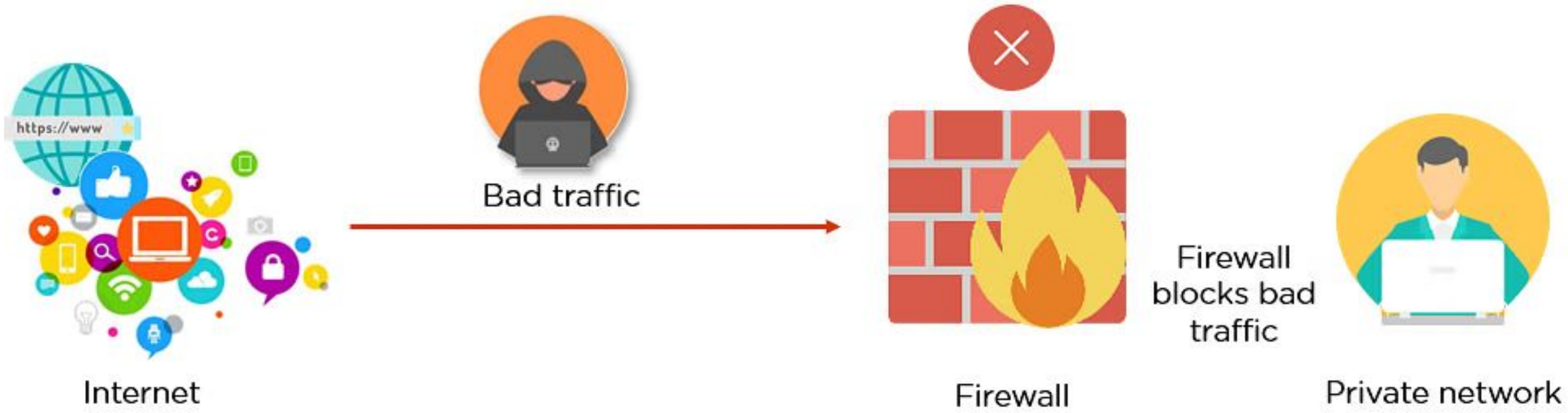
Enterprise Capabilities

What are Enterprise Capabilities?

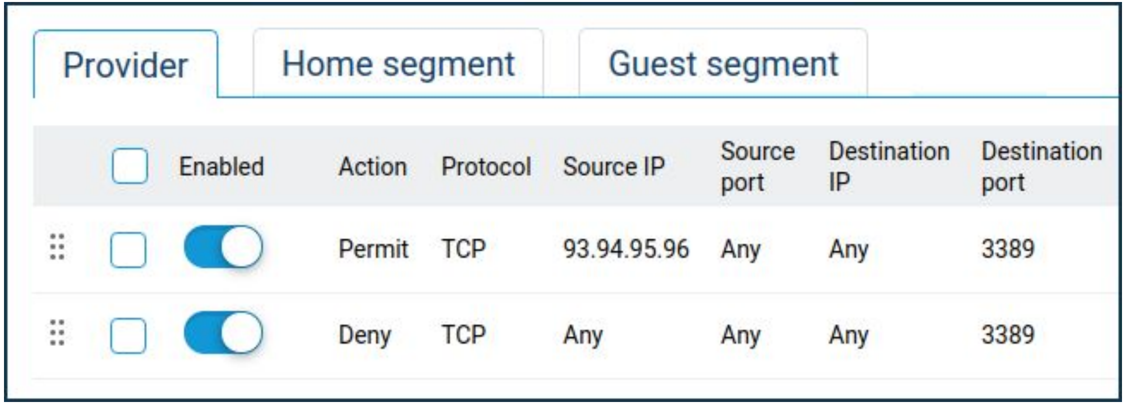
Enterprise Capabilities

- Firewalls
- IDS/IPS
- Web Filter
- OS Security
- Secure Protocols
- Email Security
- Uncategorized Capabilities

Firewalls


https://www
Bad traffic
Internet
Firewall
Firewall blocks bad traffic
Private network

Rules



	□	Enabled	Action	Protocol	Source IP	Source port	Destination IP	Destination port
⠿	□	●	Permit	TCP	93.94.95.96	Any	Any	3389
⠿	□	●	Deny	TCP	Any	Any	Any	3389

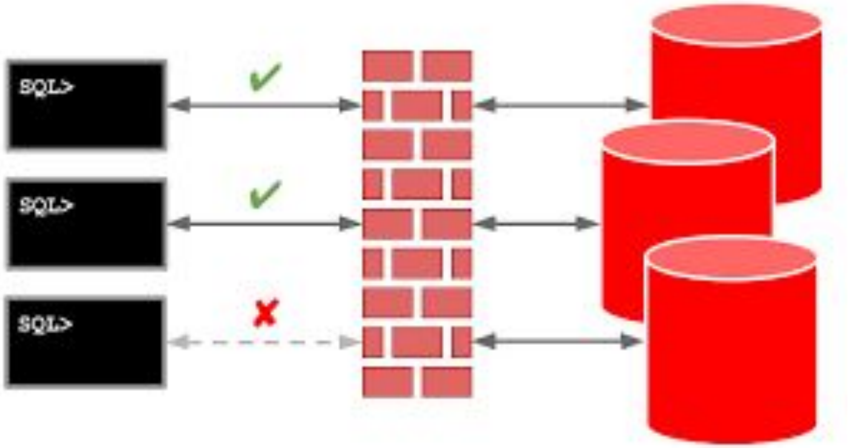
Rule 1:

Permit all TCP connections from 93.94.95.96 on any port to any destination connecting to the remote desktop protocol (3389)

Rule 2:

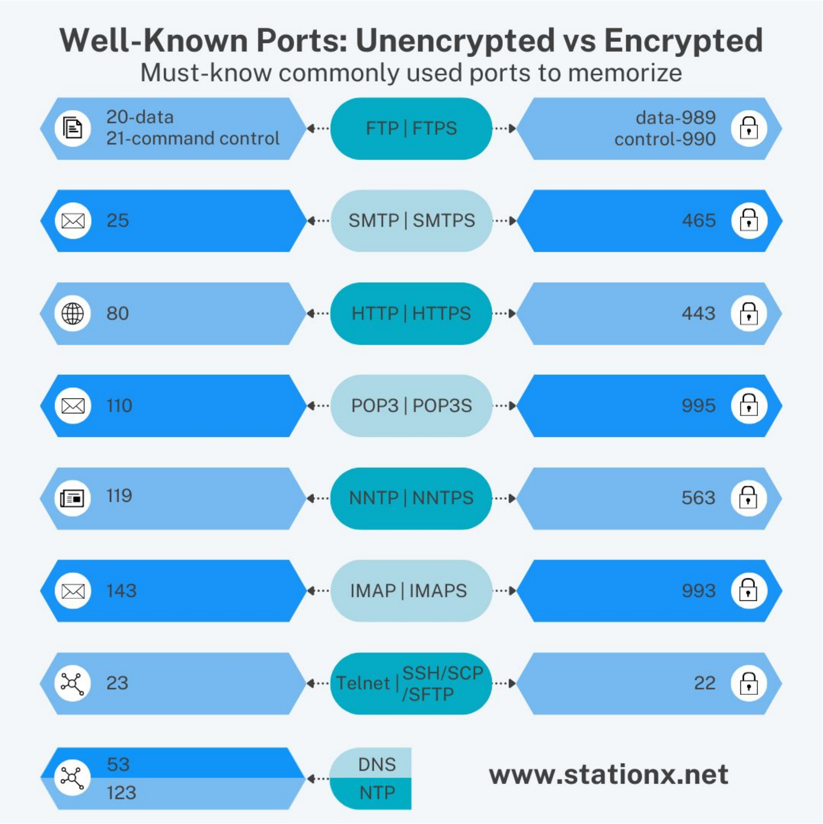
Deny all other RDP (3389) connections regardless of source and destination.

