How Secure is your Business?

Sometimes watching your six starts with 1s and 0s.

Dave Moorman

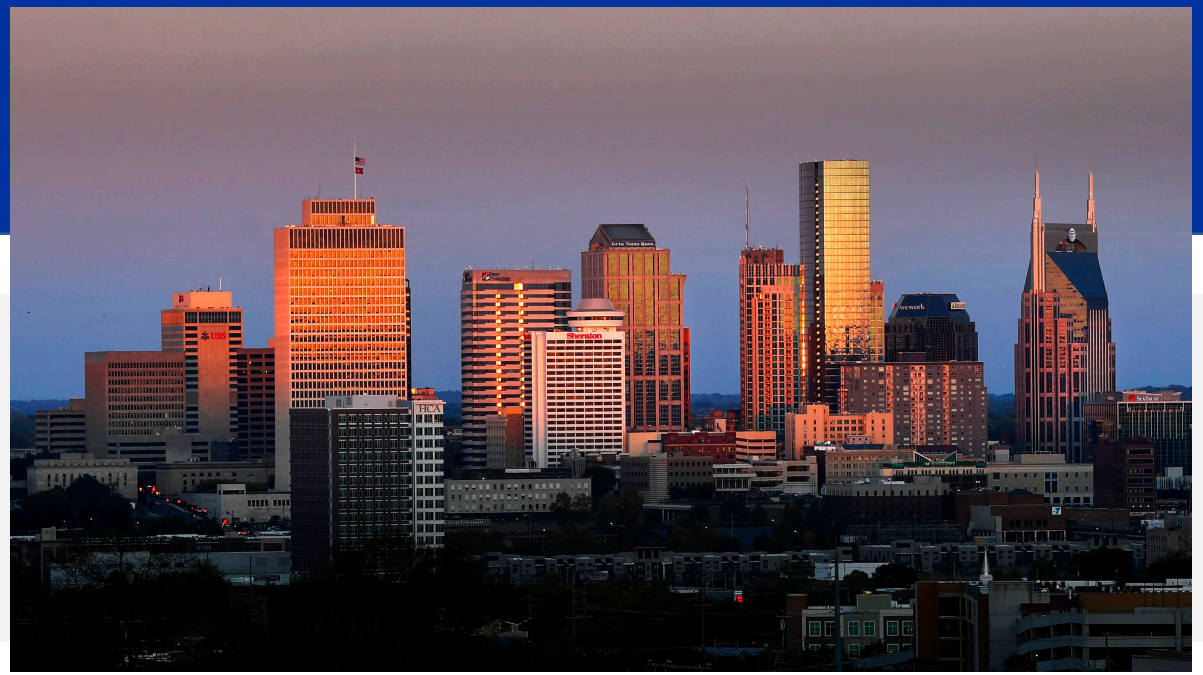
President

I Live in Milton (Atlanta), GA with my wife Kim, Max (23) & Avery (16)

- Architected and built 750+ Business Technology Environments
- Developed industry-standard processes and best practices for the managed services industry in 2005
- 2016 Developed a 12 layer Cyber Security Framework for businesses
- 2018 Developed Advanced Cyber Security practice

NOVATECH

Managed IT Services



- Founded 25+ Years Ago

- 70+ Employees in MITS Division

- Assess, Design, Install and Support Business IT Environments

Managed IT

Delivering world class IT Support since 1992

Cloud Solutions

Your applications and Data in the cloud to enhance Availability, Security & Mobility

Cyber Security Services

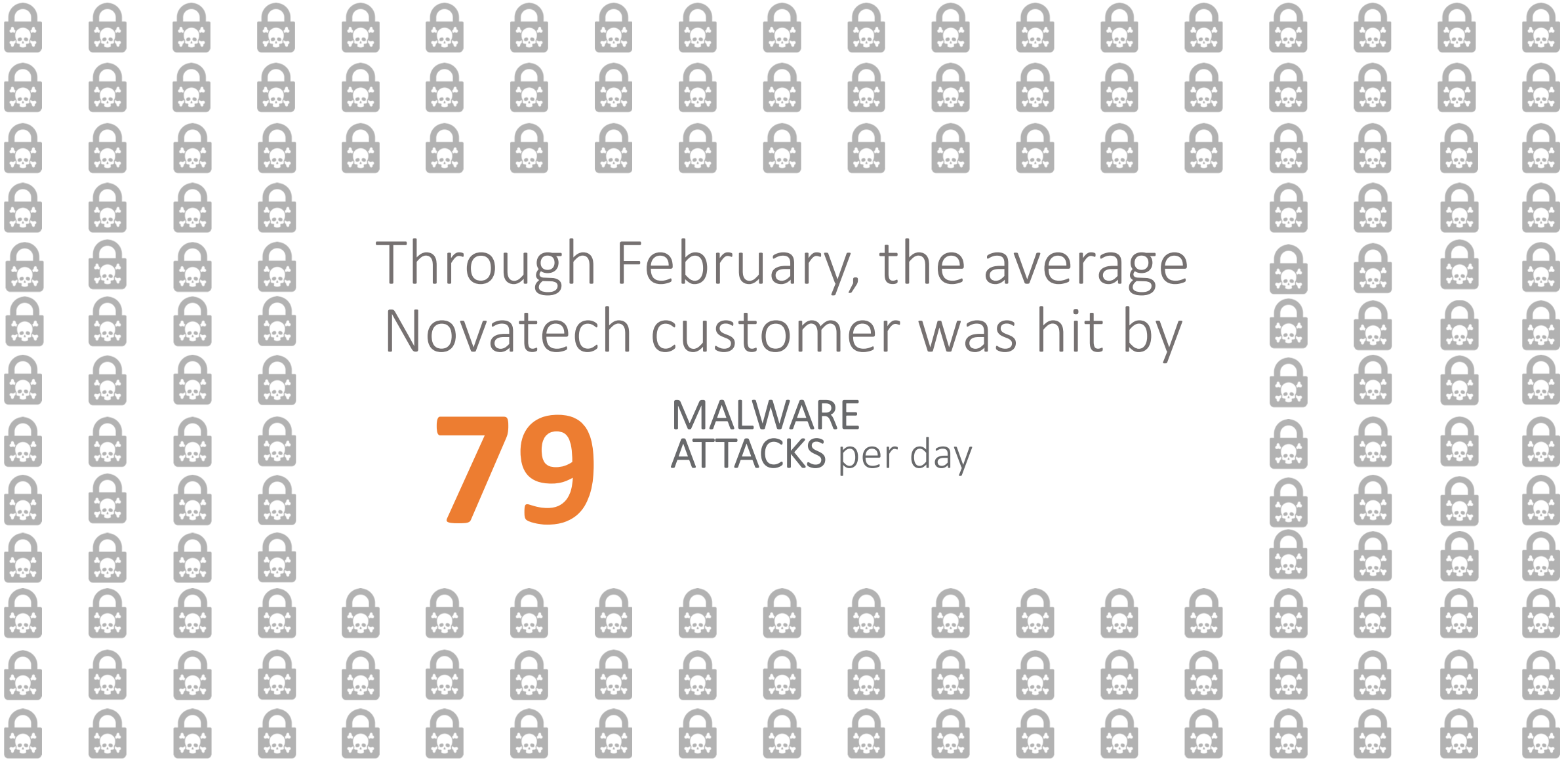
Protect your business from Cyber Attacks with our 12 layer security services

