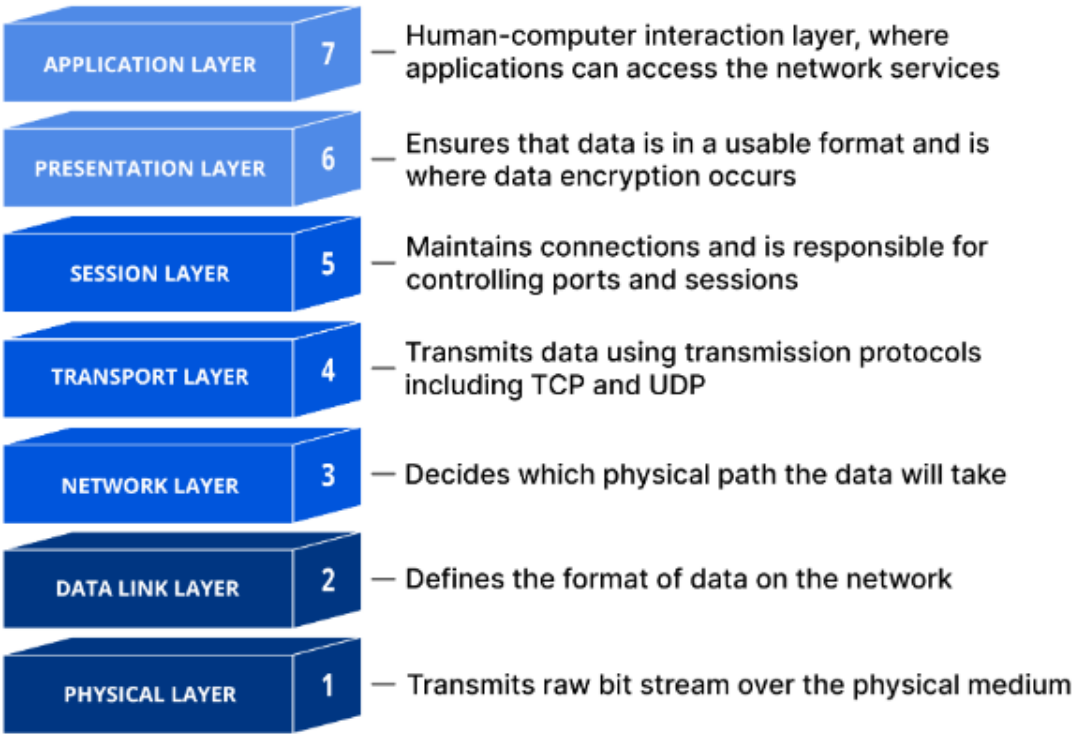
Networking

OSI Model:



Communication protocol:

SSL:

Secure Sockets Layer (SSL) is a communication protocol, or set of rules, that creates a secure connection between two devices or applications on a network. It's important to establish trust and authenticate the other party before you share credentials or data over the internet. SSL is technology your applications or browsers may have used to create a secure, encrypted communication channel over any network. However, SSL is an older technology that contains some security flaws. Transport Layer Security (TLS) is the upgraded version of SSL that fixes existing SSL vulnerabilities. TLS authenticates more efficiently and continues to support encrypted communication channels

TLS:

Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website.

Similarities between SSL and TLS?

Both SSL and TLS are communication protocols that encrypt data between servers, applications, users, and systems. They authenticate two parties connected over a network so they can exchange data securely.

TLS is the direct successor to SSL, and all versions of SSL are now deprecated. However, it's common to find the term *SSL* describing a TLS connection. In most cases, the terms *SSL* and *SSL/TLS* both refer to the TLS protocol and TLS certificates. TLS and SSL both use digital certificates that facilitate the handshake process and establish encrypted communications between a browser and a web server.

Difference between TLS and SSL?

SSL/TLS handshakes

A handshake is a process in which a browser authenticates a server's SSL or TLS certificate. This process authenticates both parties, then exchanges cryptographic keys.

An SSL handshake was an explicit connection, while a TLS handshake is an implicit one. The SSL handshake process had more steps than the TLS process. By removing additional steps and reducing the total number of cipher suites, TLS has sped up the process.

Alert messages

Alert messages are how SSL and TLS protocols communicate errors and warnings. In SSL, there are only two alert message types: warning and fatal. A warning alert indicates that an error has occurred, but the connection can continue. A fatal alert indicates that the connection must be terminated immediately. Additionally, SSL alert messages are unencrypted.