Access Lists



- The collection of rules that define what traffic is allowed and what traffic is denied.
- The default rule should be to deny all.
- Include only trusted sources and destinations
- Regularly audit these lists

Ports/Protocols



Well-Known Ports: Unencrypted vs Encrypted

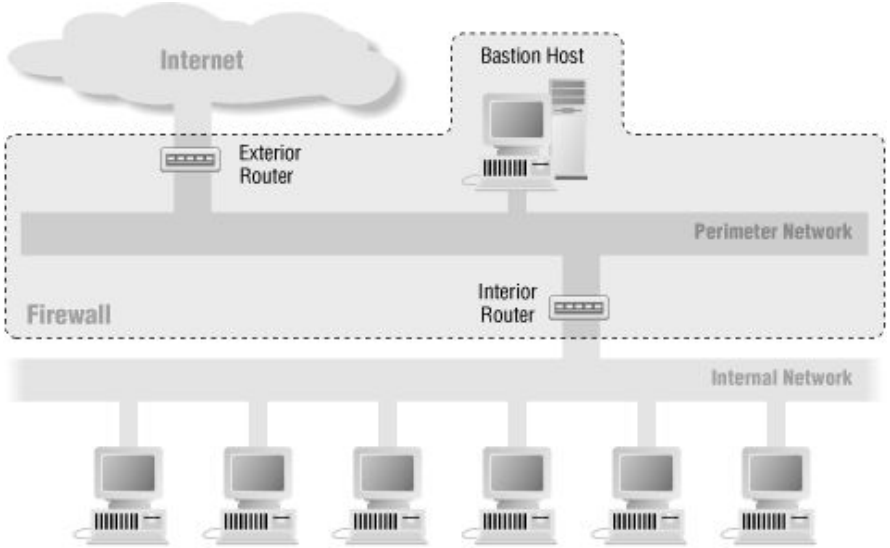
Must-know commonly used ports to memorize

20-data 21-command control	FTP | FTPS	data-989 control-990
25	SMTP | SMTPS	465
80	HTTP | HTTPS	443
110	POP3 | POP3S	995
119	NNTP | NNTPS	563
143	IMAP | IMAPS	993
23	Telnet | SSH/SCP /SFTP	22
53 123	DNS NTP	

www.stationx.net

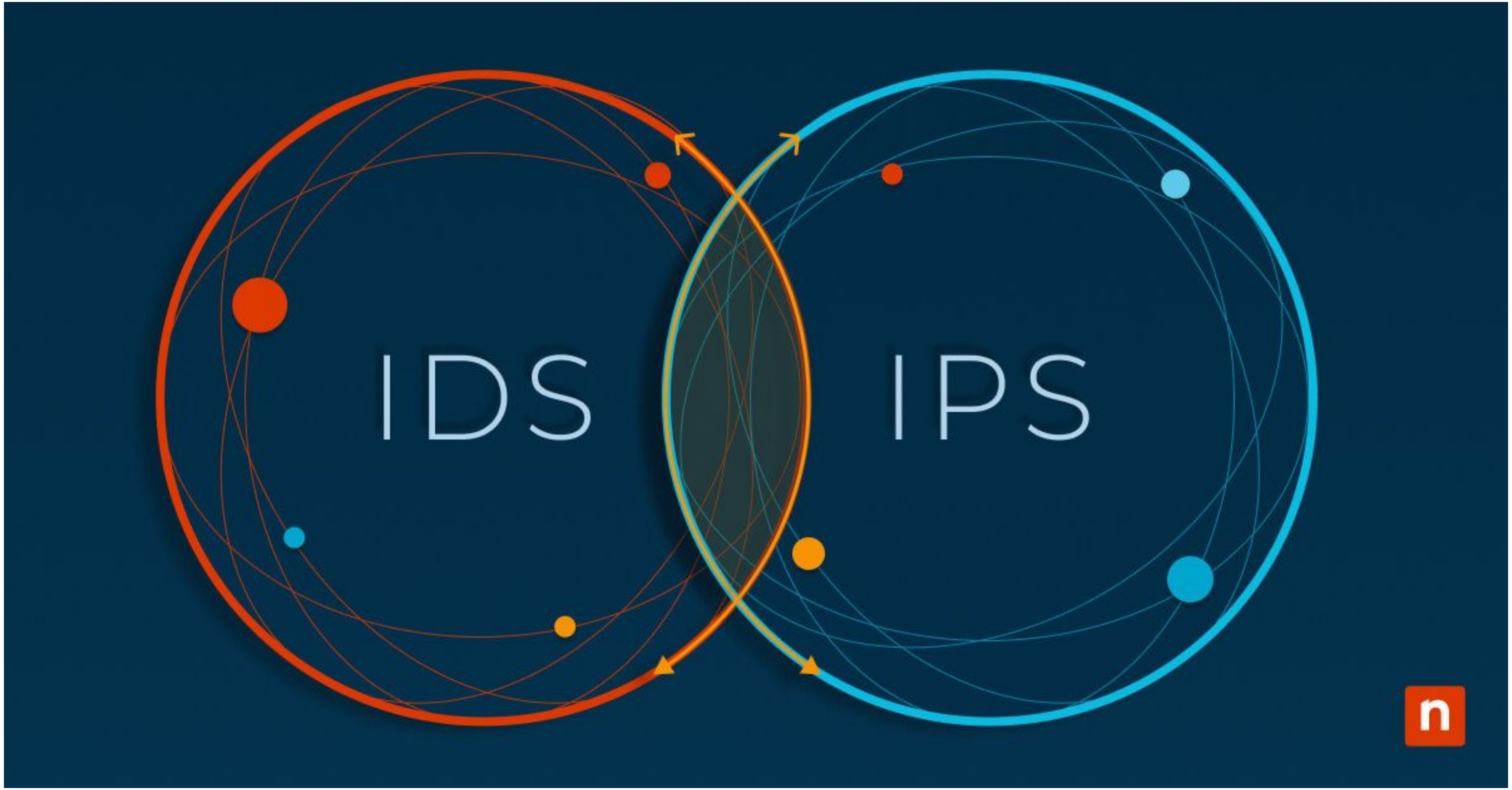
- Every network connection occurs over a port using a specific protocol.
- Transmission protocols include TCP, UDP, and ICMP
- Close all unused ports to reduce the attack surface
- Restrict or block insecure protocols (FTP, HTTP)

Screened Subnets

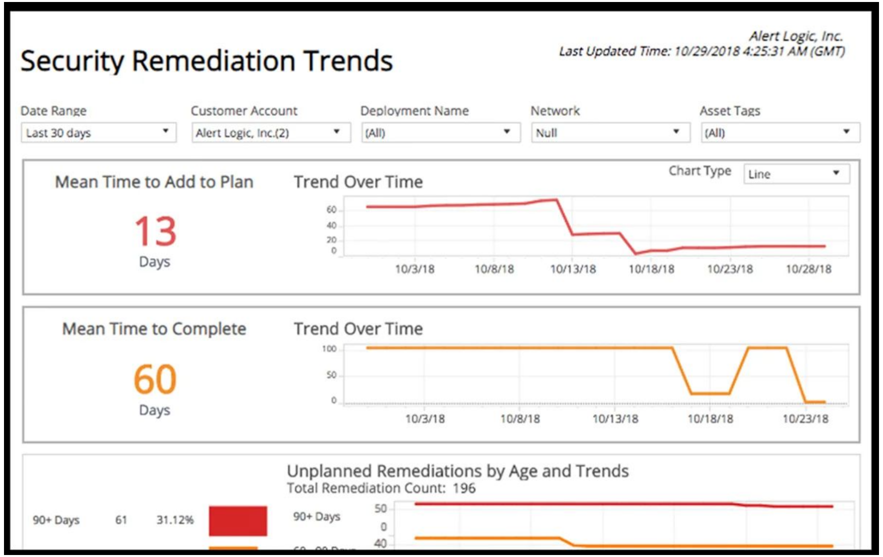


- Also known as a demilitarized zone (DMZ)
- Subnetwork that contains the external-facing services to an untrusted network (like the internet)
- Use to isolate and protect internal networks from external threats