Availability. Security. Mobility for the Modern Business

CYBER SECURITY

A New Headline Every Day

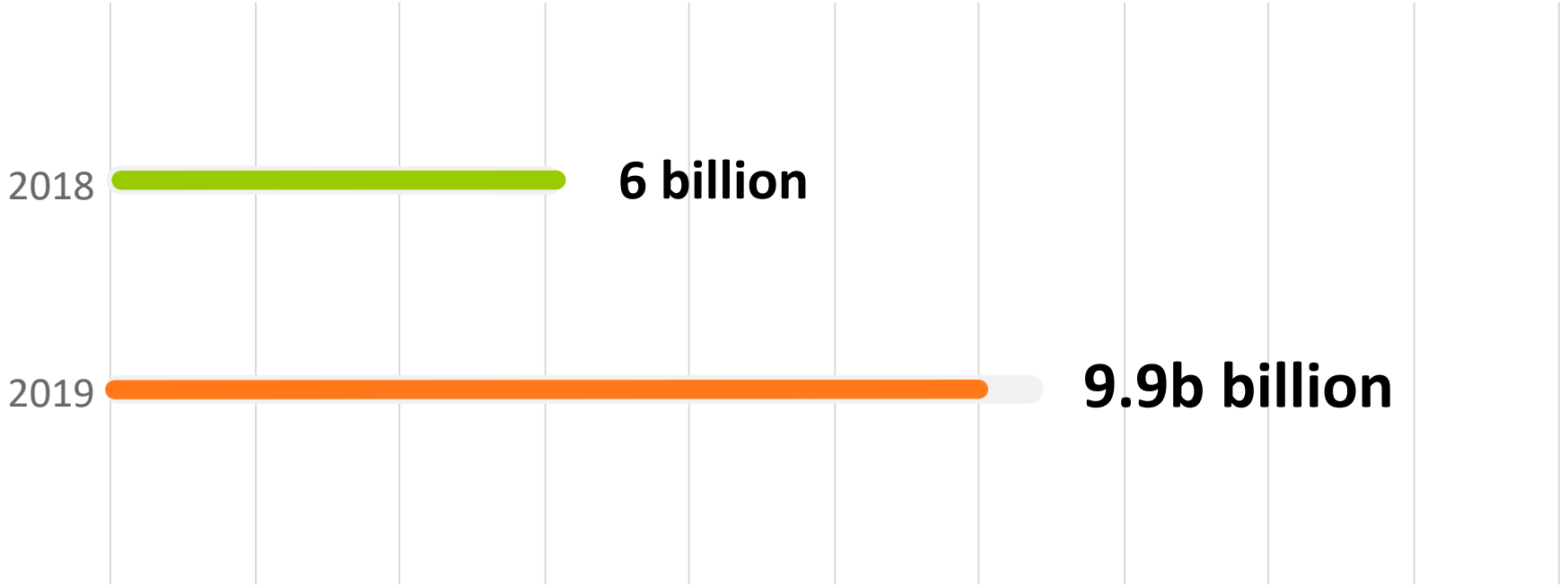
We are all under constant attack!



Through February, the average Novatech customer was hit by

79 MALWARE ATTACKS per day

In 2019 Malware attacks were up 40% compared to 2018. They were up 102% from 2017 to 1018.



Number of phishing attacks the average Novatech customer faced in 2H 2019

2,033

78%

of Internet connections were encrypted with TLS/SSL this year

22%

of all malware used TLS/SSL encryption

Only 5% of customers have deployed TLS/SSL inspection.

Business Impact

$75B

Total cost of ransomware to businesses each year[1]

$3.6M

Average total cost of a data breach[2]

22%

Businesses that had a stoppage because of malware last year[3]

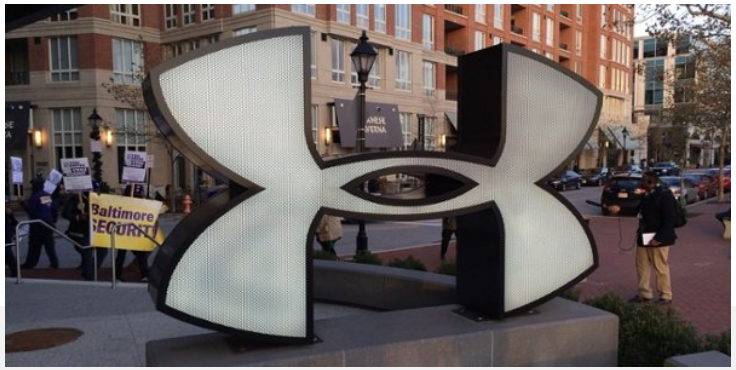
$5B

Global losses due to business email compromise scams as of December 2016[4]

Notable 2018 Cyber Security Breaches

- 5 million records breached
- Date disclosed: April 3, 2018

- 37 million records breached
- Date disclosed: April 2, 2018



- 150 million records breached
- Date disclosed: May 25, 2018

❖ 500 million guest reservations Stolen from its Starwood database.

- **What was affected:** Guest information including phone numbers, email addresses, passport numbers, reservation dates, and some payment card numbers and expiration dates.
- **When it happened:** 2014 — September 2018
- **How it happened:** Hackers accessed the reservation database for Marriott's Starwood hotels, and copied and stole guest information.

The 5th generation of Warfare

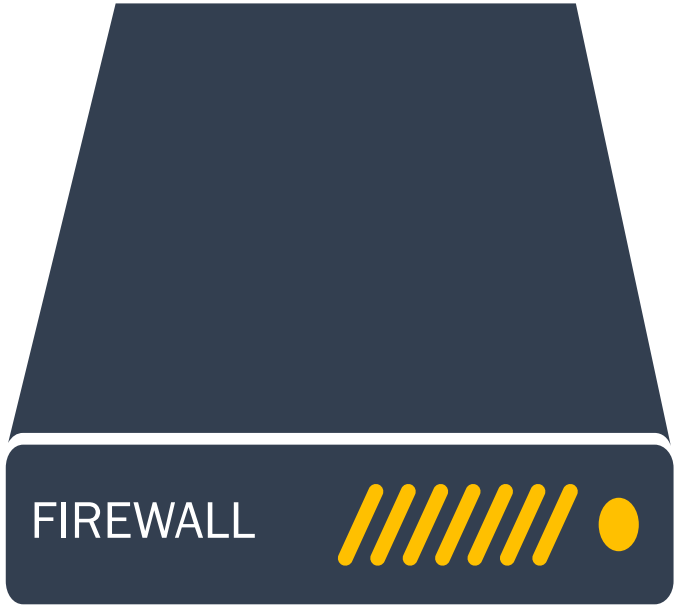
Land

Sea

Aerospace

Space

Cyber



Last 20 years of security:

