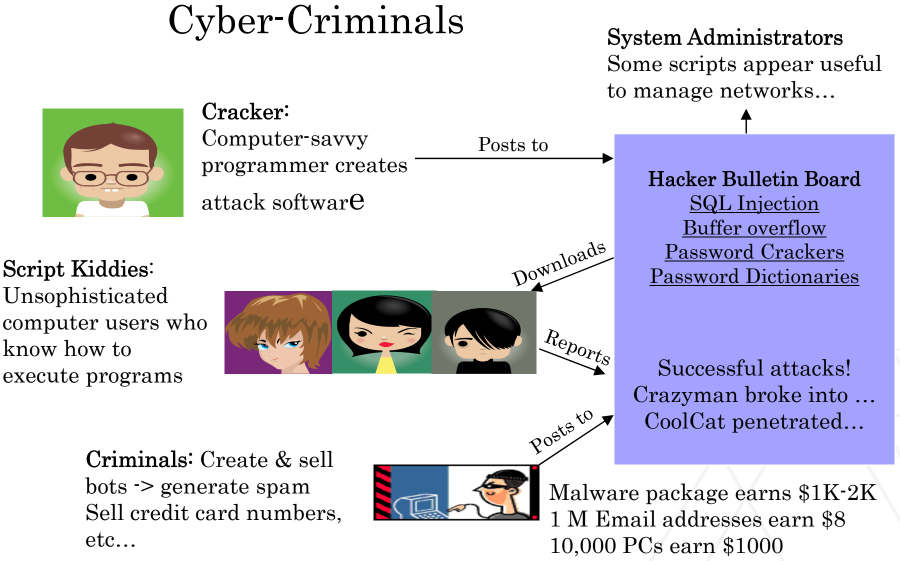
Cybersecurity is Safety

Security: We must protect our computers and data in the same way that we secure the doors to our homes.

Safety: We must behave in ways that protect us against risks and threats that come with technology.

User Awareness

Cyber-Criminals



Cracker: Computer-savvy programmer creates attack software

Script Kiddies: Unsophisticated computer users who know how to execute programs

Criminals: Create & sell bots -> generate spam Sell credit card numbers, etc…

System Administrators Some scripts appear useful to manage networks…

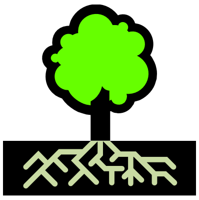
Hacker Bulletin Board
SQL Injection
Buffer overflow
Password Crackers
Password Dictionaries

Successful attacks!
Crazyman broke into …
CoolCat penetrated…

Malware package earns $1K-2K
1 M Email addresses earn $8
10,000 PCs earn $1000

Leading Threats

- Viruses
- Worms
- Trojan Horses / Logic Bombs
- Social Engineering
- Rootkits
- Botnets / Zombies



Viruses

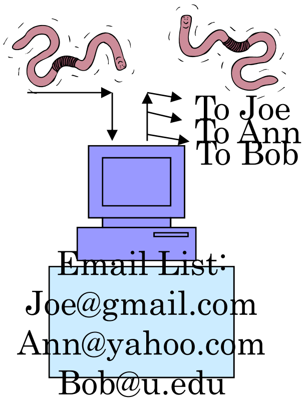
- A virus attaches itself to a program, file, or disk.
- When the program is executed, the virus activates and replicates itself.
- The virus may be benign or malignant but executes its payload at some point (often upon contact).
  - Viruses can cause computer crashes and loss of data.
- In order to recover or prevent virus attacks:
  - Avoid potentially unreliable websites/emails.
  - System Restore.
  - Re-install operating system.
  - Use and maintain anti-virus software.

Program A
Extra Code
Program B

Worms

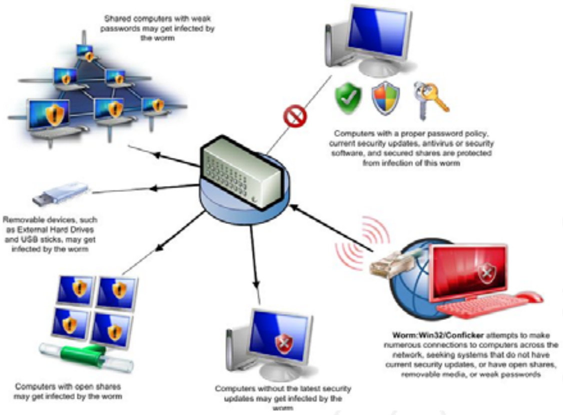
Independent program that replicates itself and sends copies from computer to computer across network connections.

Upon arrival, the worm may be activated to replicate.



To Joe
To Ann
To Bob

Email List:
Joe@gmail.com
Ann@yahoo.com
Bob@u.edu


Shared computers with weak passwords may get infected by the worm
Computers with a proper password policy, current security updates, antivirus or security software, and secured shares are protected from infection of this worm
Removable devices, such as External Hard Drives and USB sticks, may get infected by the worm
Worm:Win32/Conficker attempts to make numerous connections to computers across the network, seeking systems that do not have current security updates, or have open shares, removable media, or weak passwords
Computers with open shares may get infected by the worm
Computers without the latest security updates may get infected by the worm

Logic Bombs and Trojan Horses

Logic Bomb: Malware logic executes upon certain conditions. The program is often used for otherwise legitimate reasons.

Examples:

Software which malfunctions if maintenance fee is not paid.

Employee triggers a database erase when he is fired.

Trojan Horse: Masquerades as a benign program while quietly destroying data or damaging your system.

Download a game: It may be fun but contains hidden code that gathers personal information without your knowledge.

Social Engineering

manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

Email:
ABC Bank has noticed a problem with your account…

Phone Call:
This is John, the System Administrator. What is your password?

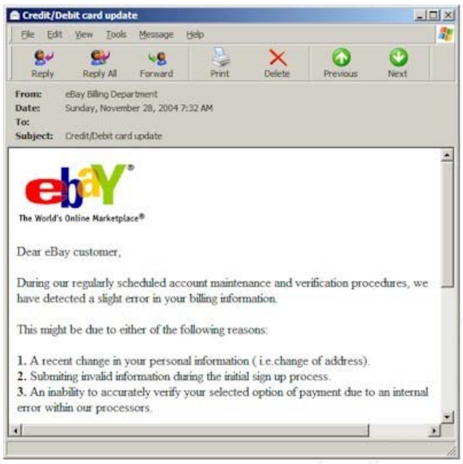
In Person:
What ethnicity are you? Your mother's maiden name?

I have come to repair your machine…

and have some lovely software patches!

Phishing: Counterfeit Email

A seemingly trustworthy entity asks for sensitive information such as SSN, credit card numbers, login IDs or passwords via e-mail.



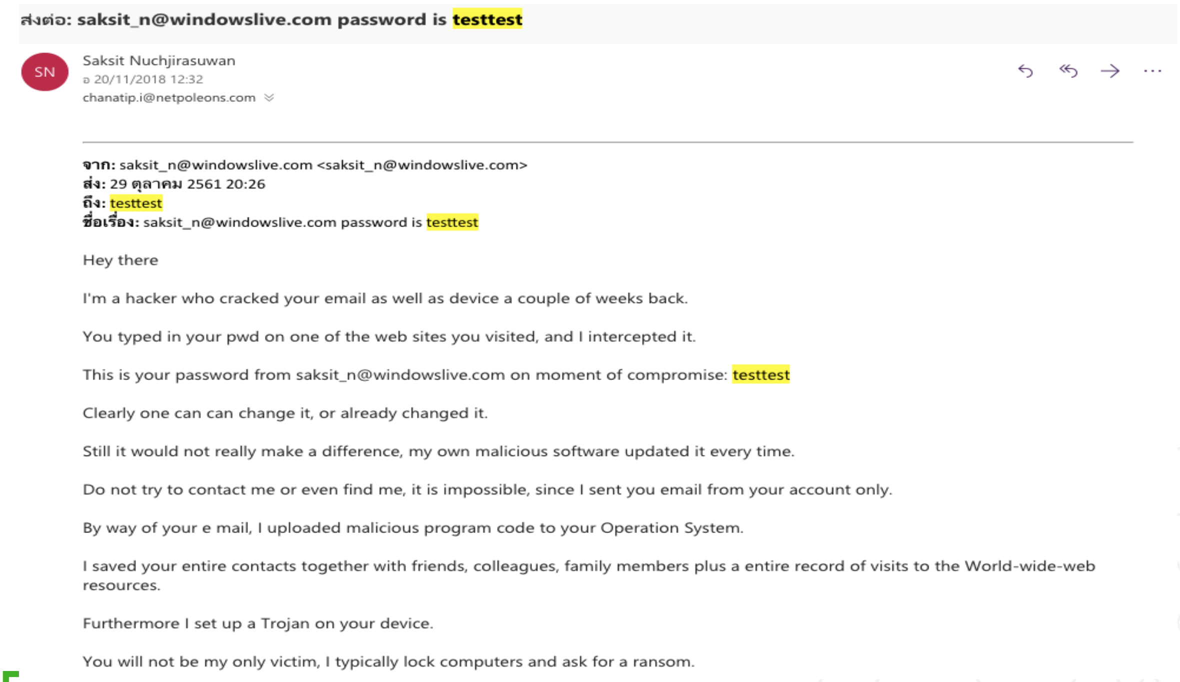
From: eBay Billing Department
Date: Sunday, November 28, 2004 7:32 AM
To:
Subject: Credit/Debit card update

Dear eBay customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e.change of address).
2. Submiting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.