IDS/IPS



Trends



Security Remediation Trends

Alert Logic, Inc.
Last Updated Time: 10/29/2018 4:25:31 AM (GMT)

Date Range	Customer Account	Deployment Name	Network	Asset Tags
Last 30 days	Alert Logic, Inc.(2)	(All)	Null	(All)

Chart Type: Line

Mean Time to Add to Plan
13
Days

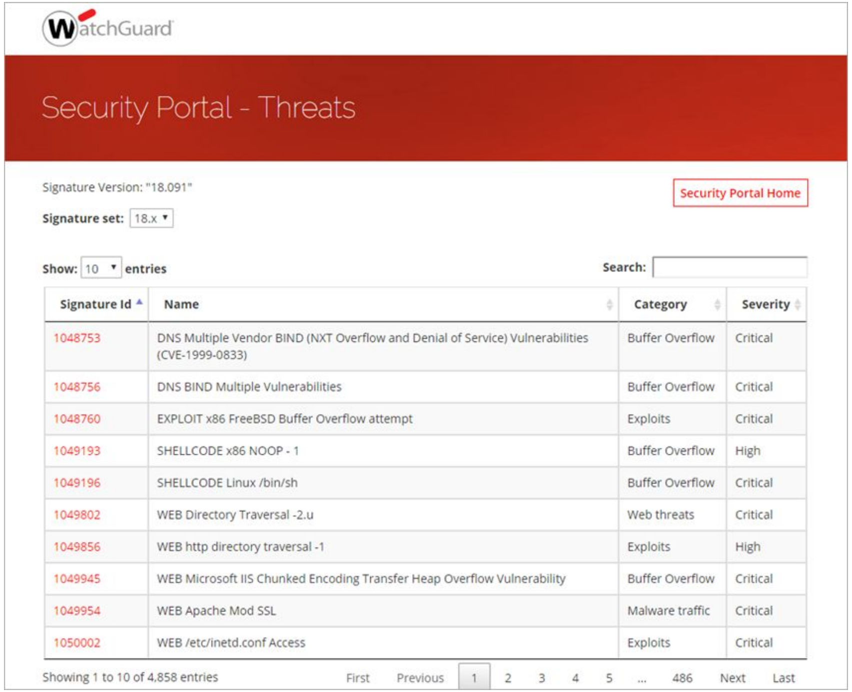
Mean Time to Complete
60
Days

Unplanned Remediations by Age and Trends
Total Remediation Count: 196

90+ Days	61	31.12%

- Unusual patterns that may indicate potential threats or anomalies
- Use machine learning and behavioral analysis tools to detect anomalies
- Integrate threat intelligence feeds to keep the IDS/IPS informed

Signatures



Security Portal - Threats

Signature Version: "18.091"

Security Portal Home

Signature set: 18.x

Show: 10 entries

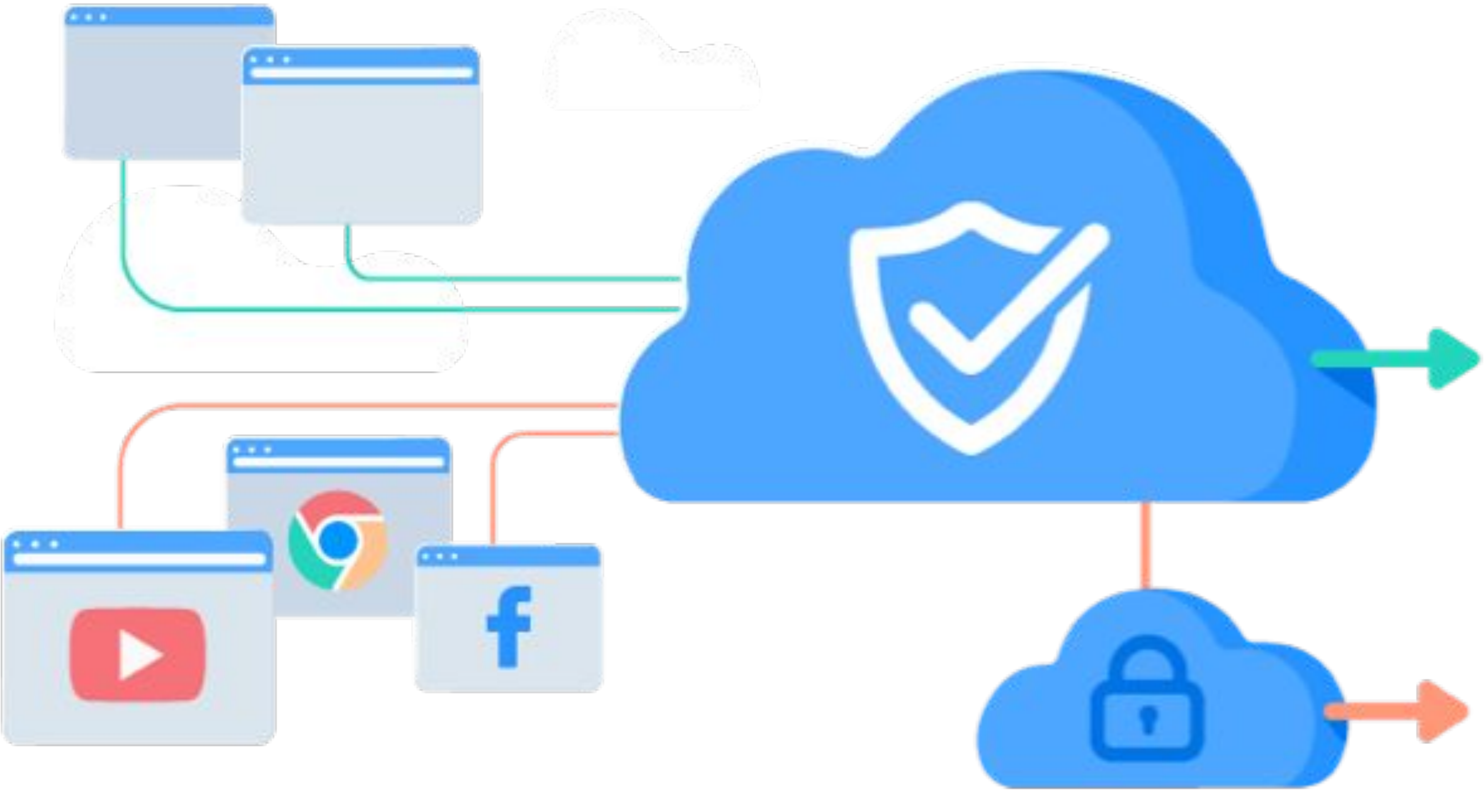
Search:

Signature Id	Name	Category	Severity
1048753	DNS Multiple Vendor BIND (NXT Overflow and Denial of Service) Vulnerabilities (CVE-1999-0833)	Buffer Overflow	Critical
1048756	DNS BIND Multiple Vulnerabilities	Buffer Overflow	Critical
1048760	EXPLOIT x86 FreeBSD Buffer Overflow attempt	Exploits	Critical
1049193	SHELLCODE x86 NOOP - 1	Buffer Overflow	High
1049196	SHELLCODE Linux /bin/sh	Buffer Overflow	Critical
1049802	WEB Directory Traversal -2.u	Web threats	Critical
1049856	WEB http directory traversal -1	Exploits	High
1049945	WEB Microsoft IIS Chunked Encoding Transfer Heap Overflow Vulnerability	Buffer Overflow	Critical
1049954	WEB Apache Mod SSL	Malware traffic	Critical
1050002	WEB /etc/inetd.conf Access	Exploits	Critical