Got a problem?
BUY A BOX

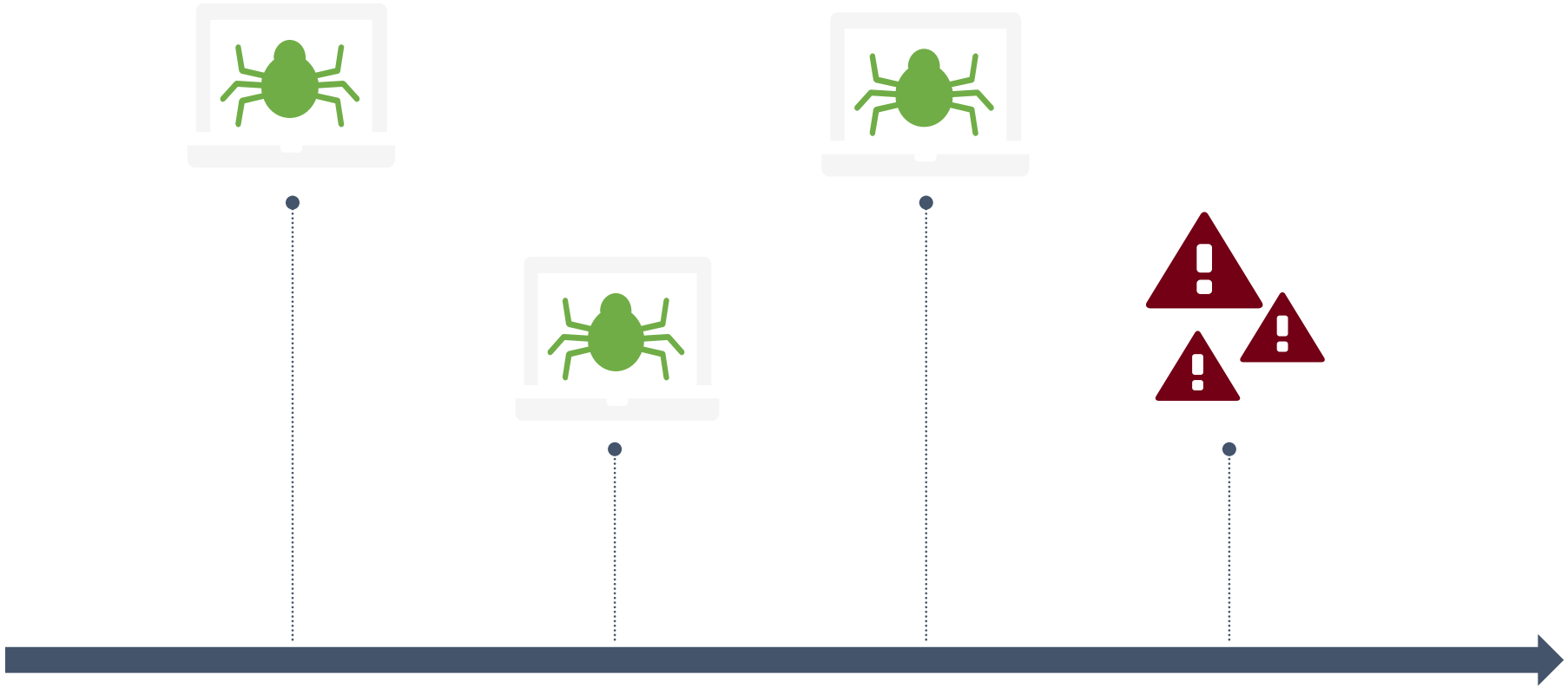
BUT...Then...

Your users have left the building.

And the way we work is changing

And it's exposing your business to new risks

Cloud applications Mobile users Wi-Fi & BYOD



AND...Then

antivirus finds malware *after* an infection.

Evolution of Cyber Crime

OLD

Hacker Organization

- Centralized
- Build from scratch
- Own servers
- Expensive
- Large targets

NEW

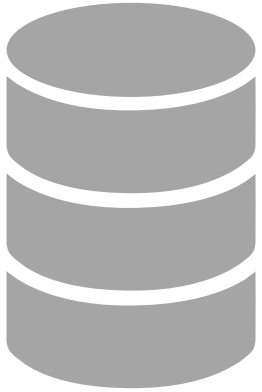
Crime Ecosystem

- Distributed
- Buy or hosted
- Specialize in areas
- Cheap
- Smaller targets

Why is this happening?
Changes in technology

SaaS

Subscribe to applications



IaaS

Rent servers and storage

CaaS

CyberCrime made easier

The Cybercrime Ecosystem.
Cybercrime is easier than ever.

And it's more accessible to everyone!