ส่งต่อ: saksit_n@windowslive.com password is testtest

Saksit Nuchjirasuwan
อ 20/11/2018 12:32
chanatip.i@netpoleons.com

จาก: saksit_n@windowslive.com <saksit_n@windowslive.com>
ส่ง: 29 ตุลาคม 2561 20:26
ถึง: testtest
ชื่อเรื่อง: saksit_n@windowslive.com password is testtest

Hey there

I'm a hacker who cracked your email as well as device a couple of weeks back.

You typed in your pwd on one of the web sites you visited, and I intercepted it.

This is your password from saksit_n@windowslive.com on moment of compromise: testtest

Clearly one can can change it, or already changed it.

Still it would not really make a difference, my own malicious software updated it every time.

Do not try to contact me or even find me, it is impossible, since I sent you email from your account only.

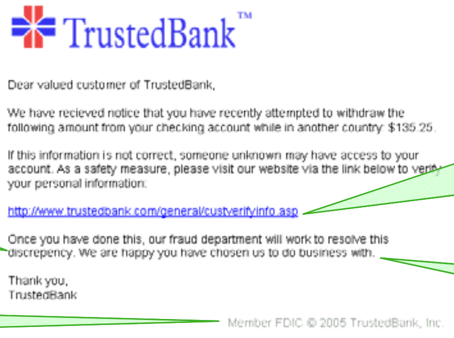
By way of your e mail, I uploaded malicious program code to your Operation System.

I saved your entire contacts together with friends, colleagues, family members plus a entire record of visits to the World-wide-web resources.

Furthermore I set up a Trojan on your device.

You will not be my only victim, I typically lock computers and ask for a ransom.

Pharming: Counterfeit Web Pages



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information.

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Misspelled

Wiping over, but not clicking the link may reveal a different address.

With whom?

Copyright date is old

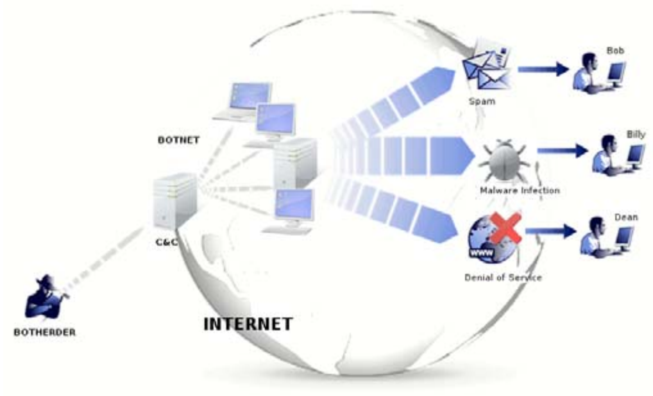
The link provided in the e-mail leads to a counterfeit webpage which collects important information and submits it to the owner.

The counterfeit web page looks like the real thing

Extracts account information

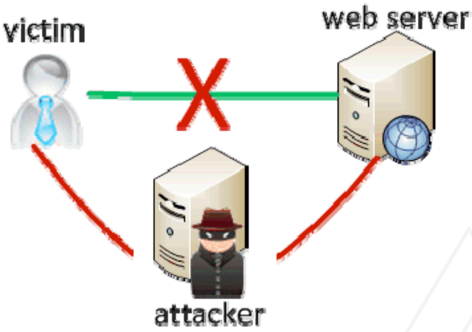
Botnet

- A botnet is a number of compromised computers used to create and send spam or viruses or flood a network with messages as a denial of service attack.
- The compromised computers are called zombies.



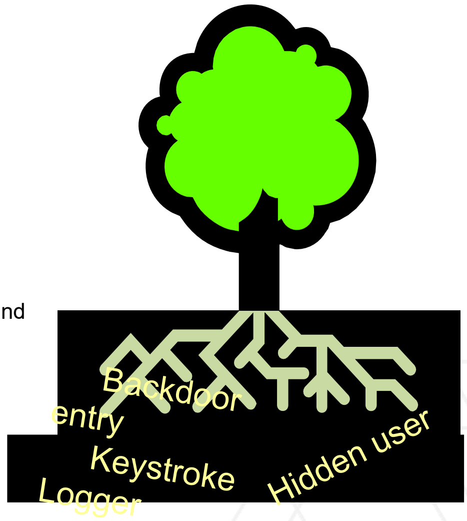
Man In The Middle Attack

An attacker pretends to be your final destination on the network. When a person tries to connect to a specific destination, an attacker can mislead him to a different service and pretend to be that network access point or server.



Rootkit

- Upon penetrating a computer, a hacker may install a collection of programs, called a rootkit.
- May enable:
  - Easy access for the hacker (and others)into the enterprise
  - Keystroke logger
- Eliminates evidence of break-in.
- Modifies the operating system.



Password Cracking

Dictionary Attack and Brute Force

Pattern	Calculation	Result	Time to Guess (2.6x10^{18} tries/month)
Personal Info: interests, relatives		20	Manual 5 minutes
Social Engineering		1	Manual 2 minutes
American Dictionary		80,000	< 1 second
4 chars: lower case alpha	26^4	5x10^5	
8 chars: lower case alpha	26^8	2x10^{11}	
8 chars: alpha	52^8	5x10^{13}	
8 chars: alphanumeric	62^8	2x10^{14}	3.4 min.
8 chars alphanumeric +10	72^8	7x10^{14}	12 min.
8 chars: all keyboard	95^8	7x10^{15}	2 hours
12 chars: alphanumeric	62^{12}	3x10^{21}	96 years
12 chars: alphanumeric + 10	72^{12}	2x10^{22}	500 years
12 chars: all keyboard	95^{12}	5x10^{23}	
16 chars: alphanumeric	62^{16}	5x10^{28}	

Georgia Data Breach Notification Law

O.C.G.A. §§10-1-910, -911, -912

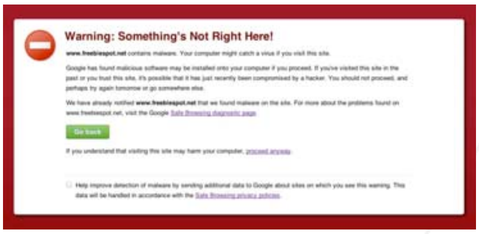
- An unauthorized acquisition of electronic data that compromises the security, confidentiality or integrity of "personal information."
- Personal Information
  - Social Security Number.
  - Driver's license or state ID number.
  - Information permitting access to personal accounts.
  - Account passwords or PIN numbers or access codes.
  - Any of the above in connection with a person's name if the information is sufficient to perform identity theft against the individual.

Identifying Security Compromises

- Symptoms:
  - Antivirus software detects a problem.
  - Disk space disappears unexpectedly.
  - Pop-ups suddenly appear, sometimes selling security software.
  - Files or transactions appear that should not be there.
  - The computer slows down to a crawl.
  - Unusual messages, sounds, or displays on your monitor.
  - Stolen laptop: 1 stolen every 53 seconds; 97% never recovered.
  - The mouse pointer moves by itself.
  - The computer spontaneously shuts down or reboots.
  - Often unrecognized or ignored problems.

Malware detection

- Spyware symptoms:
  - Changes to your browser homepage/start page.
  - Ending up on a strange site when conducting a search.
  - System-based firewall is turned off automatically.
  - Lots of network activity while not particularly active.
  - Excessive pop-up windows.
  - New icons, programs, favorites which you did not add.
  - Frequent firewall alerts about unknown programs when trying to access the Internet.
  - Poor system performance.



Warning: Something's Not Right Here!

www.freebiespot.net contains malware. Your computer might catch a virus if you visit this site.

Google has found malicious software may be installed onto your computer if you proceed. If you've visited this site in the past or you trust this site, it's possible that it has just recently been compromised by a hacker. You should not proceed, and perhaps try again tomorrow or go somewhere else.

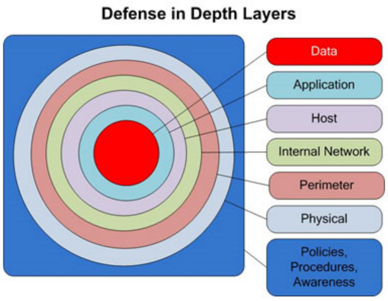
We have already notified **www.freebiespot.net** that we found malware on the site. For more about the problems found on www.freebiespot.net, visit the Google Safe Browsing diagnostic page.

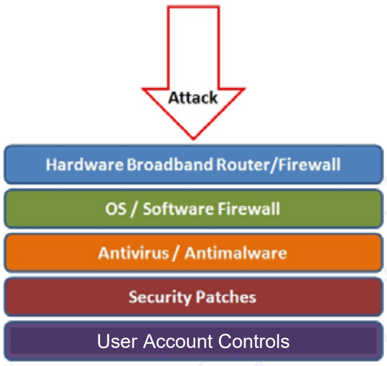
If you understand that visiting this site may harm your computer, proceed anyway.

□ Help improve detection of malware by sending additional data to Google about sites on which you see this warning. This data will be handled in accordance with the Safe Browsing privacy policies.

Best Practices to avoid these threats

Defense in depth uses multiple layers of defense to address technical, personnel and operational issues.