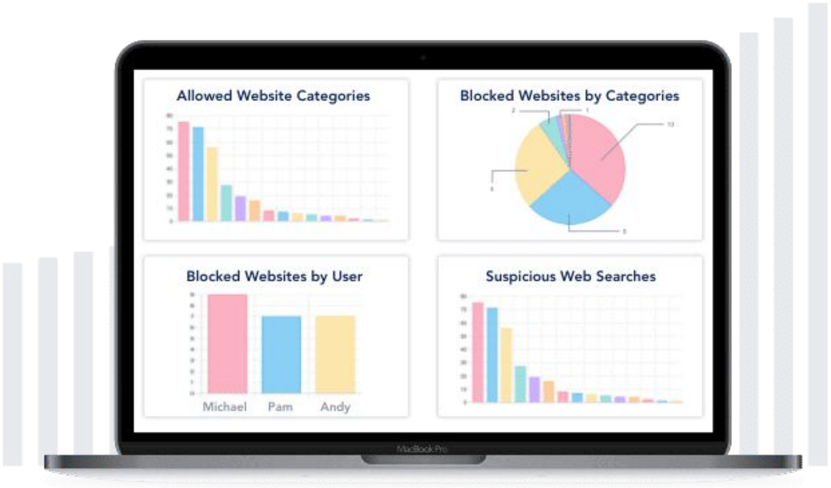
Showing 1 to 10 of 4,858 entries

- Predefined patterns of malicious activities used to detect known threats
- Update signatures to ensure detection of the latest known threats.
- Develop custom signatures based on the unique traffic patterns and threats specific to your organization

Web Filter

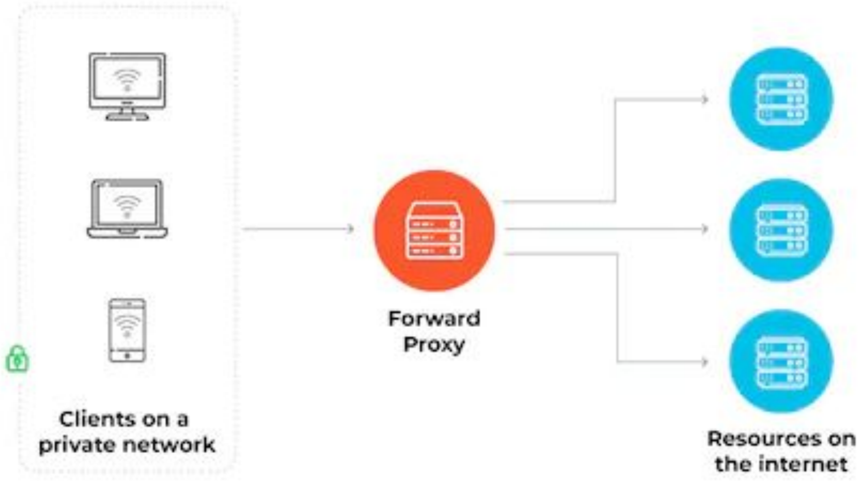


Agent-Based



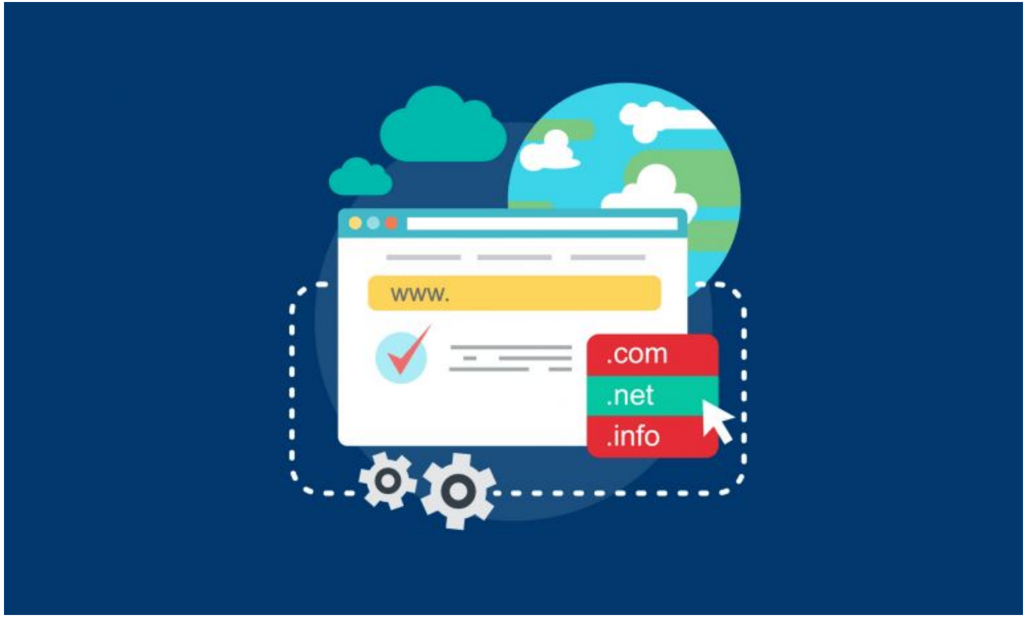
- Installed on endpoints
- Enforce web access policies directly on the device
- Provides consistent filtering regardless of the user's location or network

Centralized Proxy



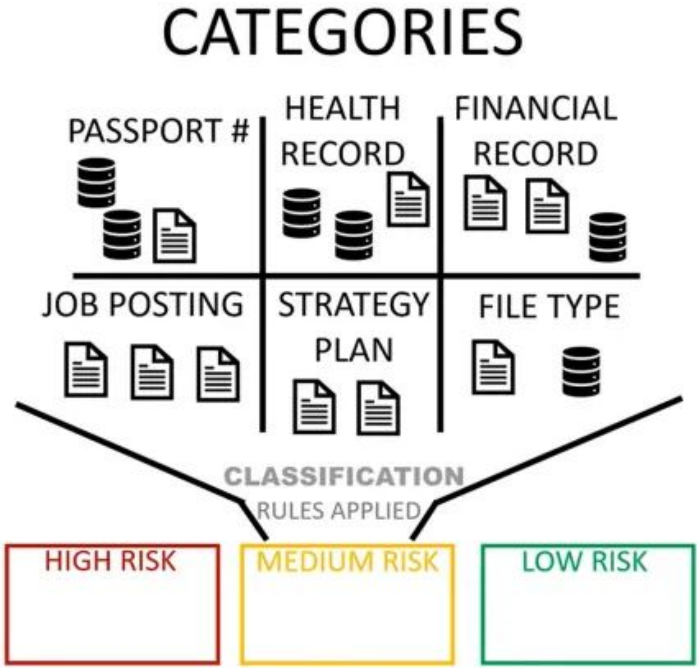
- All internet traffic is routed through
- Centralized monitoring and control of web traffic
- Simplified policy management

URL Scanning



- Inspect and analyze web addresses before allowing access
- Detect and block access to known malicious websites, phishing sites, and other harmful content