TLS has an additional alert message type called *close notify*. The close notify alert signals the end of the session. TLS alerts are also encrypted for additional security.

Message authentication

Both SSL and TLS use message authentication codes (MACs), a cryptographic technique for verifying the authenticity and integrity of messages. By using a secret key, the record protocol generates the MAC as a fixed-length code and attaches it to the original message.

The SSL protocol uses the MD5 algorithm—which is now outdated—for MAC generation. TLS uses Hash-Based Message Authentication Code (HMAC) for more complex cryptography and security.

Cipher suites

A cipher suite is a collection of algorithms that create keys to encrypt information between a browser and a server. Typically, a cipher suite includes a key exchange algorithm, a validation algorithm, a bulk encryption algorithm, and a MAC algorithm. Several algorithms in TLS were upgraded from SSL due to security concerns.

Difference between SSL certificate and TLS certificate?

At present, all SSL certificates are no longer in use. TLS certificates are the industry standard. However, the industry continues to use the term *SSL* to refer to TLS certificates.

TLS certificates have iterated upon SSL certificates and improved them over time. The final function of SSL certificates and TLS certificates hasn't changed.

Summary of differences: SSL vs. TLS		
	SSL	**TLS**
Stands For	*SSL* means Secure Sockets Layer.	*TLS* means Transport Layer Security.
Version History	SSL is now replaced with TLS. SSL moved through versions 1.0, 2.0, and 3.0.	TLS is the upgraded version of SSL. TLS has moved through versions 1.0, 1.1, 1.2, and 1.3.
Activity	Every SSL version is now deprecated.	TLS versions 1.2 and 1.3 are actively used.
Alert Messages	SSL has only two types of alert messages. Alert messages are unencrypted.	TLS alert messages are encrypted and more diverse.
Message Authentication	SSL uses MACs.	TLS uses HMACs.
Cipher Suites	SSL supports older algorithms with known security vulnerabilities.	TLS uses advanced encryption algorithms.
Handshake	An SSL handshake is complex and slow.	A TLS handshake has fewer steps and a faster connection.

Kerberos:

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC). Each user and service on the network is a principal.
The main components of Kerberos are:

- Authentication Server (AS):
  The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.

- Database:
  The Authentication Server verifies the access rights of users in the database.

- Ticket Granting Server (TGS):
  The Ticket Granting Server issues the ticket for the Server

Active Directory:

What is Active Directory and how does it work?

Active Directory (AD) is Microsoft's proprietary directory service. It runs on Windows Server and enables administrators to manage permissions and access to network resources.

Active Directory stores data as objects. An object is a single element, such as a user, group, application or device such as a printer. Objects are normally defined as either resources, such as printers or computers, or security principals, such as users or groups.

Active Directory categorizes directory objects by name and attributes. For example, the name of a user might include the name string, along with information associated with the user, such as passwords and Secure Shell keys.

The main service in Active Directory is Domain Services (AD DS), which stores directory information and handles the interaction of the user with the domain. AD DS verifies access when a user signs into a device or attempts to connect to a server over a network. AD DS controls which users have access to each resource, as well as group policies. For example, an administrator typically has a different level of access to data than an end user.

Other Microsoft and Windows operating system (OS) products, such as Exchange Server and SharePoint Server, rely on AD DS to provide resource access. The server that hosts AD DS is the domain controller.

LDAP:

The Lightweight Directory Access Protocol (LDAP) is a vendor-neutral software protocol used to lookup information or devices within a network. Whether you want to build a central authentication server for your organization or want to simplify access to internal servers and printers, LDAP is the answer.

What is LDAP?

LDAP is a standard protocol designed to maintain and access “directory services” within a network. Think of a directory service as a phonebook for different network resources like files, printers, users, devices, and servers, etc.

For example, an organization may store information for all their printers in a directory. LDAP can enable users to search for a specific printer, locate it on the network, and securely connect to it.

LDAP is widely used to build central authentication servers. These servers contain usernames and passwords for all the users within a network. Any-and-all applications and services can connect to the LDAP server to authenticate and authorize users.

LDAP directories typically contain data that is regularly accessed, but rarely changed. LDAP is designed to deliver exceptionally fast READ performance, even for larger datasets. However, the WRITE performance is significantly lower.

How does LDAP work?
To connect to a LDAP directory, a user must have an LDAP client installed on their device. Here's how a typical LDAP workflow looks like:

1. Using the client, the user establishes a secure connection with the LDAP directory.
2. They send a "search" query to the directory for a specific printer.
3. The LDAP directory authenticates the user.
4. The search operation is performed within the directory, and the address of the requested printer is returned.
5. The secure connection to the LDAP directory is closed.
6. The user connects to the printer.