Silk Road
anonymous marketplace

Ag

Hydra

Market places

Постоянно требуется написание автозаливных инжектов под
Zeus/SpyEye

от 2000$ за выполненный проект

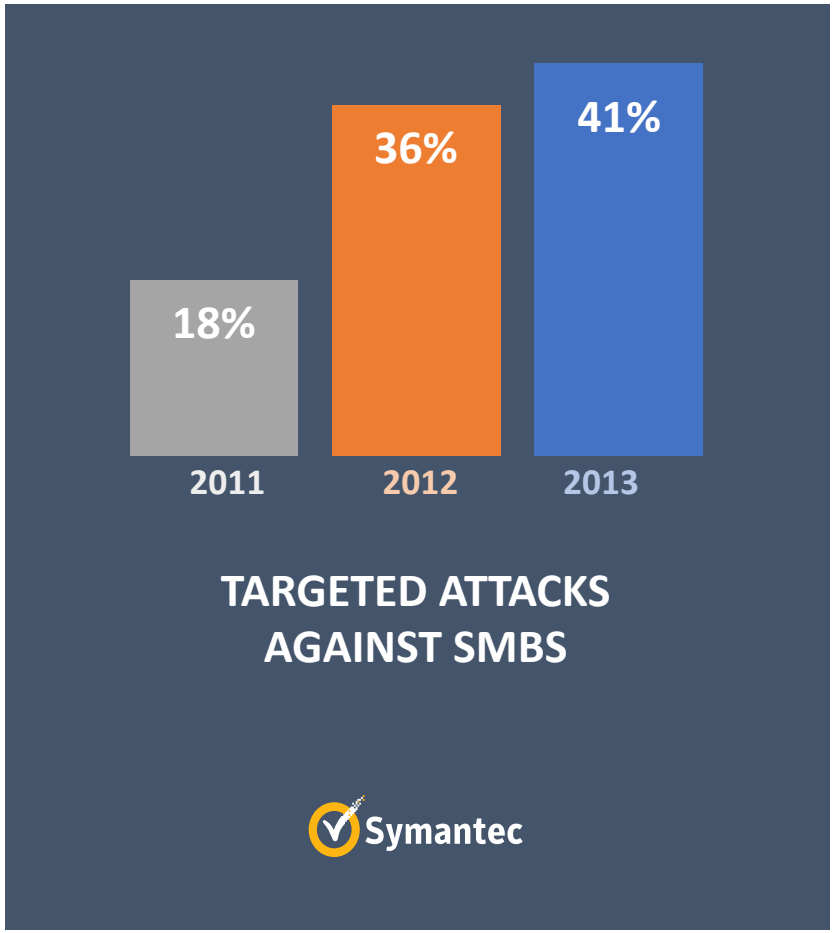
Job postings

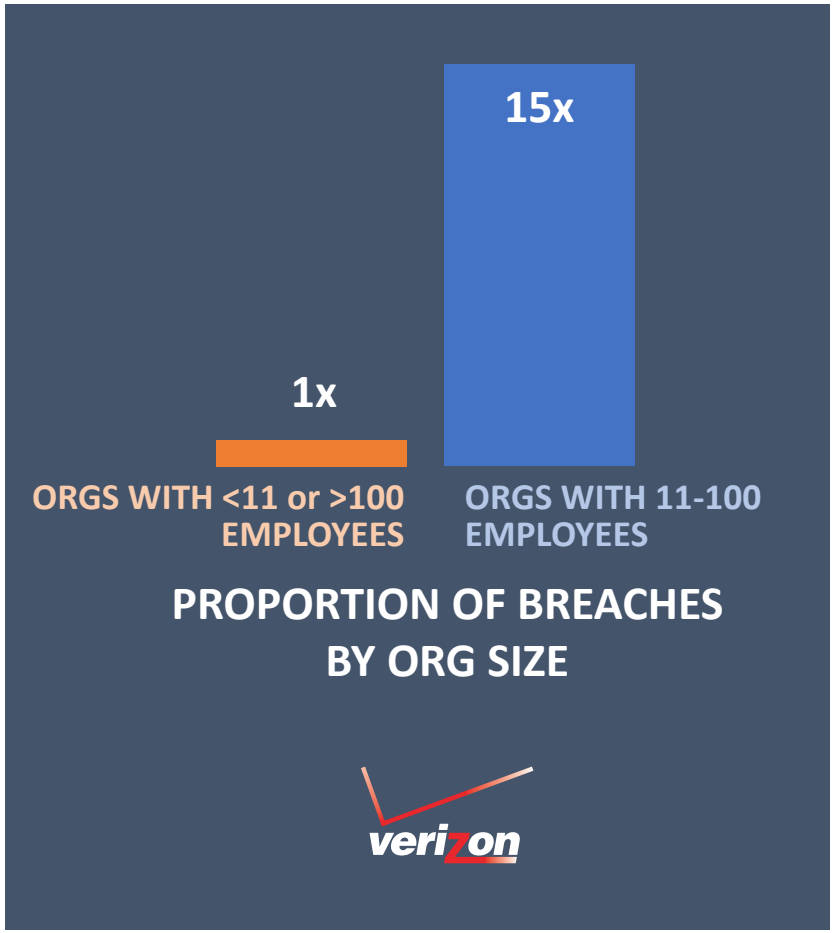
WebMoney

Perfect Money
Just perfect

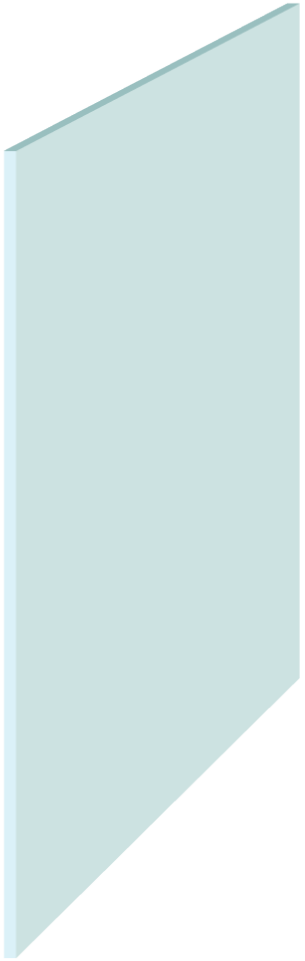
Payment systems

SMB's in the crosshairs





Security & Risk Mitigation: a Layered Approach



NORMAL GLASS

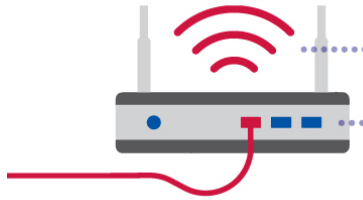
BULLET PROOF GLASS

Consisting of Normal glass and Polycarbonate layers

Security & Risk Mitigation: a Layered Approach

MODERN SMB CYBERSECURITY POSTURE

NOVATECH



YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

Office 365

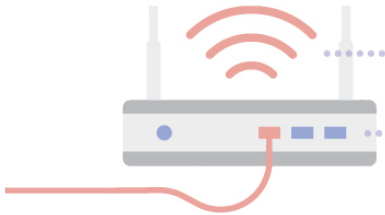
15 LAYER CYBERSECURITY DEFENSE

1.	**NGFW**	Next Generation Firewall
2.	**GEO IP**	Geolocation Internet Protocol Tracking
3.	**Patching**	OS/Application Patching
4.	**EDR**	End Point Detection & Response
5.	**ATP**	Advanced Threat Protection
6.	**UAT**	User Awareness Training
7.	**MFA**	Multi-Factor Authentication
8.	**VPN**	Virtual Private Network
9.	**RTPM**	Real Time Privilege Management
10.	**DWM**	Dark Web Monitoring
11.	**CDNS**	Cloud Predictive Network Security
12.	**CCS**	Crypto Containment System
13.	**DB&R**	Data Backup & Recovery
14.	**SEIM**	Security Event Incident Management
15.	**SOC**	Security Operations Center