Content Categorization



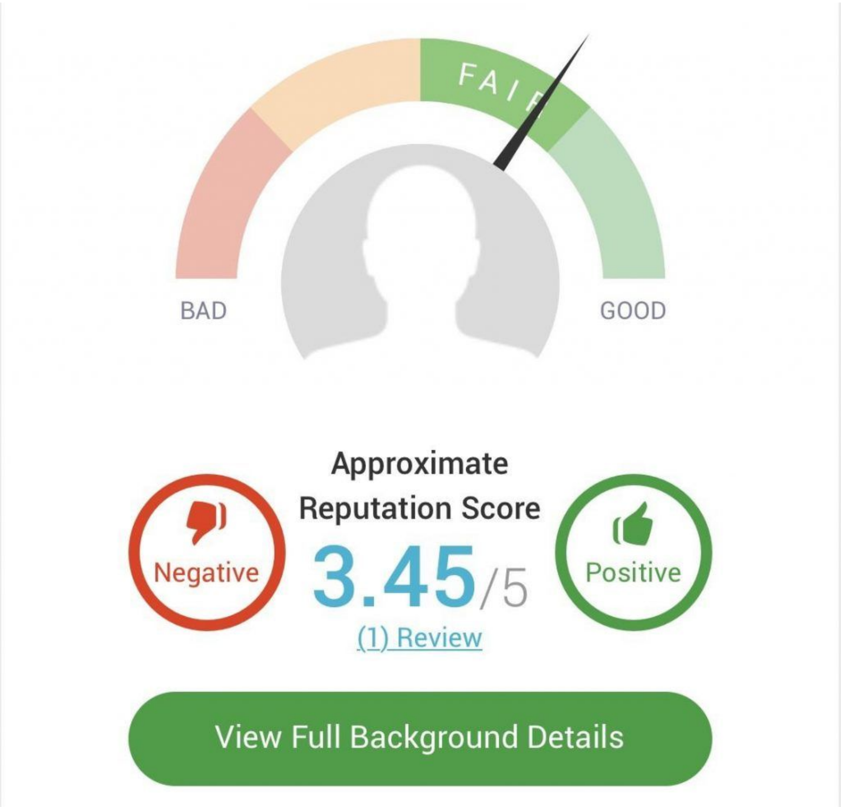
- Classify websites into predefined categories (e.g., social media, gambling, news, adult content)
- Policies can be applied to allow, block, or limit access based on categories

Block Rules

Block Safety
Build only as tall as you are.
Only knock down what you
Put the blocks away when you are finished
STOP
I will build my own to knock over! That is his work.

- Prevent access to certain types of content or known bad sites
- Blacklisting specific URLs, IP addresses, or keyword-based blocking
- Update block rules based on emerging threats and organizational policies.

Reputation



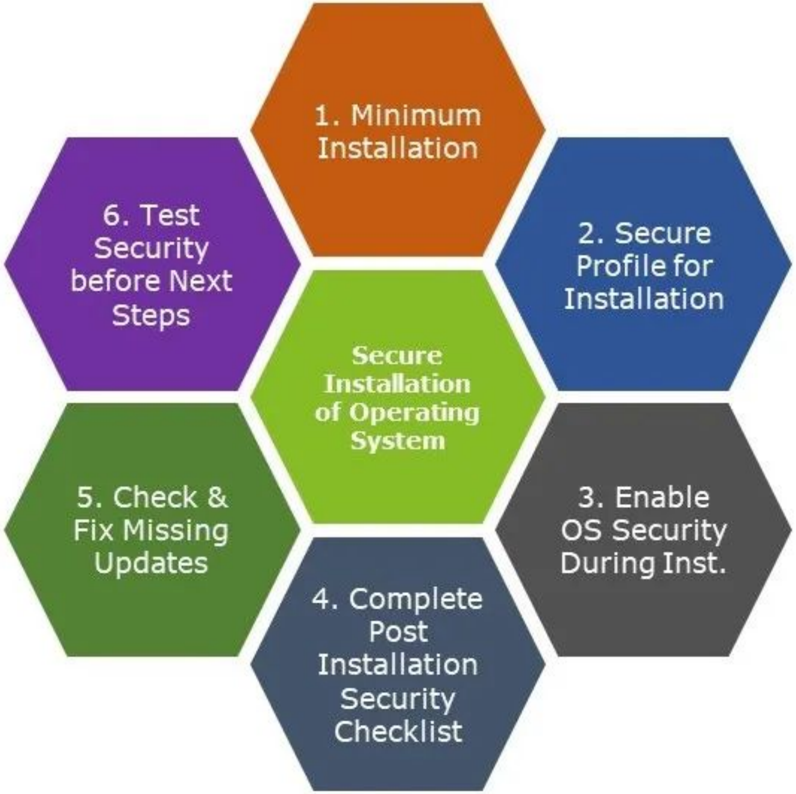
Approximate Reputation Score

3.45/5

(1) Review

- Assess and block websites based on their reputations
- Reputation scores are derived from historical data, threat intelligence, and user feedback
- Sites with poor reputations can be automatically blocked, reducing malicious content exposure

Operating System Security



Secure Installation of Operating System

1. Minimum Installation

2. Secure Profile for Installation

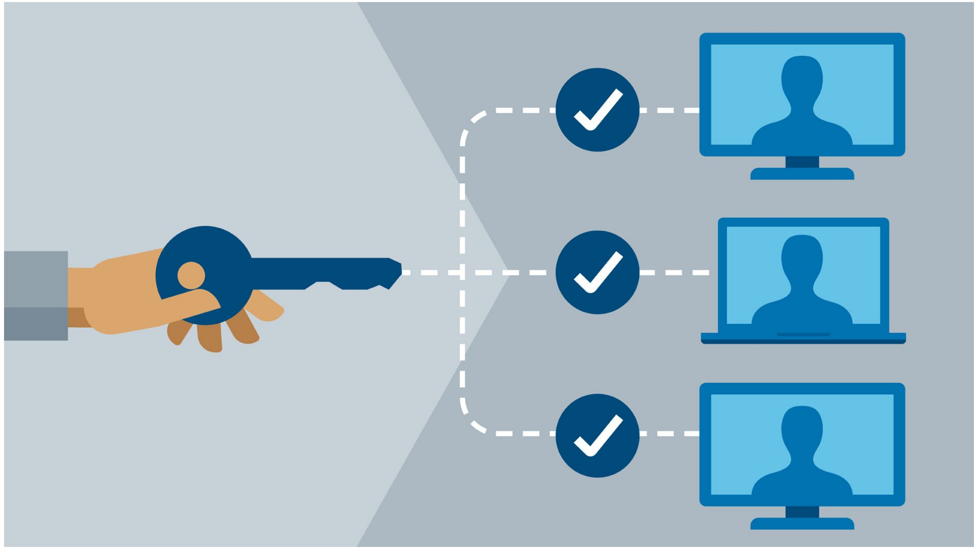
3. Enable OS Security During Inst.