TCP/IP:

Transmission Control Protocol (TCP)
TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.

Features of TCP

- TCP keeps track of the segments being transmitted or received by assigning numbers to every single one of them.
- Flow control limits the rate at which a sender transfers data. This is done to ensure reliable delivery.
- TCP implements an error control mechanism for reliable data transfer.
- TCP takes into account the level of congestion in the network.

Advantages of TCP

- It is reliable for maintaining a connection between Sender and Receiver.
- It is responsible for sending data in a particular sequence.
- Its operations are not dependent on OS.
- It allows and supports many routing protocols.
- It can reduce the speed of data based on the speed of the receiver.

Disadvantages of TCP

- It is slower than UDP and it takes more bandwidth.
- Slower upon starting of transfer of a file.
- Not suitable for LAN and PAN Networks.
- It does not have a multicast or broadcast category.
- It does not load the whole page if a single data of the page is missing.

UDP:

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as the UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. So, there is no need to establish a connection before data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network. The UDP enables process-to-process communication.

Features of UDP

- Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
- It is a suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.

Advantages of UDP

- It does not require any connection for sending or receiving data.
- Broadcast and Multicast are available in UDP.
- UDP can operate on a large range of networks.
- UDP has live and real-time data.
- UDP can deliver data if all the components of the data are not complete.

Disadvantages of UDP

- We can not have any way to acknowledge the successful transfer of data.
- UDP cannot have the mechanism to track the sequence of data.
- UDP is connectionless, and due to this, it is unreliable to transfer data.
- In case of a Collision, UDP packets are dropped by Routers in comparison to TCP.
- UDP can drop packets in case of detection of errors.

Which Protocol is Better: TCP or UDP?

- The answer to this question is difficult because it totally depends on what work we are doing and what type of data is being delivered. UDP is better in the case of online gaming as it allows us to work lag-free. TCP is better if we are transferring data like photos, videos, etc. because it ensures that data must be correct has to be sent.
- In general, both TCP and UDP are useful in the context of the work assigned by us. Both have advantages upon the works we are performing, that’s why it is difficult to say, which one is better.

NFS:

The Network File System (NFS) is a mechanism for storing files on a network. It is a distributed file system that allows users to access files and directories located on remote computers and treat those files and directories as if they were local.

For example, users can use operating system commands to create, remove, read, write, and set file attributes for remote files and directories.

The NFS software package includes commands and daemons for NFS, Network Information Service (NIS), and other services. Although NFS and NIS are installed together as one package, each is

independent and each is configured and administered individually. See *Network Information Services (NIS and NIS+) Guide* for details on NIS and NIS+.

DNS:

What is DNS?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

How does DNS work?

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

In order to understand the process behind the DNS resolution, it’s important to learn about the different hardware components a DNS query must pass between. For the web browser, the DNS lookup occurs "behind the scenes" and requires no interaction from the user’s computer apart from the initial request.

There are 4 DNS servers involved in loading a webpage:

- DNS recursor - The recursor can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursor is then responsible for making additional requests in order to satisfy the client's DNS query.

- **Root nameserver** - The root server is the first step in translating (resolving) human readable host names into IP addresses. It can be thought of like an index in a library that points to different racks of books - typically it serves as a reference to other more specific locations.

- TLD nameserver - The top level domain server (TLD) can be thought of as a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is "com").

- Authoritative nameserver - This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition. The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (the librarian) that made the initial request.

SMTP:

Email is emerging as one of the most valuable services on the internet today. Most internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) is used to retrieve those emails at the receiver's side.

SMTP Fundamentals
SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is an always-on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection through port 25. After successfully establishing a TCP connection the client process sends the mail instantly.

SMTP Protocol
The SMTP model is of two types:

1. End-to-end method
2. Store-and-forward method
3.

The end-to-end model is used to communicate between different organizations whereas the store and forward method is used within an organization. An SMTP client who wants to send the mail will contact the destination's host SMTP directly, in order to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP.

The client SMTP is the one that initiates the session so let us call it the client-SMTP and the server SMTP is the one that responds to the session request so let us call it receiver-SMTP. The client-SMTP will start the session and the receiver SMTP will respond to the request.

SSH:

SSH stands for **Secure Shell or Secure Socket Shell**. It is a cryptographic network protocol that allows two computers to communicate and share the data over an insecure network such as the internet. It is used to login to a remote server to execute commands and data transfer from one machine to another machine.