Defense in Depth Layers

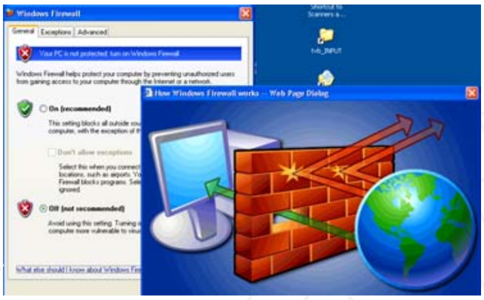


Anti-virus and Anti-spyware Software

- Anti-virus software detects certain types of malware and can destroy it before any damage is done.
- Install and maintain anti-virus and anti-spyware software.
- Be sure to keep anti-virus software up
- Ma exist.
- Co
  Pr

Host-based Firewalls

- A firewall acts as a barrier between your computer/private network and the internet. Hackers may use the internet to find, use, and install applications on your computer. A firewall prevents many hacker connections to your computer.
- Firewalls filter network packets that enter or leave your computer


Windows Firewall
General
Exceptions
Advanced
Shortcut to Scanners a...
t-b_INPUT
How Windows Firewall works -- Web Page Dialog

Your PC is not protected: turn on Windows Firewall

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

○ On (recommended)

This setting blocks all outside sou... computer, with the exception of th...

□ Don't allow exceptions

Select this when you connect... locations, such as airports. Yo... Firewall blocks programs. Sel... ignored.

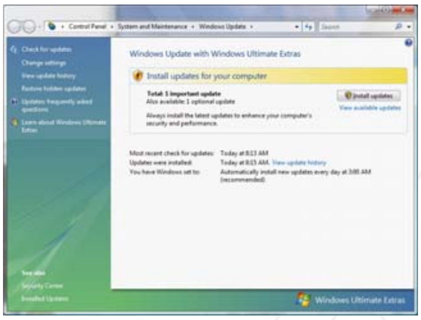
● Off (not recommended)

Avoid using this setting. Turning o... computer more vulnerable to viru...

What else should I know about Windows Fir...

Protect your Operating System

- Microsoft regularly issues patches or updates to solve security problems in their software. If these are not applied, it leaves your computer vulnerable to hackers.
- The Windows Update feature built into Windows can be set up to automatically download and install updates.
- Avoid logging in as administrator
- Apple provides regular updates to its operating system and software applications.
- Apply Apple updates using the App Store application.



Windows Update with Windows Ultimate Extras

Install updates for your computer

Total: 1 important update
Also available: 1 optional update

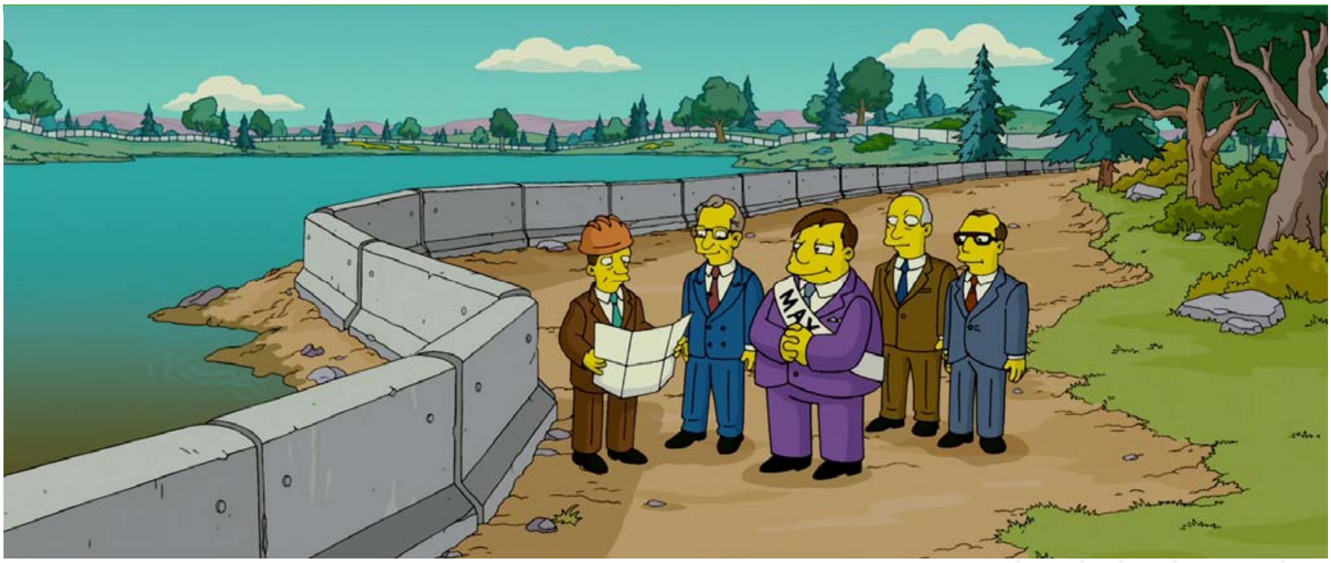
Always install the latest updates to enhance your computer's security and performance.

Most recent check for updates: Today at 8:13 AM
Updates were installed: Today at 8:15 AM.
You have Windows set to: Automatically install new updates every day at 3:00 AM (recommended)

Use Strong Passwords

Make passwords easy to remember but hard to guess

- USG standards:
- Be at least ten characters in length
- Must contain characters from at least two of the following four types of characters:
  - English upper case (A-Z)
  - English lower case (a-z)
  - Numbers (0-9)
  - Non-alphanumeric special characters ($, !, %, ^, …)
- Must not contain the user's name or part of the user's name
- Must not contain easily accessible or guessable personal information about the user or user's family, such as birthdays, children's names, addresses, etc.



Creating Strong Passwords

- A familiar quote can be a good start:

  "LOVE IS A SMOKE MADE WITH
  THE FUME OF SIGHS"
  William Shakespeare

- Using the organization standard as a guide, choose the first character of each word:
  - LIASMWTFOS
- Now add complexity the standard requires:
  - `L1A$mwTF0S` (10 characters, 2 numerals, 1 symbol, mixed English case: password satisfies all 4 types).
- Or be more creative!

Password Guidelines

- Never use admin, root, administrator, or a default account or password for administrative access.
- A good password is:
  - Private: Used by only one person.
  - Secret: It is not stored in clear text anywhere including on Post-It® notes!

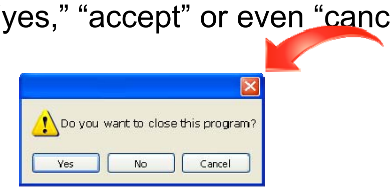
  - Easily Remembered: No need to write it down.
  - Contains the complexity required by your organization.
  - Not easy to guess by a person or a program in a reasonable time, such as several weeks.
  - Changed regularly: Follow organization standards.
- Avoid shoulder surfers and enter your credentials carefully! If a password is entered in the username field, those attempts usually appear in system logs.

Avoid Social Engineering and Malicious Software

- Do not open email attachments unless you are expecting the email with the attachment and you trust the sender.
- Do not click on links in emails unless you are absolutely sure of their validity.
- Only visit and/or download software from web pages you trust.

Avoid Stupid Hacker Tricks

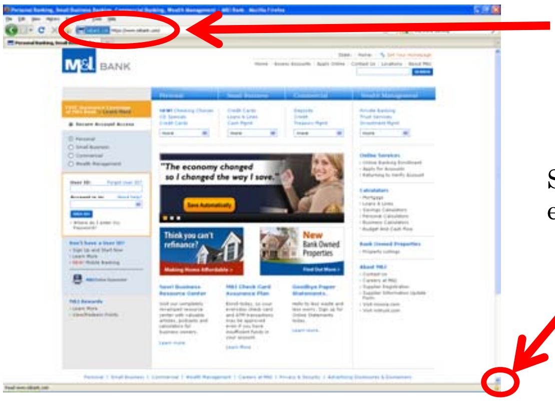
- Be sure to have a good firewall or pop-up blocker installed.
- Pop-up blockers do not always block ALL pop-ups so always close a pop-up window using the ‘X’ in the upper corner.
- Never click “yes,” “accept” or even “cancel.”


Do you want to close this program?

- Infected USB drives are often left unattended by hackers in public places.

Secure Business Transactions

- Always use secure browser to do online activities.
- Frequently delete temp files, cookies, history, saved passwords etc.