4. Complete Post Installation Security Checklist

5. Check & Fix Missing Updates

6. Test Security before Next Steps

Group Policy

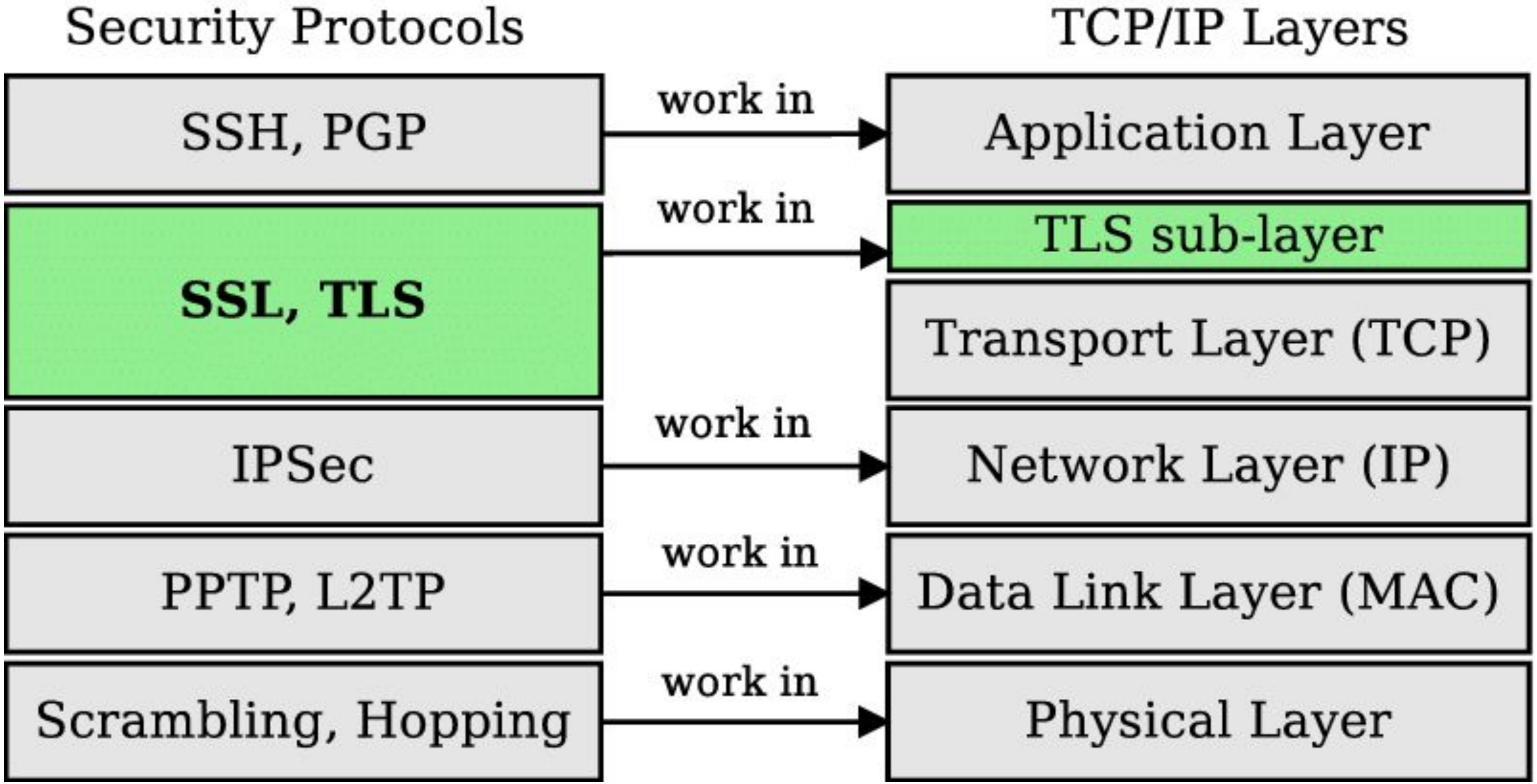


- Windows
- Enforce security settings and configurations across all devices
- Manage user permissions, configure security settings, enforce password policies...

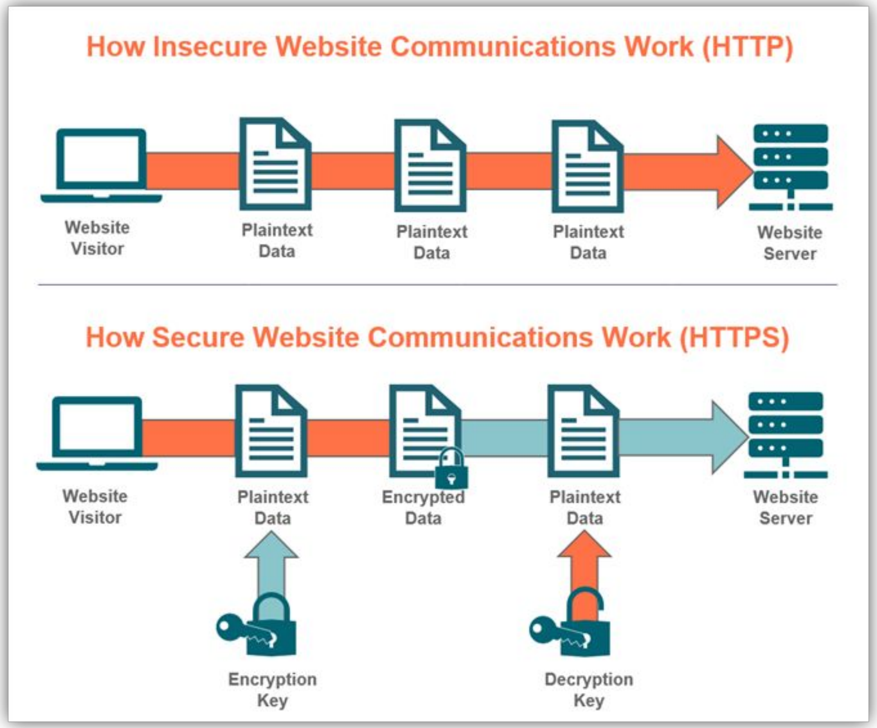
SELinux

- “Security-Enhanced Linux”
- Enforce mandatory access controls (MAC)
- Confine user programs and system services to the minimum required privileges

Secure Protocols

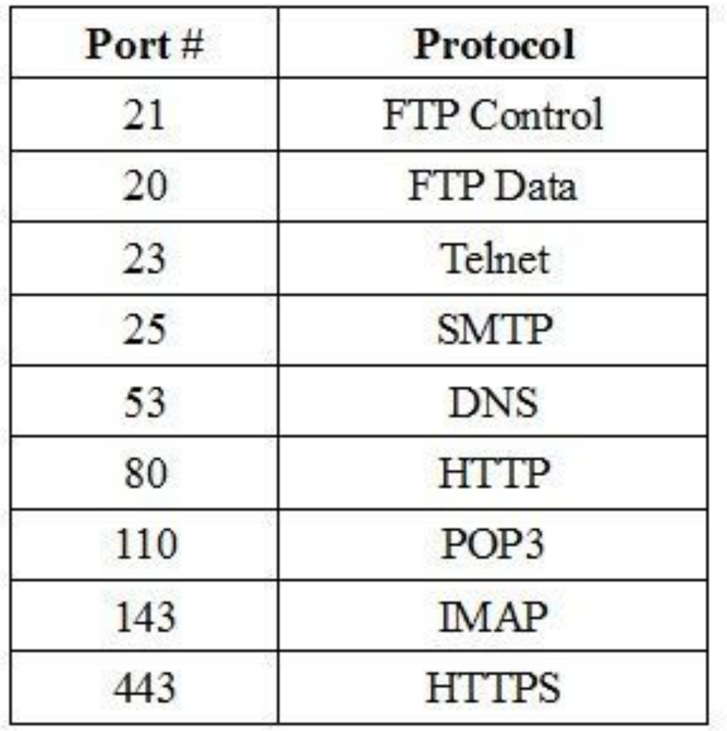


Protocol Selection



- Select secure versions of protocols for network communication
- Secure protocols provide encryption and secure authentication mechanisms
- Disable the use of outdated and insecure protocols

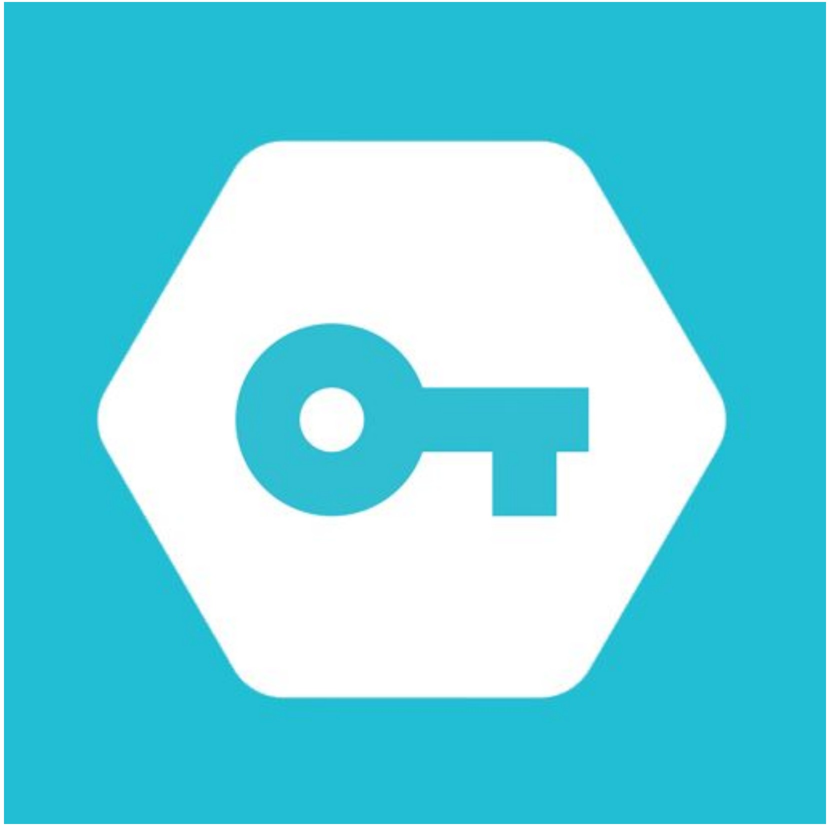
Port Selection



Port #	Protocol
21	FTP Control
20	FTP Data
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
143	IMAP
443	HTTPS