Secure communication provides a strong password authentication and encrypted communication with a public key over an insecure channel. It is used to replace unprotected remote login protocols such as **Telnet, rlogin, rsh, etc**., and insecure file transfer protocol **FTP**.

FTP:

An Explainer on FTP

At a basic level, FTP is a protocol that has one server and many clients that connect to the server in order to transfer files from one system to another. The client(s) then log into the server to execute commands. Commands allow you to move around the file tree, download files, upload files, move directories, delete, and much more. In the early days of the ARPAnet / Internet, this was revolutionary because you could take files and move them over great physical distances – even large files. FTP is not complicated, but it's exceedingly powerful and has stood the test of time.

The first FTP client applications were command-line programs developed before computers had graphical user interfaces. Such applications are still shipped with Windows, Linux, and Unix-based operating systems today.

FTP helps send files by transmitting information quickly and reliably so you can transfer large files online. File transfer protocol is commonly used for transferring large files between a client and a server. You can use FTP to exchange files between computer accounts, transfer files between an account and a desktop computer or access files in online storage.

File Transfer Protocol and Security

As great as FTP was at the time, it lacked security measures to encrypt usernames and passwords or other data going across the protocol. Thus FTPS and SFTP were made to build security measures directly into the protocol.

Decades later, we have services like Dropbox or Box that use their own protocols to move files around on the internet. You may ask yourself – why not just abandon FTP entirely and let companies use their own protocols? Here are a few reasons:

1. The backbone of the internet runs on standard protocols, like HTTP, FTP, DHCP, DNS, etc. Using a standard protocol is in line with the goals of a free and open internet.
2. It gives you flexibility in your toolset. Because of how long FTP has been around, there are tons of tools, scripts and daemons made that work with it.
3. Many devices already have FTP built into them, such as security cameras. Let's say you develop a new security camera and want it to connect to a closed protocol, like Dropbox. With FTP, you can make the connection. With a closed protocol, however, you would have to contact Dropbox and pay licensing fees for using their protocol.
4. Every client machine already supports file transfer protocol! You don't need to download a client to access FTP functions from the command line – you can even use whatever client you want to interface with FTP!

What is FTPS?

FTPS, also known as FTP-SSL, is a more secure form of FTP. FTPS is basic FTP with security added to commands and data transfer. Special security protocols TLS (Transport Layer Security) and SSL (Secure Sockets Layer) are cryptographic and provide encryption of data to protect your information as it moves from point A to point B, including username/password.

FTPS is to FTP much like HTTPS is to HTTP: an added layer of security while keeping the original protocol relatively unchanged.

What is SFTP?

SFTP, also known as SSH FTP, encrypts both commands and data while in transmission. This means all your data and credentials are encrypted as they pass through the internet. If you've ever used a Unix-based system, you're likely familiar with SSH. It's a protocol that allows you to remotely connect to other systems and execute commands from the command line. SSH is how most servers in the world are administered, so the protocol had to be very secure. SFTP was created as an extension of SSH to transfer files through the secure channel (SSH).

Unlike FTP and FTPS, SFTP protocol is packet-based as opposed to text-based. This makes file and data transfers using the SFTP faster than other secure FTP connections.

SFTP vs FTP

In our opinion, if you are able to use SFTP – use it. FTP is great for legacy devices that don't support any sort of encryption, but if you have access to encryption, it's better to use SFTP. You don't want your files intercepted by a malicious hacker downstream of your machine if you can help it.

SFTP vs FTPS

Both SFTP and FTPS provide a high level of protection. The biggest difference between these two protocols is how connections are authenticated and managed.

1. SFTP connections can be authenticated using a user id and password to connect to the server. SSH keys can also be used to authenticate SFTP connections. You will need to generate an SSH private key and public key to connect with the SFTP server.
2. With FTPS the usernames and passwords are also encrypted. To connect, your FTPS client will first check if the server's certificate is trusted. The certificate is considered trusted if either the certificate was signed off by a known certificate authority (CA), like Verisign, or if the certificate was self-signed (by your partner) and you have a copy of their public certificate in your trusted key store.

HTTP/HTTPS:

HTTP

HTTP stands for HyperText Transfer Protocol. It is invented by Tim Berner. HyperText is the type of text which is specially coded with the help of some standard coding language called HyperText Markup Language (HTML). HTTP provides a standard between a web browser and a web server to establish communication. It is a set of rules for transferring data from one computer to another. Data such as text, images, and other multimedia files are shared on the World Wide Web. Whenever a web user opens their web browser, the user indirectly uses HTTP. It is an application protocol that is used for distributed, collaborative, hypermedia information systems.