NOVATECH

MODERN SMB CYBERSECURITY POSTURE

NOVATECH



YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

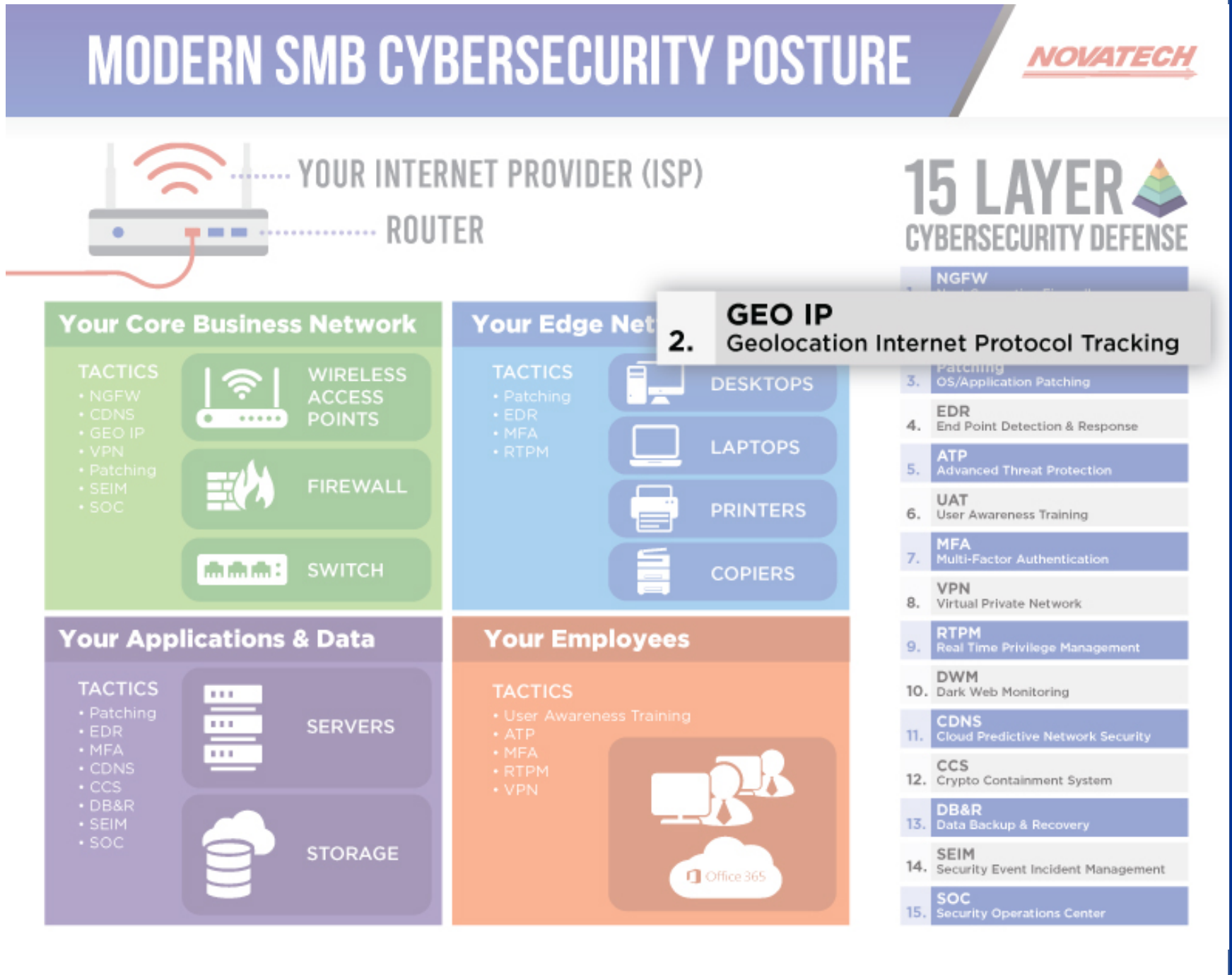
TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

Office 365

15 LAYER CYBERSECURITY DEFENSE

1. **NGFW** Next Generation Firewall
2. GEO IP Geolocation Internet Protocol Tracking
3. **Patching** OS/Application Patching
4. **EDR** End Point Detection & Response
5. **ATP** Advanced Threat Protection
6. **UAT** User Awareness Training
7. **MFA** Multi-Factor Authentication
8. **VPN** Virtual Private Network
9. **RTPM** Real Time Privilege Management
10. **DWM** Dark Web Monitoring
11. **CDNS** Cloud Predictive Network Security
12. **CCS** Crypto Containment System
13. **DB&R** Data Backup & Recovery
14. **SEIM** Security Event Incident Management
15. **SOC** Security Operations Center

A **next generation firewall (NGFW)** is, as Gartner defines it, a “deep-packet inspection **firewall** that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the **firewall**



Geo-IP filtering, a technology that can block web traffic from entire countries, can be an effective way to stop hackers from attacking your business. As the name suggests, it blocks network connections based on geographic location – information it gets based on **IP** addresses.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH

YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

LAPTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

Office 365

15 LAYER CYBERSECURITY DEFENSE

1. NGFW — Next Generation Firewall
2. GEO IP
3. **Patching** — OS/Application Patching
4. End Point Detection & Response
5. ATP — Advanced Threat Protection
6. UAT — User Awareness Training
7. MFA — Multi-Factor Authentication
8. VPN — Virtual Private Network
9. RTPM — Real Time Privilege Management
10. DWM — Dark Web Monitoring
11. CDNS — Cloud Predictive Network Security
12. CCS — Crypto Containment System
13. DB&R — Data Backup & Recovery
14. SEIM — Security Event Incident Management
15. SOC — Security Operations Center

Patching is a process to repair a vulnerability or a flaw that is identified after the release of an application or a software. Newly released patches can fix a bug or a security flaw, can help to enhance applications with new features, fix security vulnerability.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH

YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

Office 365

15 LAYER CYBERSECURITY DEFENSE

1. NGFW — Next Generation Firewall
2. GEO IP — Geolocation Internet Protocol Tracking
3. Patching — OS/Application Patching
4. EDR — End Point Detection & Response
5. Advanced Threat Protection
6. UAT — User Awareness Training
7. MFA — Multi-Factor Authentication
8. VPN — Virtual Private Network
9. RTPM — Real Time Privilege Management
10. DWM — Dark Web Monitoring
11. CDNS — Cloud Predictive Network Security
12. CCS — Crypto Containment System
13. DB&R — Data Backup & Recovery
14. SEIM — Security Event Incident Management
15. SOC — Security Operations Center

Endpoint Detection and Response (EDR), also known as Endpoint Threat Detection and Response is a cyber technology that continually monitors and responds to mitigate cyber threats.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH

YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

Office 365

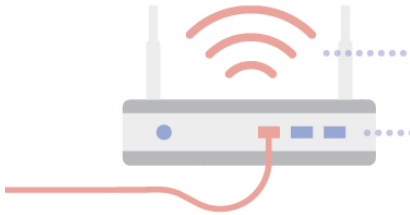
15 LAYER CYBERSECURITY DEFENSE

1. NGFW — Next Generation Firewall
2. GEO IP — Geolocation Internet Protocol Tracking
3. Patching — OS/Application Patching
4. EDR
5. ATP — Advanced Threat Protection
6. User Awareness Training
7. MFA — Multi-Factor Authentication
8. VPN — Virtual Private Network
9. RTPM — Real Time Privilege Management
10. DWM — Dark Web Monitoring
11. CDNS — Cloud Predictive Network Security
12. CCS — Crypto Containment System
13. DB&R — Data Backup & Recovery
14. SEIM — Security Event Incident Management
15. SOC — Security Operations Center

Advanced threat protection (ATP) refers to a category of security solutions that defend against sophisticated malware or hacking-based attacks targeting sensitive data.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH



YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

Office 365

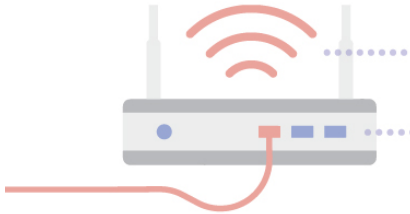
15 LAYER CYBERSECURITY DEFENSE

1. **NGFW** Next Generation Firewall
2. **GEO IP** Geolocation Internet Protocol Tracking
3. **Patching** OS/Application Patching
4. **EDR** End Point Detection & Response
5. **ATP** Advanced Threat Protection
6. **UAT** User Awareness Training
7. **MFA** Multi-Factor Authentication
8. **VPN** Virtual Private Network
9. **RTPM** Real Time Privilege Management
10. **DWM** Dark Web Monitoring
11. **CDNS** Cloud Predictive Network Security
12. **CCS** Crypto Containment System
13. **DB&R** Data Backup & Recovery
14. **SEIM** Security Event Incident Management
15. **SOC** Security Operations Center

What is User Security **Awareness**? ... **User** security **awareness training** provides employees with the information they need to understand the dangers of social engineering, detect potential attacks, and take the appropriate actions to protect your business with security best practices.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH



YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

PRINTERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

Office 365

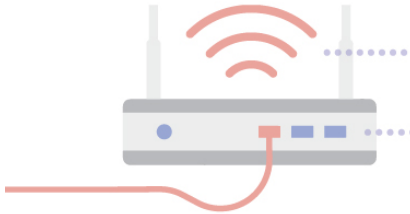
15 LAYER CYBERSECURITY DEFENSE

1. **NGFW** Next Generation Firewall
2. **GEO IP** Geolocation Internet Protocol Tracking
3. **Patching** OS/Application Patching
4. **EDR** End Point Detection & Response
5. **ATP** Advanced Threat Protection
6. **UAT** User Awareness Training
7. **MFA** Multi-Factor Authentication
8. Virtual Private Network
9. **RTPM** Real Time Privilege Management
10. **DWM** Dark Web Monitoring
11. **CDNS** Cloud Predictive Network Security
12. **CCS** Crypto Containment System
13. **DB&R** Data Backup & Recovery
14. **SEIM** Security Event Incident Management
15. **SOC** Security Operations Center

Multi-factor authentication (MFA) or (2FA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH



YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

PRINTERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

Office 365

15 LAYER CYBERSECURITY DEFENSE

1. **NGFW** Next Generation Firewall
2. **GEO IP** Geolocation Internet Protocol Tracking
3. **Patching** OS/Application Patching
4. **EDR** End Point Detection & Response
5. **ATP** Advanced Threat Protection
6. **UAT** User Awareness Training
7. **MFA** Multi-Factor Authentication
8. **VPN** Virtual Private Network
9. **RTPM** Real Time Privilege Management
10. **DWM** Dark Web Monitoring
11. **CDNS** Cloud Predictive Network Security
12. **CCS** Crypto Containment System
13. **DB&R** Data Backup & Recovery
14. **SEIM** Security Event Incident Management
15. **SOC** Security Operations Center

A **virtual private network (VPN)** extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH

YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employe

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

Office 365

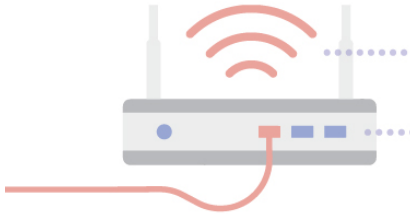
15 LAYER CYBERSECURITY DEFENSE

1. **NGFW** Next Generation Firewall
2. **GEO IP** Geolocation Internet Protocol Tracking
3. **Patching** OS/Application Patching
4. **EDR** End Point Detection & Response
5. **ATP** Advanced Threat Protection
6. **UAT** User Awareness Training
7. **MFA** Multi-Factor Authentication
8. **VPN**
9. **RTPM** Real Time Privilege Management
10. Dark Web Monitoring
11. **CDNS** Cloud Predictive Network Security
12. **CCS** Crypto Containment System
13. **DB&R** Data Backup & Recovery
14. **SEIM** Security Event Incident Management
15. **SOC** Security Operations Center

Real Time Privilege Management (RTPM)
Restricting Admin accounts will enhance all your cybersecurity efforts and is one of the best ways to help stop malware and thwart attackers. Some estimates say that having users run with Standard privileges can help mitigate 94% or more of Microsoft vulnerabilities.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH



YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Tra
- ATP
- MFA
- RTPM
- VPN

Office 365

15 LAYER CYBERSECURITY DEFENSE

1. **NGFW** Next Generation Firewall
2. **GEO IP** Geolocation Internet Protocol Tracking
3. **Patching** OS/Application Patching
4. **EDR** End Point Detection & Response
5. **ATP** Advanced Threat Protection
6. **UAT** User Awareness Training
7. **MFA** Multi-Factor Authentication
8. **VPN** Virtual Private Network
9. **RTPM** Real Time Privilege Management

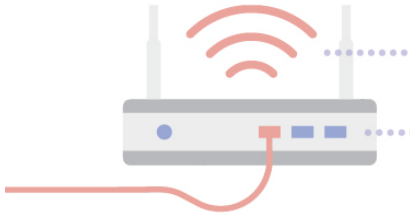
10. DWM Dark Web Monitoring

11. **CDNS** Cloud Predictive Network Security
12. **CCS** Crypto Containment System
13. **DB&R** Data Backup & Recovery
14. **SEIM** Security Event Incident Management
15. **SOC** Security Operations Center

Dark web monitoring (DWM), also known as cyber monitoring, is an identity theft prevention product that enables you to monitor your identity information on the dark web, and receive notifications if your information is found online.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH



YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Tra
- ATP
- MFA
- RTPM
- VPN

Office 365

15 LAYER CYBERSECURITY DEFENSE

1. **NGFW** Next Generation Firewall
2. **GEO IP** Geolocation Internet Protocol Tracking
3. **Patching** OS/Application Patching
4. **EDR** End Point Detection & Response
5. **ATP** Advanced Threat Protection
6. **UAT** User Awareness Training
7. **MFA** Multi-Factor Authentication
8. **VPN** Virtual Private Network
9. **RTPM** Real Time Privilege Management
10. **DWM** Dark Web Monitoring

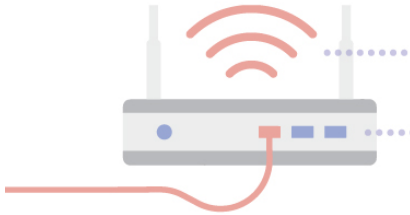
11. CDNS Cloud Predictive Network Security

12. **CCS** Crypto Containment System
13. **DB&R** Data Backup & Recovery
14. **SEIM** Security Event Incident Management
15. **SOC** Security Operations Center

Cloud Predictive Network Security (CPNS) OpenDNS is a company and service that extends the Domain Name System by adding features such as phishing protection and optional content filtering in addition to DNS lookup, if its DNS servers are used.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH



YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

Office 365

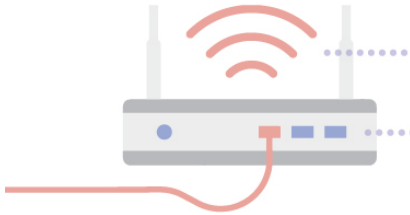
15 LAYER CYBERSECURITY DEFENSE

1. **NGFW** Next Generation Firewall
2. **GEO IP** Geolocation Internet Protocol Tracking
3. **Patching** OS/Application Patching
4. **EDR** End Point Detection & Response
5. **ATP** Advanced Threat Protection
6. **UAT** User Awareness Training
7. **MFA** Multi-Factor Authentication
8. **VPN** Virtual Private Network
9. **RTPM** Real Time Privilege Management
10. **DWM** Dark Web Monitoring
11. **CDNS**
12. **CCS** Crypto Containment System
13. **DB&R** Data Backup & Recovery
14. **SEIM** Security Event Incident Management
15. **SOC** Security Operations Center

Crypto Containment System (CCS) is a monitoring agent that was developed by Novatech to look for encrypted files. Once detected the system drops drive shares (i.e. D) to contain the outbreak of a ransomware attack.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH



YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

Office 365

15 LAYER CYBERSECURITY DEFENSE

1. **NGFW** Next Generation Firewall
2. **GEO IP** Geolocation Internet Protocol Tracking
3. **Patching** OS/Application Patching
4. **EDR** End Point Detection & Response
5. **ATP** Advanced Threat Protection
6. **UAT** User Awareness Training
7. **MFA** Multi-Factor Authentication
8. **VPN** Virtual Private Network
9. **RTPM** Real Time Privilege Management
10. **DWM** Dark Web Monitoring
11. **CDNS** Cloud Predictive Network Security
12. **CCS** Crypto Containment System
13. **DB&R** Data Backup & Recovery
14. **SEIM** Security Event Incident Management
15. **SOC** Security Operations Center

A **data backup** is the result of copying or archiving files and folders for the purpose of being able to restore them in case of **data** loss. **Data** loss can be caused by many things ranging from computer viruses to hardware failures to file corruption to fire, flood, or theft (etc).