- Use standard ports associated with secure protocols to ensure compatibility
- Limit the number of open ports to reduce attack surface
- Use firewall rules to restrict access to extra ports

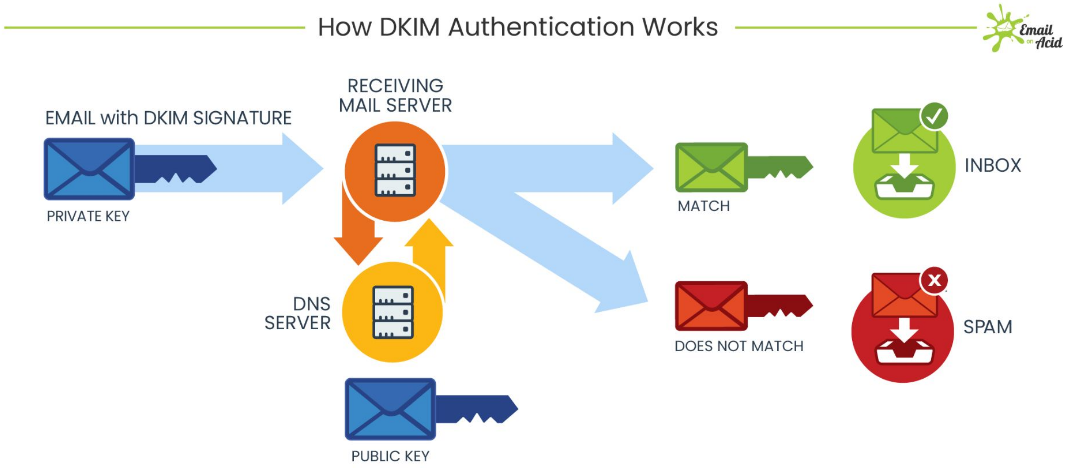
Transport Method



- Use secure transport methods like VPNs for remote access or WPA3 for wireless access
- Ensures that data is encrypted during transit
- Implement secure tunnels (e.g., IPsec or SSL/TLS) to protect sensitive communications

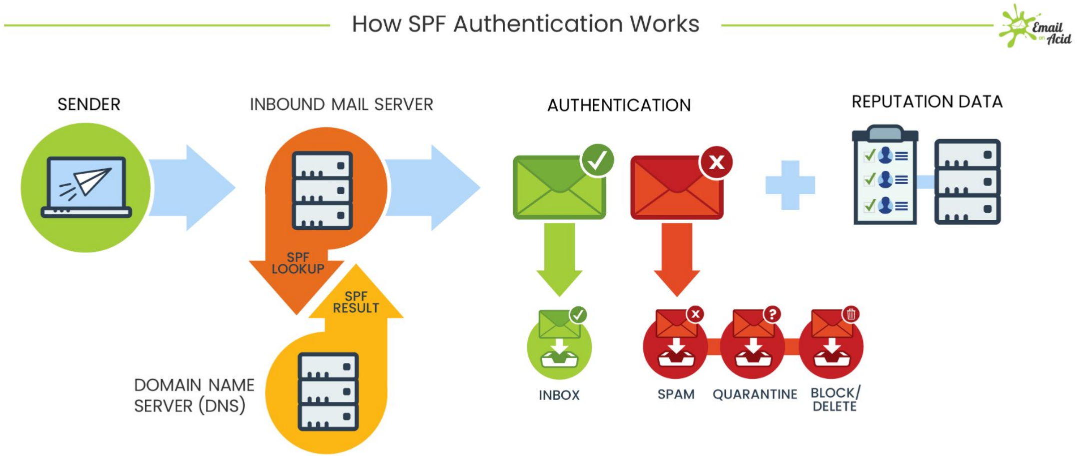
Email Security

DKIM



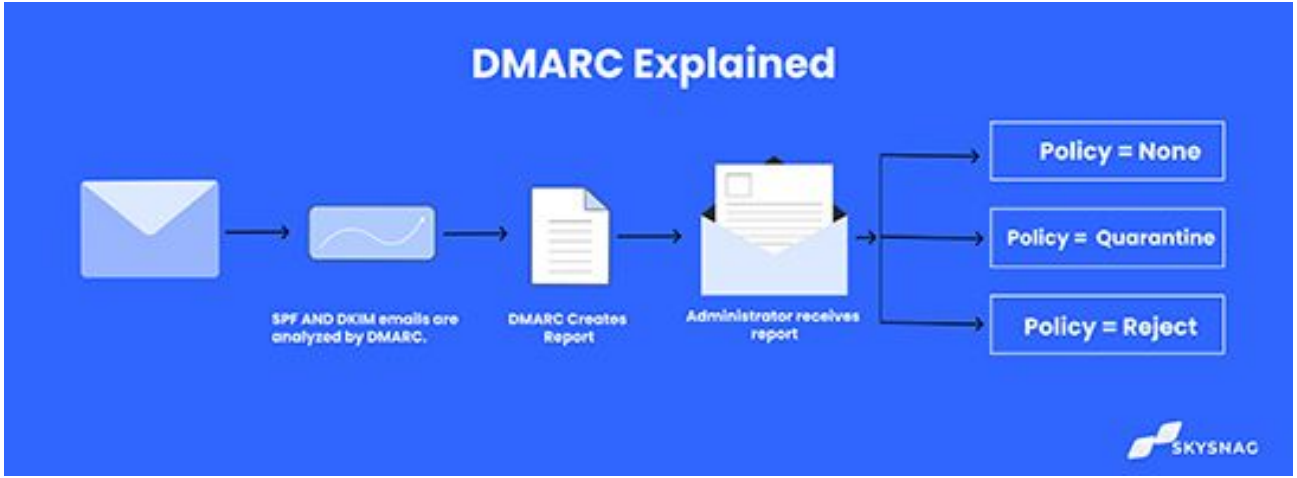
- Uses the digital signature to identify if the email is authorized by the owner of a domain
- Designed to detect forged sender addresses in email, a technique often used in phishing and email spam.

SPF



- Verifies the sender of an email and helps identify mail servers authorized to send emails for a given domain
- Can identify email from spoofers, scammers and phishers as they try to send malicious email from a domain that belongs to a company or brand.