M&I BANK
"The economy changed so I changed the way I save."
Think you can't refinance?
New Bank Owned Properties

https://

Symbol indicating enhanced security

Backup Important Information

- No security measure is 100% reliable.
- Even the best hardware fails.
- What information is important to you?
- Is your backup:

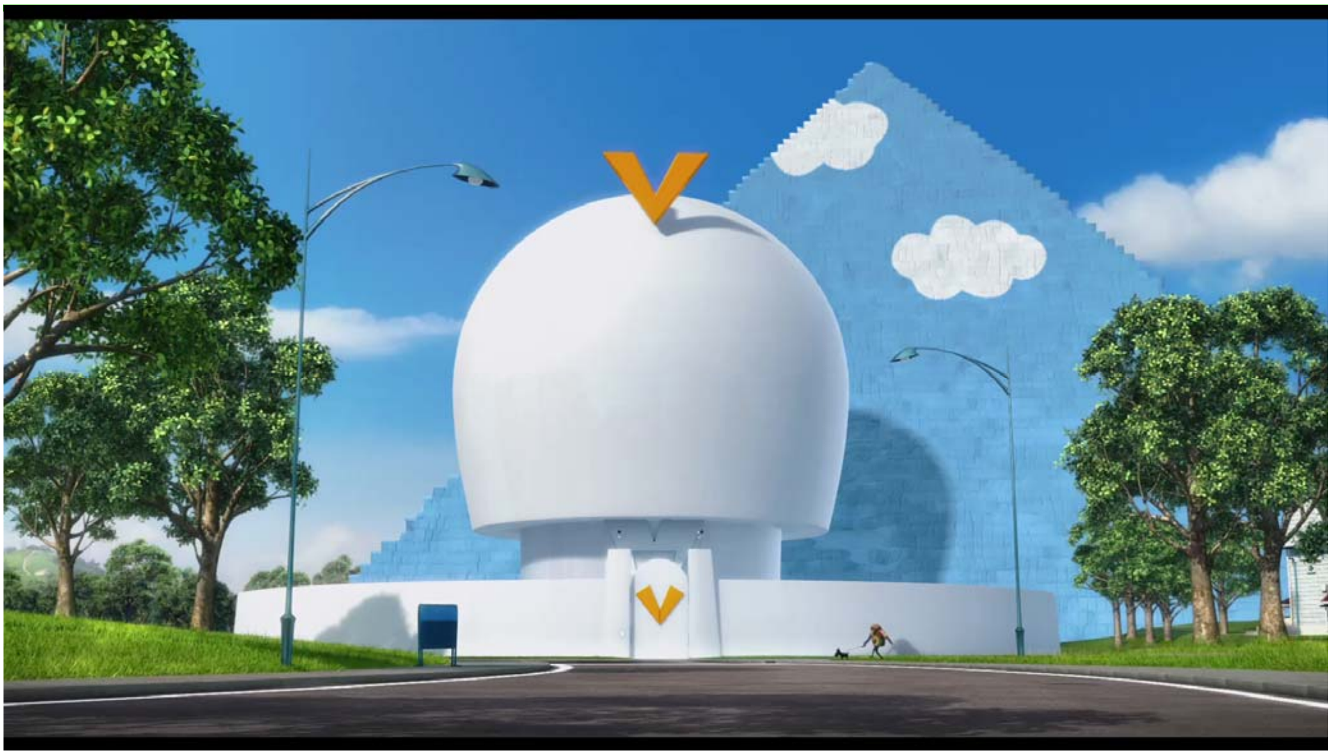
Recent?

Off-site & Secure?

Process Documented?

Encrypted?

Tested?



Cyber Incident Reporting

If you suspect a cybersecurity incident, notify your organization's help desk or the USG ITS help desk immediately. Be prepared to supply the details you know and contact information.

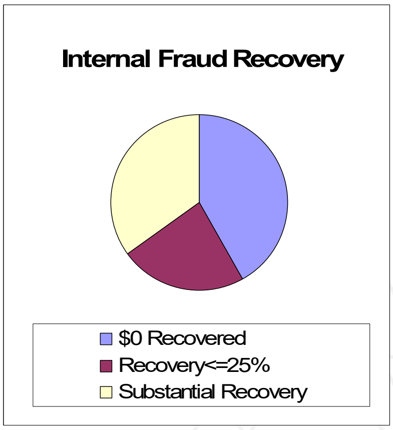
1. Do not attempt to investigate or remediate the incident on your own.
2. Inform other users of the system and instruct them to stop work immediately.
3. Unless instructed, do not power down the machine.
4. Unless instructed, do not remove the system from the network.

The cybersecurity incident response team will contact you as soon as possible to gather additional information.

Each USG organization is required to have a specific plan to handle cybersecurity incidents. Refer to local policies, standards and guidelines for specific information.

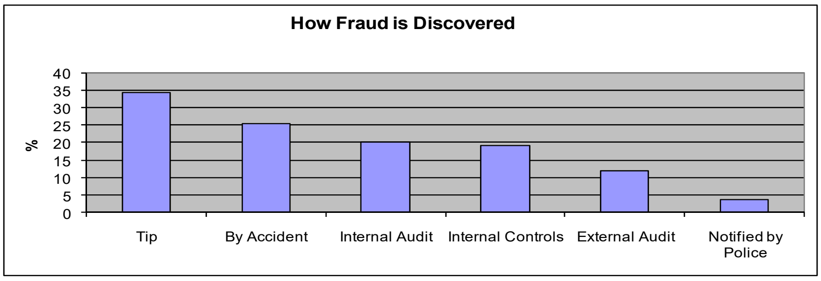
Fraud

- Organizations lose 5-6% of revenue annually due to internal fraud = $652 Billion in U.S. (2006)
- Average scheme lasts 18 months, costs $159,000
- 25% costs exceed $1M
- Smaller companies suffer greater average dollar losses than large companies



Essentials of Corporate Fraud, T L Coenen, 2008, John Wiley & Sons

Fraud Discovery



Tips are the most common way fraud is discovered.
Tips come from:
Employee/Coworkers 64%,
Anonymous 18%,
Customer 11%,
Vendor 7%
If you suspect possible fraud, report it anonymously to the USG ethics hot line at 877-516-3466.

Essentials of Corporate Fraud, T L Coenen, 2008, John Wiley & Sons

Security Trend in 2019

What should we know before get loss?

CYBER SECURITY TRENDS TO WATCH IN 2019

1. Operational technology and critical infrastructure security

Large industrial and critical infrastructure installations now depend on the Internet for remote management and monitoring. At the other end of the scale, cardiac pacemakers embedded in patients have required software updates to fix security vulnerabilities. This trend is set to continue, and we'll see an increase in attacks and security flaws being identified in technology that aren't traditional targets. Internet of Things devices will continue to be targeted given their low level of security, and we're likely to see some more significant operational technology and critical infrastructure security incidents in the coming year.

2. The two faces of cloud security

As application delivery continues to migrate to a software-as-a-service delivery model, security around cloud-based applications will need improvement. Enterprises are getting better at securing these apps, but ease of access consistently introduces risks to organizations where the necessary level of security hardening hasn't been applied. This is difficult to manage, however, as the use of some apps are undertaken as Shadow IT.

Enterprise applications should continue to integrate with centralized identity and access management tools such as Azure Active Directory, but applications that fall outside of enterprise IT responsibility will continue to experience incidents due to poor security consideration.

https://www.pluralsight.com/blog/security-professional/cyber-security-trends-2019

CYBER SECURITY TRENDS TO WATCH IN 2019

3. Commercial espionage and political warfare

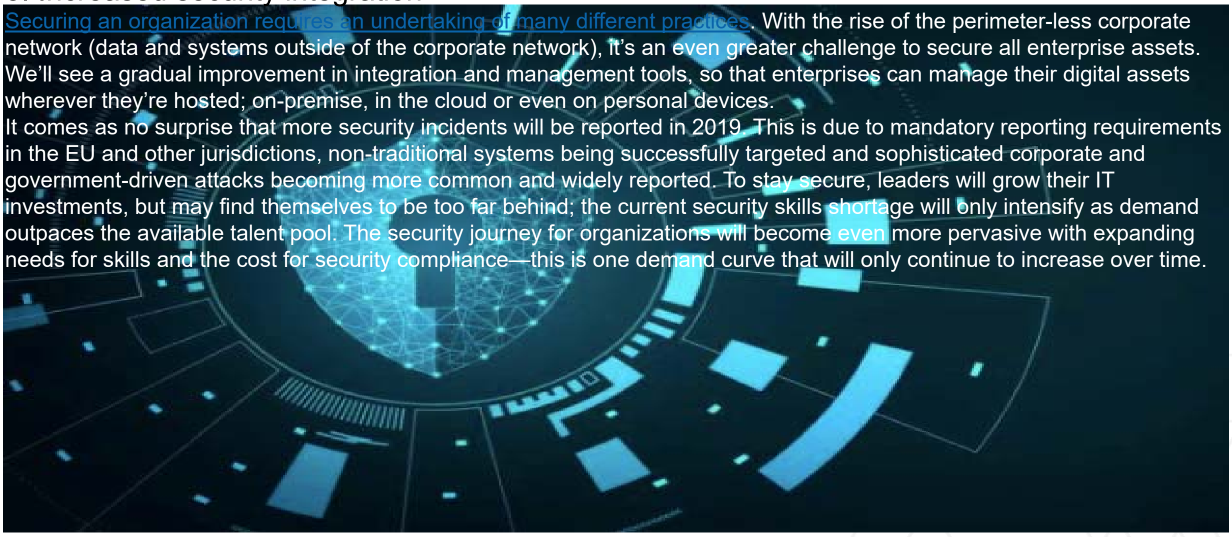
Whilst most developed countries have laws against cyber-attacks, the Internet is a global network. More governments are recognizing attacks and cyber defense as key elements to their military capability. Commercial organizations need to be conscious their digital assets must be protected from competitors, especially those operating from countries with weak data protection and security laws. 2019 will see increases in commercial espionage and intelligence capturing in order to provide competitive advantage.

4. Boardroom concerns (again) for GDPR and the US

The GDPR became effective in May 2018 and carried with it an intense focus by boardrooms. Since then, there's been great anticipation as to how the enforcement of the law will play out. Company boards are likely to redouble this focus once the first substantial fines are handed down by regulators following breaches. As talks of a US version of GDPR continue for another year, US-based companies will be watching for trends in enforcement overall effectiveness of the law to improve data protection.

CYBER SECURITY TRENDS TO WATCH IN 2019

5. Increased security integration



Securing an organization requires an undertaking of many different practices. With the rise of the perimeter-less corporate network (data and systems outside of the corporate network), it's an even greater challenge to secure all enterprise assets. We'll see a gradual improvement in integration and management tools, so that enterprises can manage their digital assets wherever they're hosted; on-premise, in the cloud or even on personal devices.