- ✓ RTO – Recovery Time Objective
- ✓ RPO – Recovery Point Objective
- ✓ Data Retention – How far back can I go to perform a restore in time.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH

YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

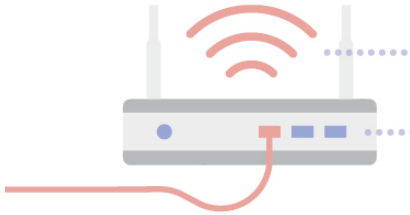
15 LAYER CYBERSECURITY DEFENSE

1. **NGFW** Next Generation Firewall
2. **GEO IP** Geolocation Internet Protocol Tracking
3. **Patching** OS/Application Patching
4. **EDR** End Point Detection & Response
5. **ATP** Advanced Threat Protection
6. **UAT** User Awareness Training
7. **MFA** Multi-Factor Authentication
8. **VPN** Virtual Private Network
9. **RTPM** Real Time Privilege Management
10. **DWM** Dark Web Monitoring
11. **CDNS** Cloud Predictive Network Security
12. **CCS** Crypto Containment System
13. **DB&R** Data Backup & Recovery
14. **SEIM** Security Event Incident Management
15. **SOC** Security Operations Center

Security information and event management (SIEM), software products and services combine security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH



YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

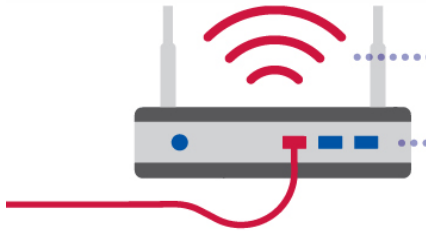
15 LAYER CYBERSECURITY DEFENSE

1. **NGFW** Next Generation Firewall
2. **GEO IP** Geolocation Internet Protocol Tracking
3. **Patching** OS/Application Patching
4. **EDR** End Point Detection & Response
5. **ATP** Advanced Threat Protection
6. **UAT** User Awareness Training
7. **MFA** Multi-Factor Authentication
8. **VPN** Virtual Private Network
9. **RTPM** Real Time Privilege Management
10. **DWM** Dark Web Monitoring
11. **CDNS** Cloud Predictive Network Security
12. **CCS** Crypto Containment System
13. **DB&R** Data Backup & Recovery
14. **SEIM**
15. **SOC** Security Operations Center

Security Operation Center (SOC) A security operations center is a facility where information systems and IT Infrastructure are monitored, assessed, and defended.

MODERN SMB CYBERSECURITY POSTURE

NOVATECH



YOUR INTERNET PROVIDER (ISP)

ROUTER

Your Core Business Network

TACTICS
- NGFW
- CDNS
- GEO IP
- VPN
- Patching
- SEIM
- SOC

WIRELESS ACCESS POINTS

FIREWALL

SWITCH

Your Edge Network

TACTICS
- Patching
- EDR
- MFA
- RTPM

DESKTOPS

LAPTOPS

PRINTERS

COPIERS

Your Applications & Data

TACTICS
- Patching
- EDR
- MFA
- CDNS
- CCS
- DB&R
- SEIM
- SOC

SERVERS

STORAGE

Your Employees

TACTICS
- User Awareness Training
- ATP
- MFA
- RTPM
- VPN

Office 365

15 LAYER CYBERSECURITY DEFENSE

1. **NGFW** Next Generation Firewall
2. **GEO IP** Geolocation Internet Protocol Tracking
3. **Patching** OS/Application Patching
4. **EDR** End Point Detection & Response
5. **ATP** Advanced Threat Protection
6. **UAT** User Awareness Training
7. **MFA** Multi-Factor Authentication
8. **VPN** Virtual Private Network
9. **RTPM** Real Time Privilege Management
10. **DWM** Dark Web Monitoring
11. **CDNS** Cloud Predictive Network Security
12. **CCS** Crypto Containment System
13. **DB&R** Data Backup & Recovery
14. **SEIM** Security Event Incident Management
15. **SOC** Security Operations Center

The 3-2-1 Backup Strategy

A 3-2-1 strategy means having at least 3 total copies of your data, 2 of which are local (On Site) but on different equipment and 1 is offsite

Onsite Production Data

Onsite Backup Data

Offsite Backup Data

RTO: Recovery Time Objective

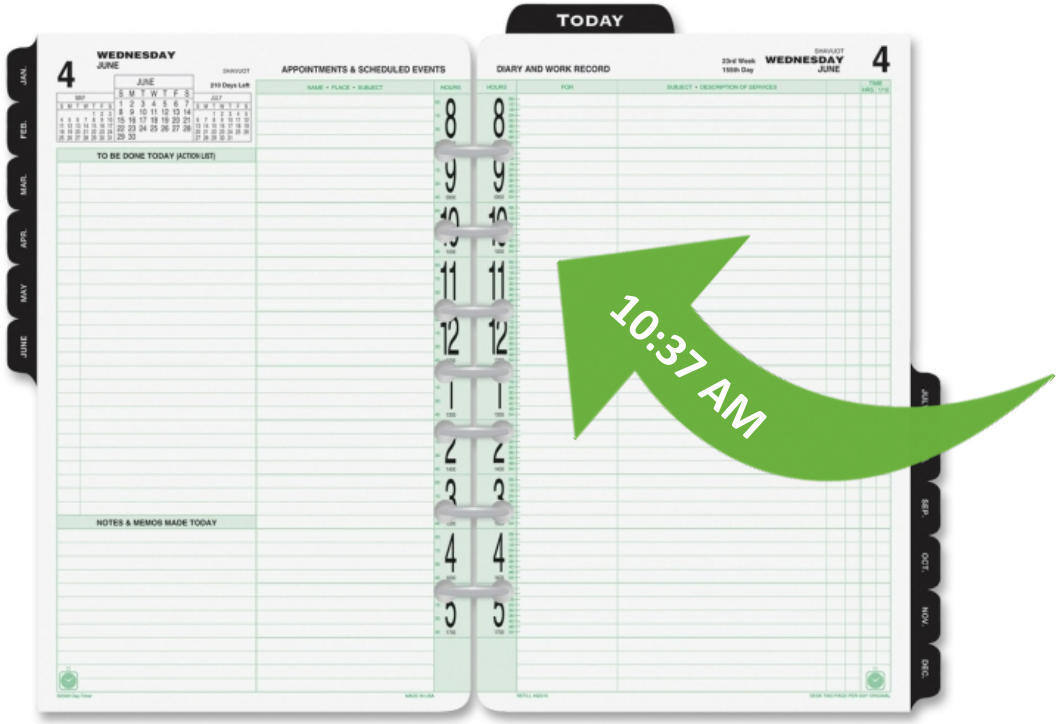
The TIME it will take to recover your data.