DMARC



- Specifies how your domain handles emails that fail SPF or DKIM checks
- Uses a TXT file stored in your DNS to alert your inbox provider how to deal with these emails

EMAIL AUTHENTICATION RECORDS

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

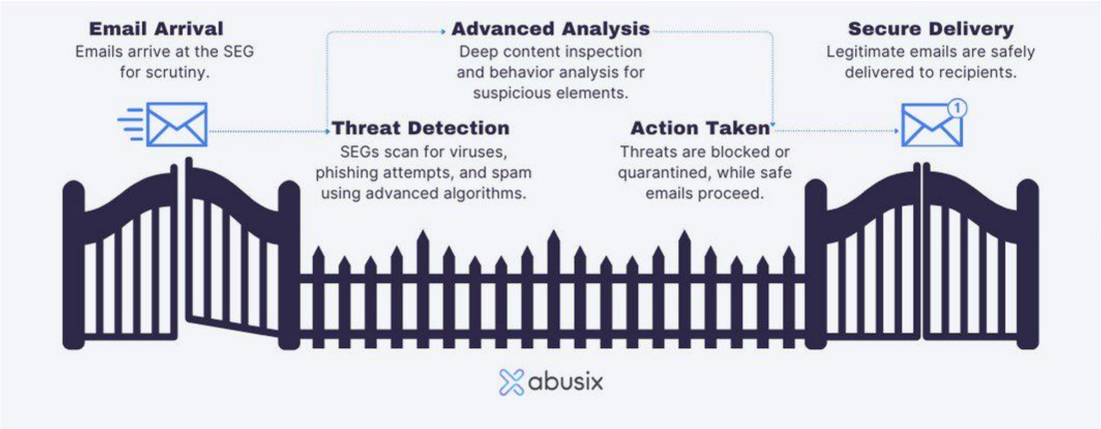
- Additional layers of security

HIGHLY RECOMMENDED

USE IT TO:

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

Secure Email Gateway



Email Arrival
Emails arrive at the SEG for scrutiny.
Advanced Analysis
Deep content inspection and behavior analysis for suspicious elements.
Secure Delivery
Legitimate emails are safely delivered to recipients.
Threat Detection
SEGs scan for viruses, phishing attempts, and spam using advanced algorithms.
Action Taken
Threats are blocked or quarantined, while safe emails proceed.
abusix

- Prevent unwanted emails like spam, phishing attacks, malware, and fraudulent content
- Prevent sensitive data leakages by analyzing outgoing messages and encrypting those that contain sensitive information

Miscellaneous Capabilities

DNS Filtering

- Block access to malicious or unwanted domains by controlling which DNS queries are resolved
- Maintain custom blocklists to prevent access to known malicious or non-business-related domains

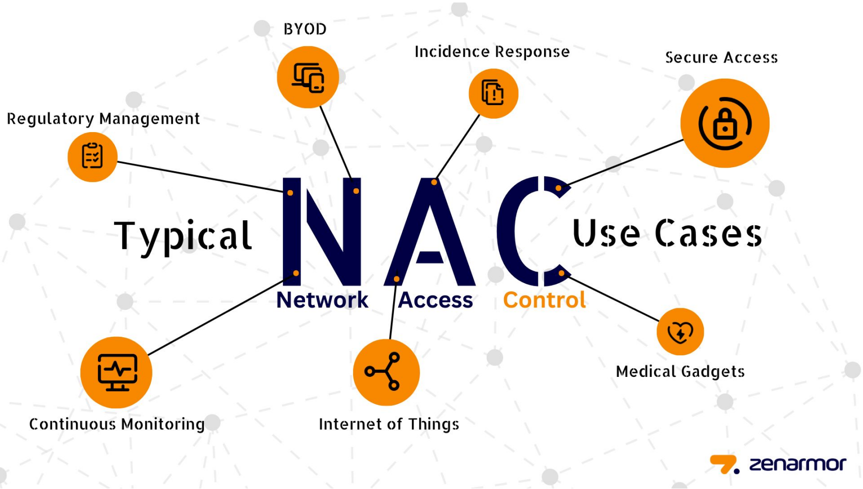
File Integrity Monitoring

- Tracks changes to files to ensure that unauthorized modifications do not occur
- Monitor critical system and configuration files, alerting administrators to any unauthorized changes

Data Loss Prevention

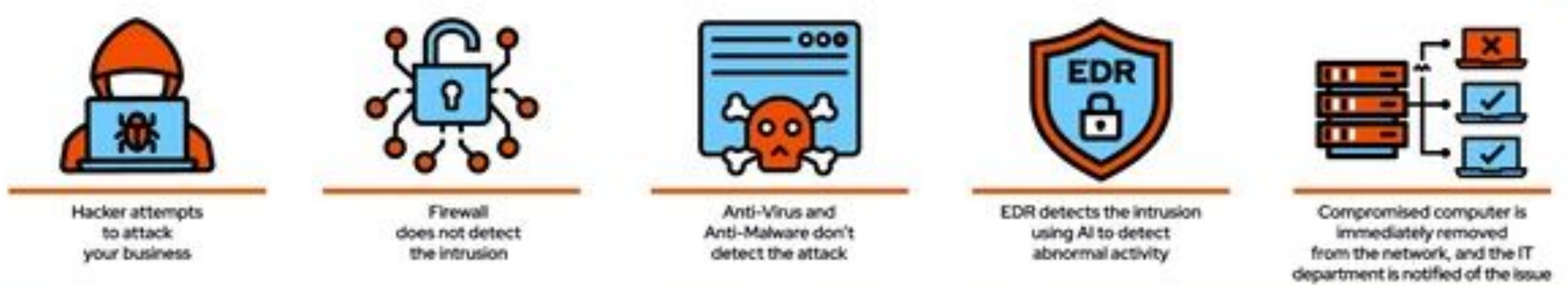
- Protects sensitive data from unauthorized access, use, or exfiltration
- Identifies and classifies sensitive data, such as financial records
- Provides alerts and detailed reports on potential data breaches

Network Access Control



- Ensures only authorized and compliant devices can access the network
- Authenticates and authorizes devices before granting network access
- Assesses the security posture of devices (e.g., checking for updated antivirus, patches) before granting access

Endpoint/Extended Detection and Response



Hacker attempts to attack your business

Firewall does not detect the intrusion

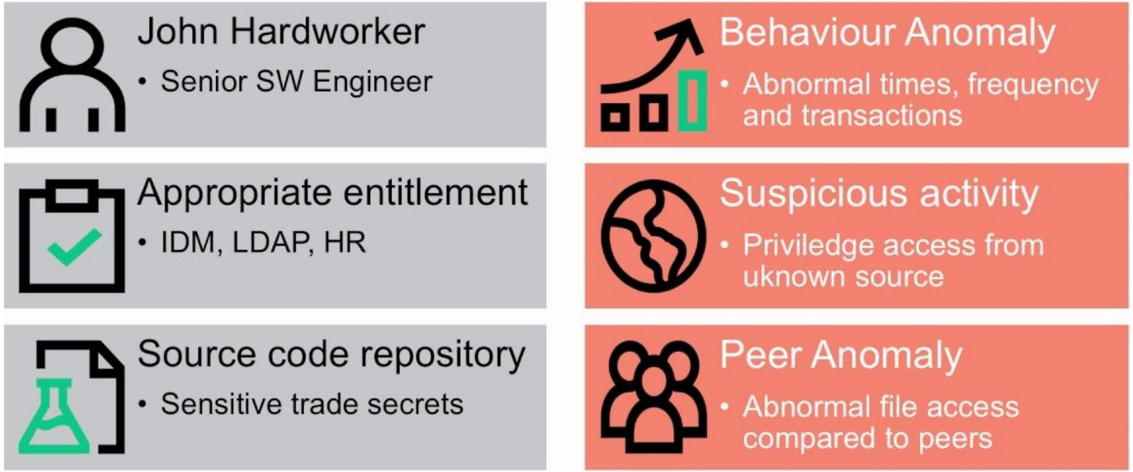
Anti-Virus and Anti-Malware don't detect the attack

EDR detects the intrusion using AI to detect abnormal activity

Compromised computer is immediately removed from the network, and the IT department is notified of the issue

- EDR and XDR provide advanced threat detection and response capabilities across endpoint
- Continuously monitor endpoints for suspicious activities
- Automated response capabilities, such as isolating infected endpoints and blocking malicious activities

User Behavior Analytics



John Hardworker

- Senior SW Engineer

Behaviour Anomaly

- Abnormal times, frequency and transactions

Appropriate entitlement

- IDM, LDAP, HR

Suspicious activity

- Priviledge access from uknown source

Source code repository

- Sensitive trade secrets

Peer Anomaly

- Abnormal file access compared to peers

- Leverages machine learning and data analytics to detect unusual user activities Establishes a baseline of normal user behavior
- Identifies deviations from the normal behavior