It comes as no surprise that more security incidents will be reported in 2019. This is due to mandatory reporting requirements in the EU and other jurisdictions, non-traditional systems being successfully targeted and sophisticated corporate and government-driven attacks becoming more common and widely reported. To stay secure, leaders will grow their IT investments, but may find themselves to be too far behind; the current security skills shortage will only intensify as demand outpaces the available talent pool. The security journey for organizations will become even more pervasive with expanding needs for skills and the cost for security compliance—this is one demand curve that will only continue to increase over time.

CYBERSECURITY TRENDS 2019

Our pick of the biggest cybersecurity trends that need to be on your radar for 2019 according to a wide range of industry experts

https://www.computerworlduk.com/security/security-trends-for-2019-3689719

Better, smarter IoT botnets

The first truly global case of a powerful internet of things (IoT) botnet was Mirai in 2016. It was achieved with a few lines of quite simple code, but was so effective because it targeted objects like IP cameras that were connected to the internet but rarely secured or updated, and managed to bring down a decent chunk of the internet.

The internet providers and DNS companies have buffeted their defenses since Mirai, but the IoT market - which could reach $6.5 trillion by 2024 - is only going to increase dramatically. Some manufacturers may have sharpened up their products to be updatable but certainly not all will have, especially when these things become interwoven into the fabric of everyday life.

CYBERSECURITY TRENDS 2019

Attacks on critical national infrastructure

A recent parliamentary committee warned that critical national infrastructure is at risk from cyber attackers. The National Cyber Security Centre also recently warned that states hostile to Britain would likely target the infrastructure of Britain.

While high profile real-world examples of these sorts of attacks have been relatively scarce (especially in Britain - with only WannaCry and NotPetya coming close to date) some experts are warning that 2019 could see intra-state rivalries become more realised in the cyber realm.

Even taking hostile states out of the equation, attackers motivated by money might see weakness in the country's current approach to critical national infrastructure and hit it for financial reasons before it's fixed.

James Wickes, CEO and cofounder of Cloudview, said that attacks on infrastructure could also be linked to the increase in internet-connected devices.

Crypto-jacking

If 2017 saw the Tulip-mania style boom and bust of crypto currencies, 2018 saw a significant uptick in crypto-jacking, the process of taking control of a device or network of devices to use the additional compute for crypto mining.

Webroot went as far as to claim in its mid-year threat report that crypto-jacking accounted for as much as 35 percent of all threats - and that its customers attempted to visit websites running crypto-jacking scripts three percent of the time. The most popular crypto mining domain was Xxgasm.com for 31 percent of traffic while Coinhive.com accounted for 38 percent of traffic.

CYBERSECURITY TRENDS 2019

More ransomware

Ransomware has persisted for so long both because it can be used to such devastating effect and for its relative simplicity.
Indeed, scripts are available to buy on the dark web for mere pennies in many cases, just point and shoot.
According to John Fokker, head of cyber investigations at McAfee, the ransomware underworld will "consolidate", creating "fewer but stronger malware-as-a-service families that will actively work together".
"We also predict a continuation of the strongest ransomware 'brands' using affiliate structures to increase their threat," he adds.

Good old blackmail

According to enterprise architect at Carbon Black's threat analysis unit, Paul Drapeau, compromised data sets could very easily enable a new path to traditional blackmail.
"Breaches in Facebook and other social media platforms represent a wealth of data to be mined by bad actors," he says.
"This data could be used to correlate activities between people to find illegal, scandalous or compromising behaviour and then leverage that for traditional blackmail at scale."
What could that look look? "'Pay me the bitcoins or your spouse/employer gets copies of these direct messages' an example note might read," he explains. "We can fight ransomware with anti-malware tools or backups but we depend on giant companies to protect our more personal details.

CYBERSECURITY TRENDS 2019

APT groups, nation states, state-sponsored attacks

Kaspersky believes that the advanced persistent threat groups (think Fancy Bear, Shadow Brokers) might do more to cover their tracks - less outspoken branding or signature attacks, in short, which would make detection and attribution "extremely difficult".
The vendor adds that one of the most likely scenarios in this new approach would be building tools catered to highly specific targets.
According to Priscilla Moriuchi, director of strategic threat development at Recorded Future, state-sponsored groups are likely to place an increasing focus on telecommunications companies and ISPs.

Encrypted traffic malware

The increased understanding of the importance of encryption could well be exploited by groups that hide malware itself within encrypted traffic.
Omar Yaacoubi, founder and CEO of Barac, points out Google research that suggests 80 percent of all traffic will be encrypted in 2019, and a PwC study that says 60 percent of attacks will occur on encrypted traffic.
"The downside of encryption is that security tools can't inspect encrypted traffic for malware, making it the perfect place for a threat actor to hide any kind of malicious traffic," he says. "A recent Vanson Bourne survey of 500 CIOs found that 90 percent of firms had experienced or expected to experience a network attack using SSL/TLS, and 87 percent believed their defences were less effective because of this emerging trend to bury malware in encrypted traffic.

CYBERSECURITY TRENDS 2019

AI-assisted imposters

Nvidia just this month unveiled extremely lifelike human face rendering, and there's no reason that this technology won't end up in the hands of bad actors, whether they're hacking groups or nation states.

Could facial rendering technologies like these be used to create entirely new personas, perhaps for the spreading of disinformation - in a country like the USA that under the Obama administration made propaganda against its own population entirely legal? That might sound paranoid, but fifteen years ago you'd be paranoid for suggesting people were watching you through your webcam, until that, well, happened.

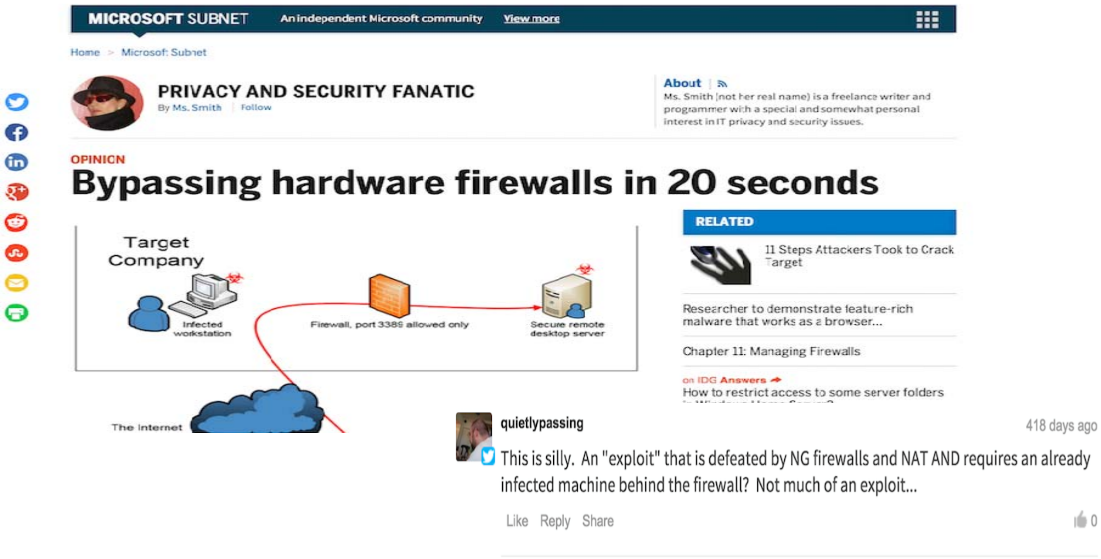
FORCEPOINT

POWERED BY Raytheon

Protecting the human point.

5 Security Concepts that we almost misunderstood

1. TECHNOLOGY BASED



MICROSOFT SUBNET An independent Microsoft community View more

Home > Microsoft Subnet

PRIVACY AND SECURITY FANATIC
By Ms. Smith | Follow

About
Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

OPINION

Bypassing hardware firewalls in 20 seconds

Target Company
Infected workstation
Firewall, port 3389 allowed only
Secure remote desktop server
The Internet

RELATED

11 Steps Attackers Took to Crack Target

Researcher to demonstrate feature-rich malware that works as a browser...

Chapter 11: Managing Firewalls

on IDG Answers
How to restrict access to some server folders

quietlypassing 418 days ago

This is silly. An "exploit" that is defeated by NG firewalls and NAT AND requires an already infected machine behind the firewall? Not much of an exploit...

Like Reply Share 0

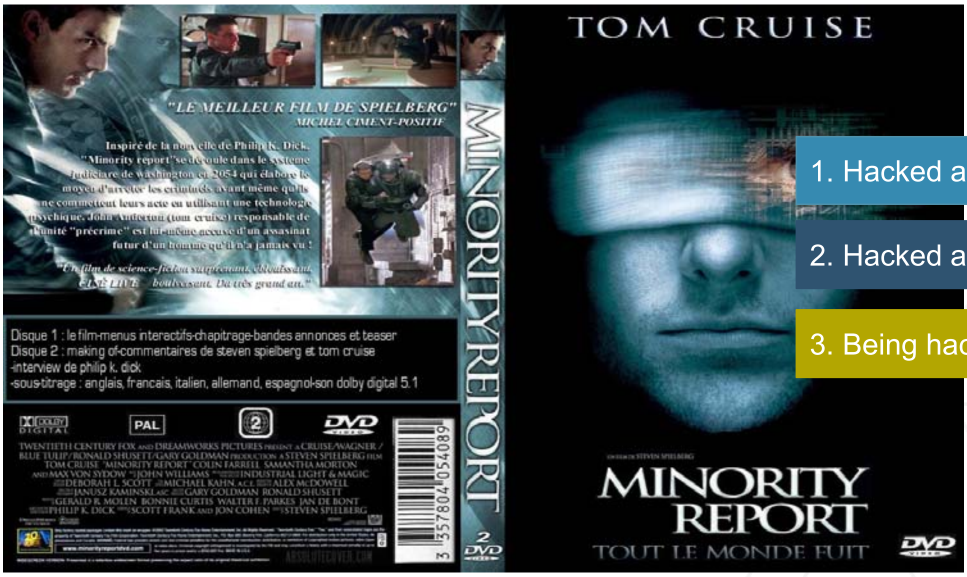
2. THE UNKNOWN PAIN POINT

Website Security: How Do Websites Get Hacked?