How long can you afford to not have access to your data?

- A day?
- An hour?
- 15 minutes?
- Not at all?

RPO: Recovery Point Objective

The POINT at which your last backup was performed.

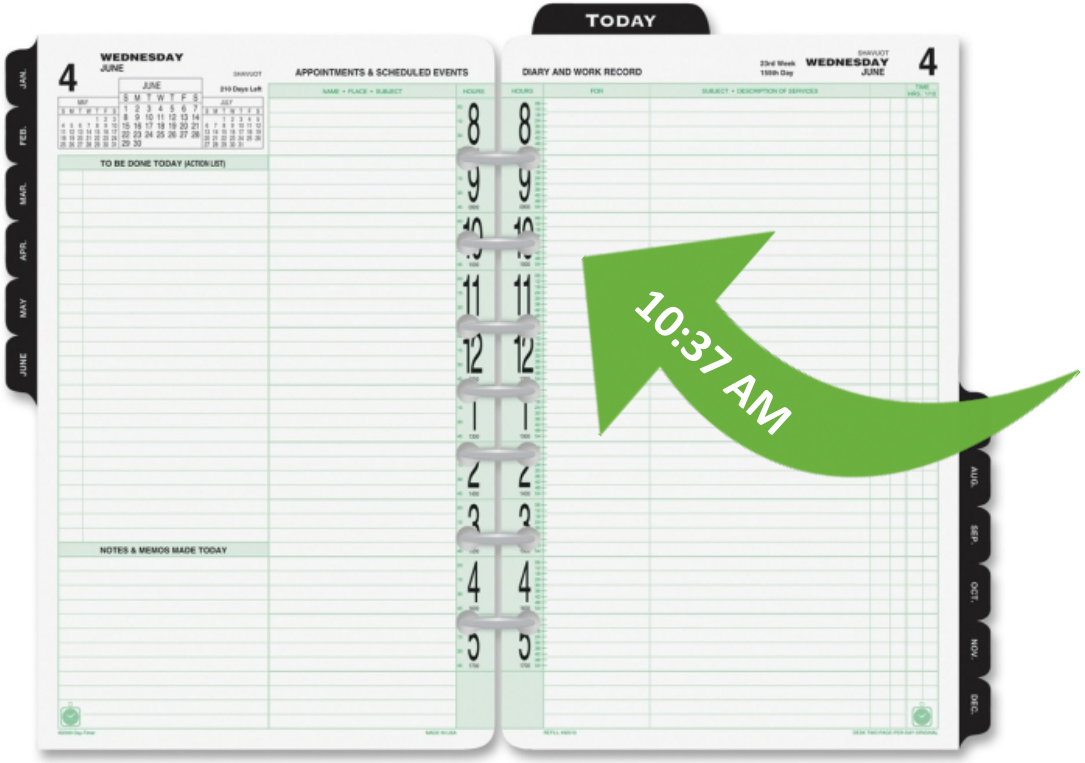


How much data can you afford to lose…data that was created in:

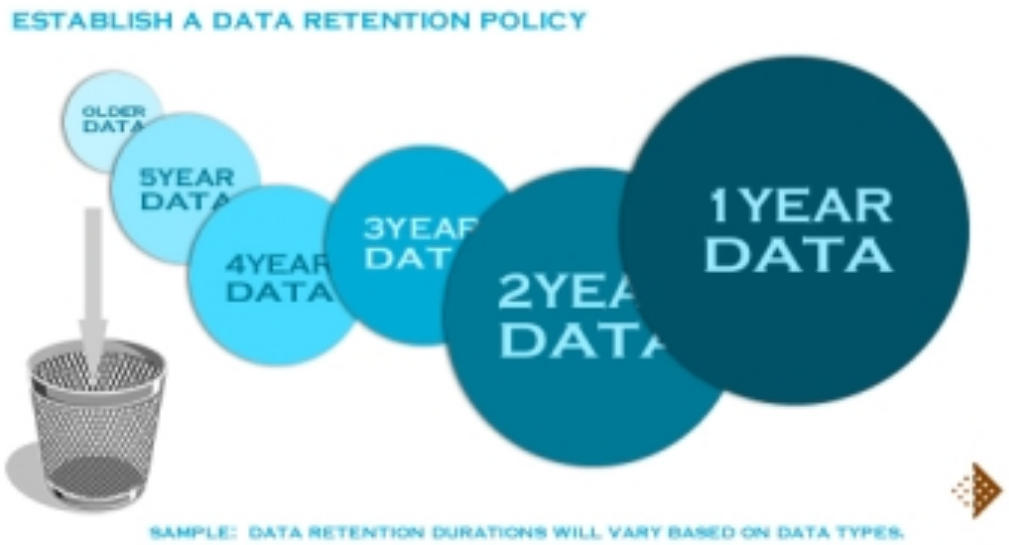
- An hour?
- A day?
- 15 Minutes?
- None at all?

RPT / RTO

These two factors, along with your budget / requirements, should determine how, and how often, your system should be backed up.



Establishing a Data Retention Policy



An organization's data retention policies are guidelines that describe what data will be stored, how long it will be kept and other factors concerning the retention of the data, based on:

- Operational needs
- Legal requirements - Compliance
- Insurance requirements
- Personal Feelings ☺

The overall goal is to organize and save information so it can be searched and accessed at a later date and to dispose of information that is no longer needed.

Data Backup Capacity Planning

Creating a plan based on current *backup capacity requirements* will assist you in forecasting your storage needs for a given budget cycle. For example:

Our standard recommendation is 4 times your current data footprint. That means:

2 Terabytes of Production Data = 8 TB of Available Backup storage.

Many variables must be considered:

- Rate of data change
- Backup file compression
- Backup frequency
- Even your chosen backup application

Off-Site Data vs Offsite Images

Servers & Production Data

Offsite Backup

Backed up Production Data in DR format

Servers & Production Data

Offsite Backup

Server Images in Bootable file format in DRaaS format

* These 2 types of offsite backups deliver 2 different results

BUSINESS TECH TALKS

NOVATECH

A One-Page BDR Plan

	Hardware/Software Failure e.g. Server Failure / Crash	Site Failure e.g. Fire, Tornado, Theft	Geographic Failure e.g. Tornado, Flood, Hurricane, Earthquake
What is an acceptable RTO for my organization? (Minutes, Hours, Days)			
What is an acceptable RPO for my organization? (Minutes, Hours, Days)			
How far back do I need/want to go back in time? (Days, Months, Years)			
Does my Industry have data Compliance criteria? (Days, Months, Years)			
Is backup data encryption a requirement?	On Premises (Local)?	In Transit?	At Rest in the Cloud?
Is the environment virtual, physical, or hybrid?			