Characteristics of HTTP

- HTTP is IP based communication protocol that is used to deliver data from server to client or vice-versa.
- Any type of content can be exchanged as long as the server and client are compatible with it.
- It is a request and response protocol based on client and server requirements.

HTTPS

HTTPS stands for Hyper Text Transfer Protocol Secure. HTTP Secure (HTTPS), could be a combination of the Hypertext Transfer Protocol with the SSL/TLS convention to supply encrypted communication and secure distinguishing proof of an arranged web server. HTTPS is more secure than HTTP because HTTPS is certified by the SSL(Secure Socket Layer). Whatever website you are visiting on the internet, if its URL is HTTP, then that website is not secure.

Characteristics of HTTPS

- HTTPS encrypts all message substance, including the HTTP headers and the request/response data. The verification perspective of HTTPS requires a trusted third party to sign server-side digital certificates.
- HTTPS is presently utilized more frequently by web clients than the first non-secure HTTP, fundamentally to ensure page genuineness on all sorts of websites, secure accounts and to keep client communications.

In short, both of these are protocols using which the information of a particular website is exchanged between the Web Server and Web Browser. But there are some differences between these two. A concise difference between HTTP and HTTPS is that HTTPS is much more secure compared to HTTP.

AS2:

AS2 (Applicability Statement 2) is a http based protocol to transmit messages (especially EDI messages) safely, cheaply and quickly.

Load Balancer:

A load balancer distributes network or application traffic across a number of servers. Load balancers are used to increase the capacity and reliability of applications. Session management can improve the performance of your web applications. It can also provide increased scalability, security, and improved end-user experience.

a.) Network Load Balancer / Layer 4 (L4) Load Balancer:
Based on the network variables like IP address and destination ports, Network Load balancing is the distribution of traffic at the transport level through the routing decisions. Such load balancing is TCP i.e. level 4, and does not consider any parameter at the application level like the type of content, cookie data, headers, locations, application behavior etc. Performing network addressing translations without inspecting the content of discrete packets, Network Load Balancing cares only about the network layer information and directs the traffic on this basis only.

b.) Application Load Balancer / Layer 7 (L7) Load Balancer:
Ranking highest in the OSI model, Layer 7 load balancer distributes the requests based on multiple parameters at the application level. A much wider range of data is evaluated by the L7 load balancer including the HTTP headers and SSL sessions and distributes the server load based on the decision arising from a combination of several variables. This way application load balancers control the server traffic based on the individual usage and behavior.

c.) Global Server Load Balancer/Multi-site Load Balancer:
With the increasing number of applications being hosted in cloud data centers, located at varied geographies, the GSLB extends the capabilities of general L4 and L7 across various data centers facilitating the efficient global load distribution, without degrading the experience for end users. In addition to the efficient traffic balancing, multi-site load balancers also help in quick recovery and seamless business operations, in case of server disaster or disaster at any data center, as other data centers at any part of the world can be used for business continuity.

Firewall:

Firewalls prevent unauthorized access to networks through software or firmware. By utilizing a set of rules, the firewall examines and blocks incoming and outgoing traffic.

There are multiple types of firewalls based on their traffic filtering methods, structure, and functionality. A few of the types of firewalls are:

- **Packet Filtering**

A packet filtering firewall controls data flow to and from a network. It allows or blocks the data transfer based on the packet's source address, the destination address of the packet, the application protocols to transfer the data, and so on.

- **Proxy Service Firewall**

This type of firewall protects the network by filtering messages at the application layer. For a specific application, a proxy firewall serves as the gateway from one network to another.

- **Stateful Inspection**

Such a firewall permits or blocks network traffic based on state, port, and protocol. Here, it decides filtering based on administrator-defined rules and context.

- **Next-Generation Firewall**

According to Gartner, Inc.’s definition, the next-generation firewall is a deep-packet inspection firewall that adds application-level inspection, intrusion prevention, and information from outside the firewall to go beyond port/protocol inspection and blocking.

- **Unified Threat Management (UTM) Firewall**

A UTM device generally integrates the capabilities of a stateful inspection firewall, intrusion prevention, and antivirus in a loosely linked manner. It may include additional services and, in many cases, cloud management. UTMs are designed to be simple and easy to use.

- **Threat-Focused NGFW**

These firewalls provide advanced threat detection and mitigation. With network and endpoint event correlation, they may detect evasive or suspicious behavior.