By Tony Perez on May 18, 2015 . • 5 Comments

1. Employ **Defense in Depth** Principles – layers like an onion.
2. Leverage best practices like **Least Privileged** – not everyone needs administrative privileges.
3. Place emphasis on how people access your website, leverage things like **Multi-Factor and Two-Factor Authentication**.
4. Protect yourself against the exploitation of software vulnerabilities through use of a Website Firewall **–** focuses on Known and Unknown Attacks.
5. **Backups** are your friends – think of them as your safety net, try to have at least 60 days available.
6. **Register your website with Search Engines** – Google and Bing have Webmaster Tools, leverage their infrastructure to tell you the health of your website.

3. SUCCESSFUL IN THE PAST


TOM CRUISE
"LE MEILLEUR FILM DE SPIELBERG"
MICHEL CIMENT-POSITIF
MINORITY REPORT
TOUT LE MONDE FUIT
Disque 1 : le film-menus interactifs-chapitrage-bandes annonces et teaser
Disque 2 : making of-commentaires de steven spielberg et tom cruise
-interview de philip k. dick
-sous-titrage : anglais, francais, italien, allemand, espagnol-son dolby digital 5.1
PAL
DVD

1. Hacked and Known
2. Hacked and Unknown
3. Being hacked

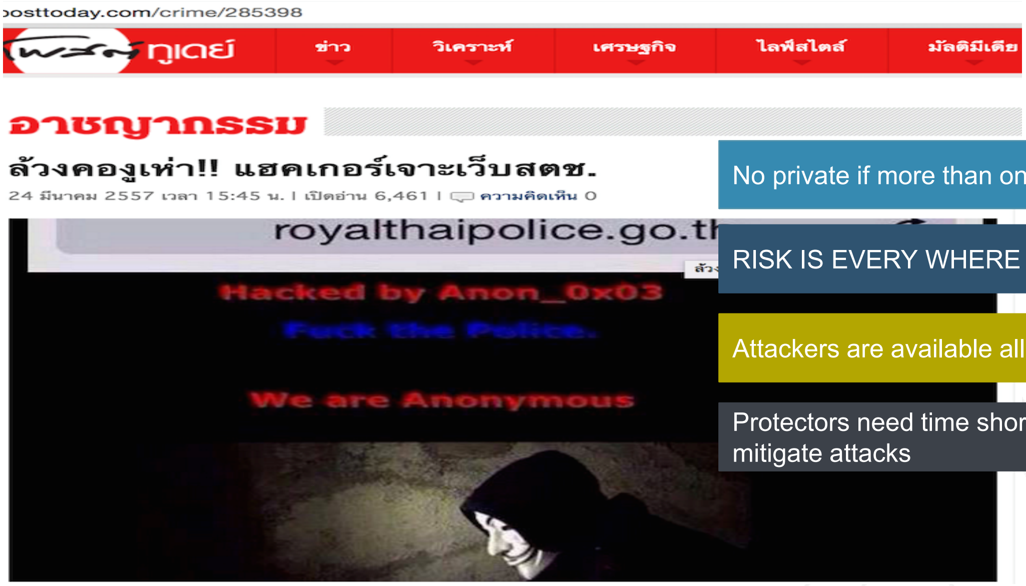
4. COPY CAT IS PERFECT

What is Adaptive Security?

May 27, 2015 Posted By Chris Riley In Blogs, Rugged DevOps Tagged Adaptive, Prevent, Security 0 Comments

- What is the core business?
- Who can access our resource?, when and how?
- What are our security strength and weakness?
- Security Policy and standard up to date?

5. PRIVATE IS SECURE?



อาชญากรรม

ล้วงคองูเห่า!! แฮคเกอร์เจาะเว็บสตช.

24 มีนาคม 2557 เวลา 15:45 น. | เปิดอ่าน 6,461 | ความคิดเห็น 0

royalthaipolice.go.th

Hacked by Anon_0x03

Fuck the Police.

We are Anonymous

No private if more than one people

RISK IS EVERY WHERE

Attackers are available all times

Protectors need time shortly to fix and mitigate attacks

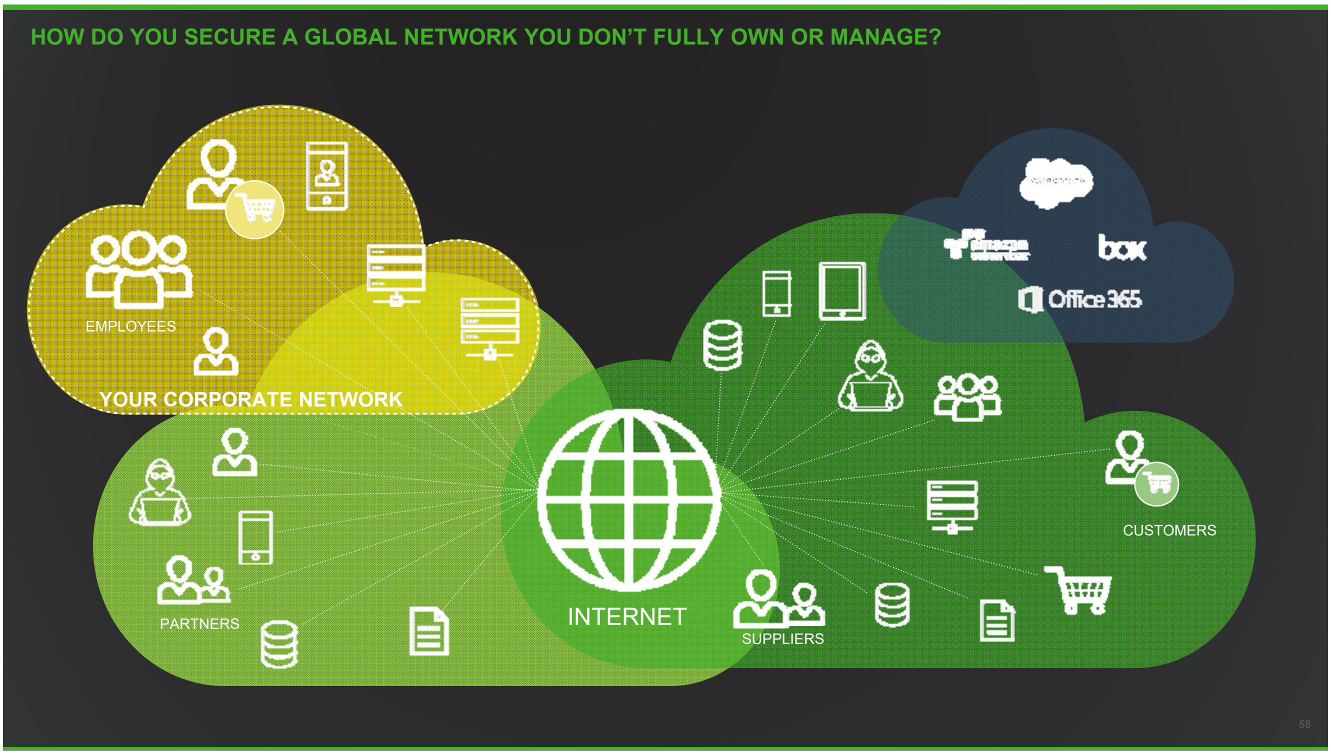
HUMAN POINT

How do you know who are threats and what the critical assess you lose?

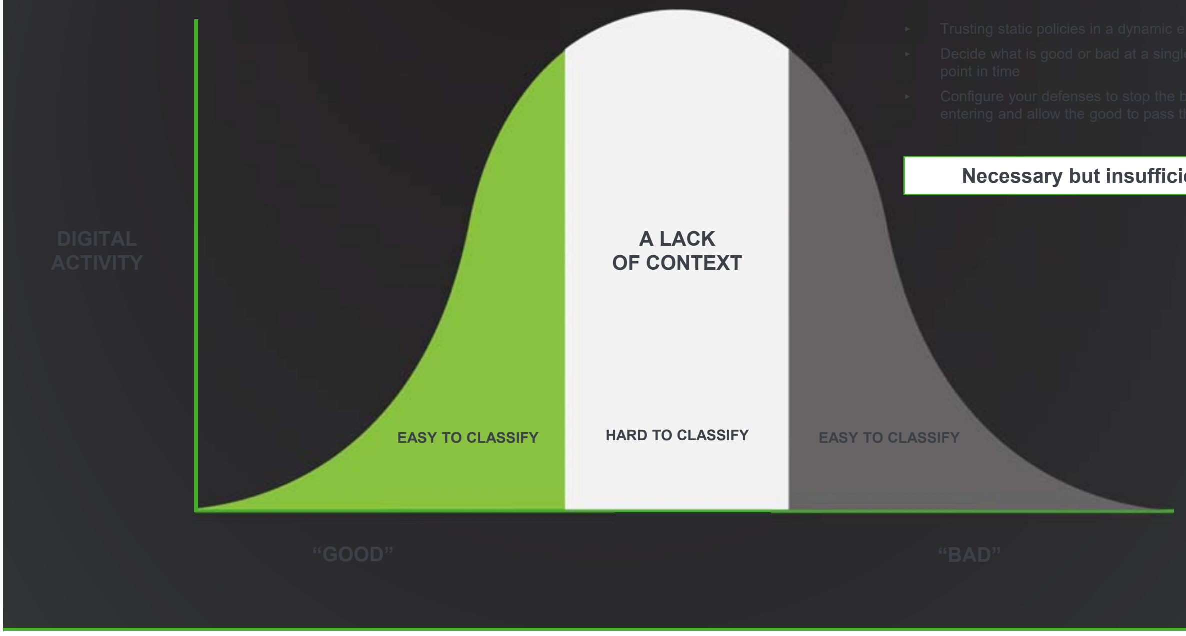
A COMPANY PURPOSE BUILT TO SOLVE TODAY'S PROBLEMS

Raytheon	websense	STONESOFT	skyfence	REDOWL
INSIDER THREAT, CROSS DOMAIN	WEB, EMAIL, DLP	NGFW	CASB	UEBA

HOW DO YOU SECURE A GLOBAL NETWORK YOU DON'T FULLY OWN OR MANAGE?



THE TRADITIONAL APPROACH TO CYBERSECURITY

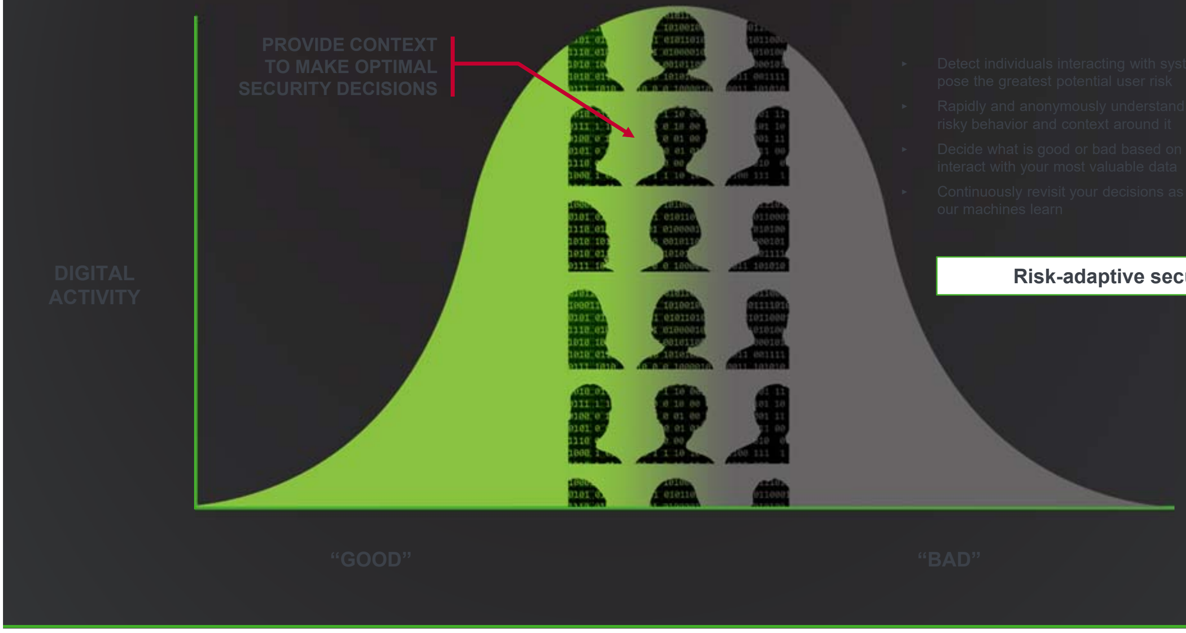


THREAT CENTRIC

- Trusting static policies in a dynamic environment
- Decide what is good or bad at a single point in time
- Configure your defenses to stop the bad from entering and allow the good to pass through

Necessary but insufficient

A NEW PARADIGM: HUMAN-CENTRIC CYBERSECURITY

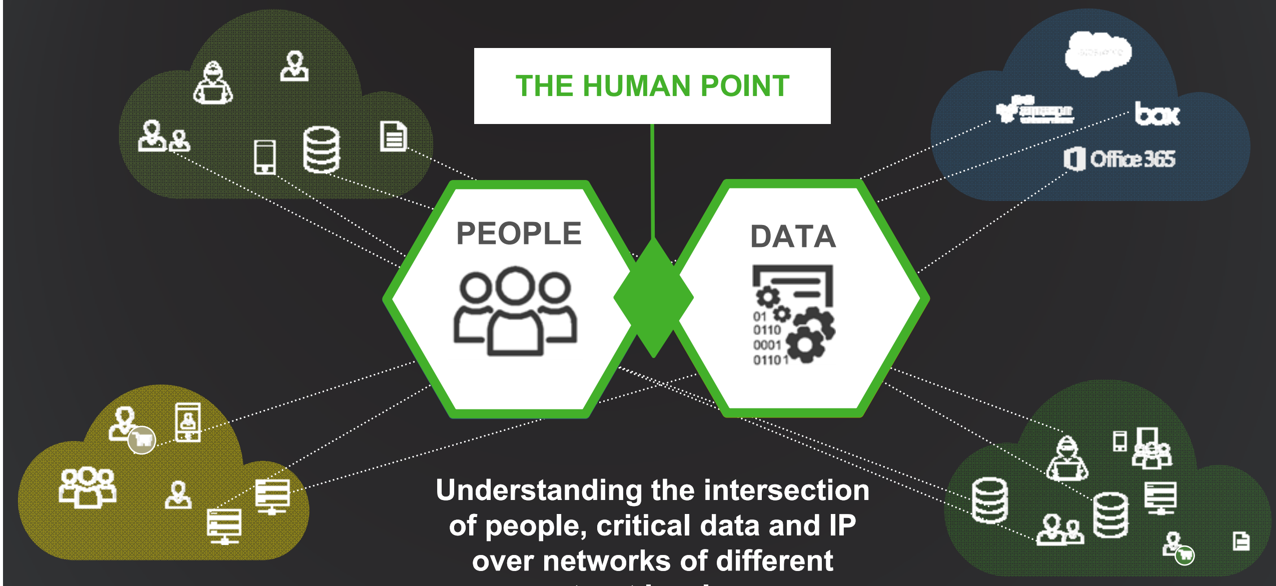


BEHAVIOR CENTRIC

- Detect individuals interacting with system that pose the greatest potential user risk
- Rapidly and anonymously understand potential risky behavior and context around it
- Decide what is good or bad based on how users interact with your most valuable data
- Continuously revisit your decisions as you and our machines learn

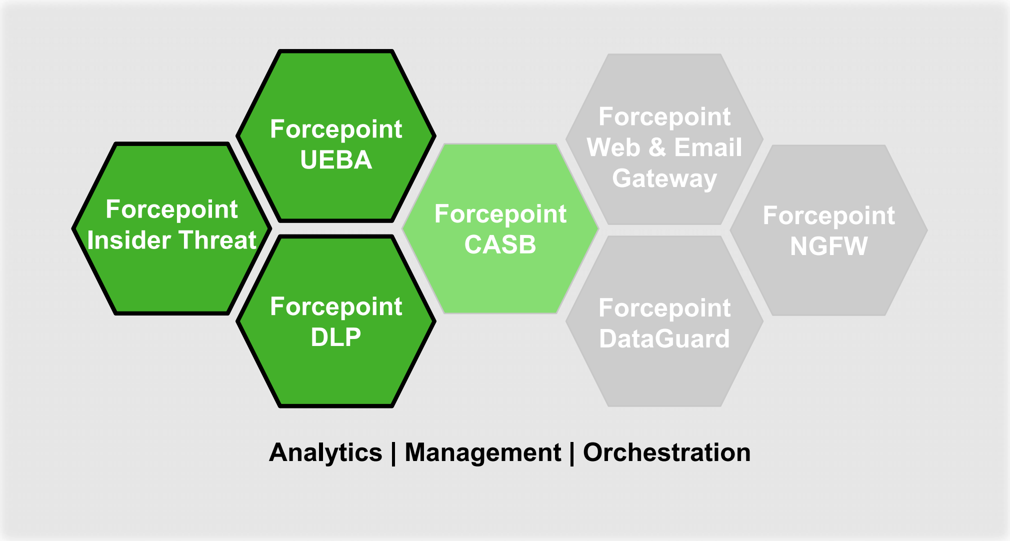
Risk-adaptive security

FOCUS ON THE TRUE CONSTANTS



Understanding the intersection of people, critical data and IP over networks of different trust levels.

FORCEPOINT'S HUMAN POINT SYSTEM



Analytics | Management | Orchestration

THE FORCEPOINT SOLUTION FOR DATA AND USERS

the rhythm of your people **AND** the flow of your data

Forcepoint UEBA

- Risk analytics platform for broad view of user activity and risk scoring
- Context of behavior – not just anomalies
  - Communications + logs + Machine data + HR info
- Out of box analytics + flexibility to adapt to new threats

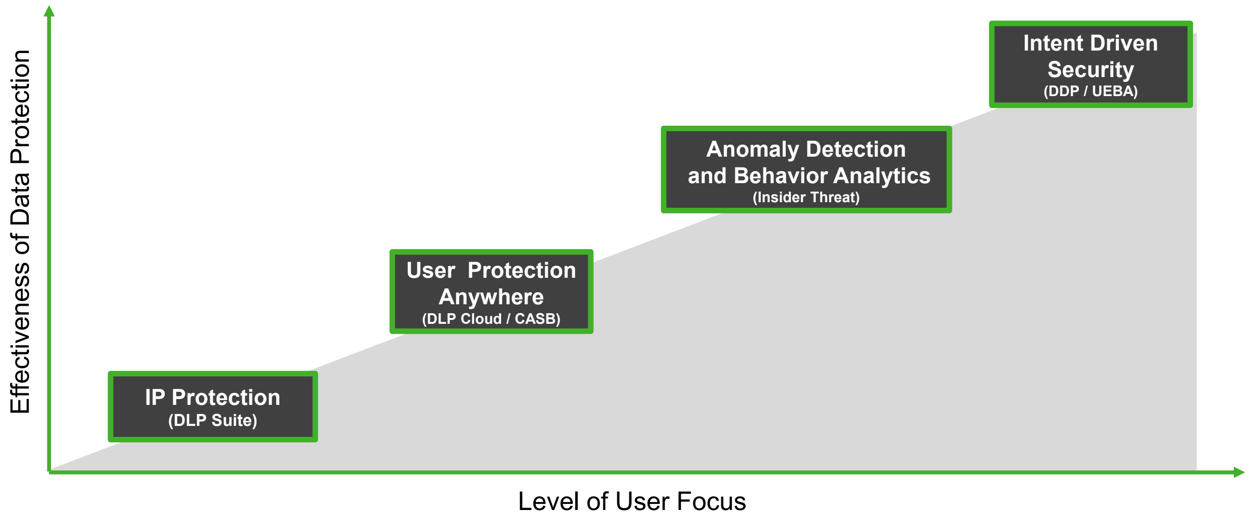
Forcepoint Insider Threat

- Endpoint-based deep visibility and analysis of user behavior
- User risk scoring
  - Baseline & deviations
  - Machine logs + user actions
  - Correlate user across systems
- Detailed monitoring that respects user privacy

Forcepoint DLP

- Identify and control flow of data
  - Cloud
  - Endpoint
  - Network
  - Discovery
- Secure regulated data
- Protect intellectual property

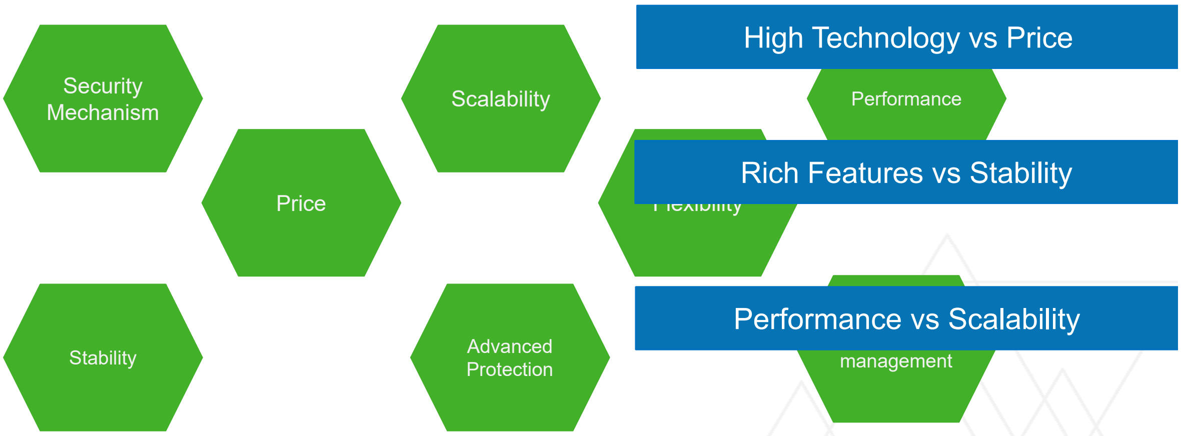
THE JOURNEY TO BETTER DATA PROTECTION AND COMPLIANCE



HUMAN POINT

How do you know who are threats and what the critical assess you lose?

WHAT IS THE MOST IMPORTANT VALUE OF OUR FIREWALL WHICH WE NEED?



High Technology vs Price

Rich Features vs Stability

Performance vs Scalability

Security Mechanism

Price

Scalability

Performance

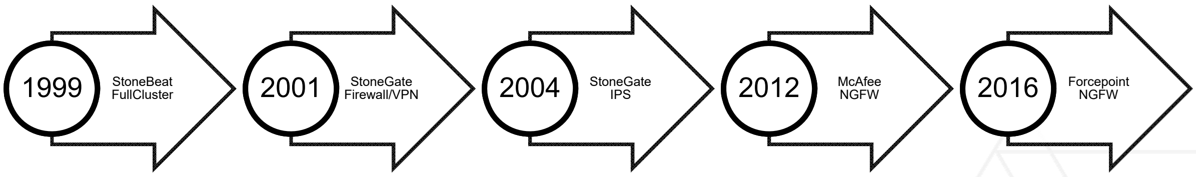
Flexibility

Stability

Advanced Protection

management

Forcepoint'sNGFW Historical Background



1999 StoneBeat FullCluster

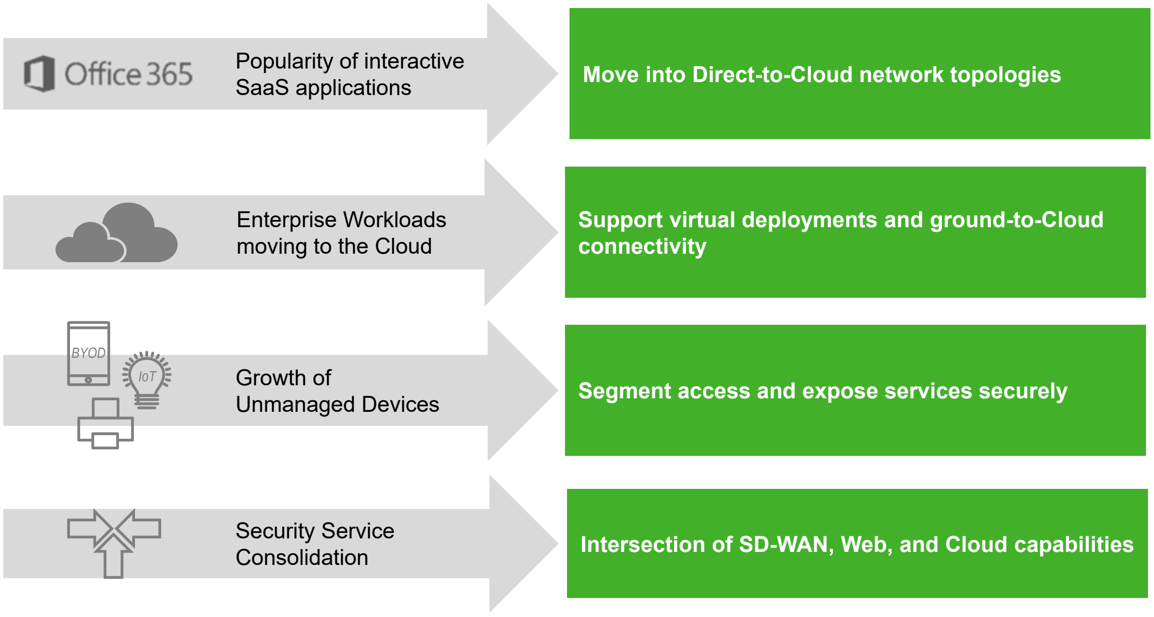
2001 StoneGate Firewall/VPN

2004 StoneGate IPS

2012 McAfee NGFW

2016 Forcepoint NGFW

NETWORK SECURITY IS BEING DRIVEN BY NEW NEEDS



Popularity of interactive SaaS applications → Move into Direct-to-Cloud network topologies

Enterprise Workloads moving to the Cloud → Support virtual deployments and ground-to-Cloud connectivity

Growth of Unmanaged Devices → Segment access and expose services securely

Security Service Consolidation → Intersection of SD-WAN, Web, and Cloud capabilities

Traditional Products Can LIMIT You in this New World

NETWORKING

SD-WAN and Availability weak

- Not built into each level: net, device, admin

SECURITY

Vulnerable to modern attacks

- Bypassed by evasions
- Efficacy of exploits & malware

OPERATIONS

Unmanageable at scale

- Insufficient automation
- Nightmare updates

Why Organizations **Shortlist** Forcepoint

SD-WAN MULTI-LINK™ OPTIMIZATION

Unique and praised by end users VPN Mesh technology

CLUSTERING & HIGH AVAILABILITY

The best clustering capabilities available on the market place

#1 NGFW & IPS SECURITY

Top-ranked security on NSS Labs' NGFW and NGIPS tests

SINGLE-PANE MANAGEMENT

Simply the smartest management system in the industry

OPERATIONAL EFFICIENCY

Zero-touch deployments and one-click updates/upgrades

TRUE ENTERPRISE SOLUTION

Greater Agility with Lower TCO

THE ENDS