Enterprise Security Assignment: Case Study Report

BY

Deepak Jain - 2021MT12286

Smita Pawar - 2021MT13008

Gajanana Hegde - 2021MT13053

Manam Bharadwaj - 2021MT13176

Table of Contents

Introduction

The purpose of this document is to provide an overview of security architectural design for the Work Integrated Learning Program (WILP), a division of BITS Pilani, whose brief it is to provide the highest quality education experience to industry professionals. WILP is currently implementing new IT systems, something that also requires a complete overhaul of their IT security. This document will focus on the enterprise security architecture aspect of this new IT infrastructure. For the purpose of simplicity, total userbase is downsized to around 1/5th of BITS Pilani, i.e. 5-8k WILP students, ~200 Staff. So, solutions and suggestions in this document will be applicable for any medium sized educational institute or enterprise [1]

To start with, as per the authors' meeting with WILP authorities for planning and requirements gathering, WILP is worried about several security issues :-

(a) Compliance with various security policies and privacy legislations.

(b) Cybersecurity - attacks from external sources, as well as from internal sources (e.g. rogue students/ disgruntled employees).

(c) WILP by definition, allows enrolment of only working professionals from all sort of industries/army/air force etc. Hence confidentiality of student records is non-negotiable. Budget is not a constraint when it comes to security and safety.

(d) Protection of WILP computer systems from inadvertent damage say accidental errors by inexperienced staff/teaching assistants etc or due to local weather conditions as the offices and campuses are spread as the offices and campuses are distributed all over the world.

WILP, BITS Pilani has IT systems in all of their offices :-

(a) **Head office**. There is one head office looking over central administration of ~200 staff and 5-8K students. It has all central office systems.

(b) **Regional offices**. There are 3 regional offices containing student records for example admission-verification documents/grades/class enrolments/ contact info etc, Regional office systems, payroll information like staff name, contact, location, verification documentation, perf review for past 10 years etc.

(c) **Regional campuses/.** - There are 7 regional campuses with IT teaching laboratories, staff workstations. As mentioned above there are around 200 professors plus 20 support staff over total 11 offices so around 20 employees per campus, local office systems. File servers, printers etc devices. IOT devices that need device as well as endpoint security.

Business Requirements and Risk assessments

While historically WILP has been following a hybrid learning model where students had to attend some of the classes/exams from the nearest regional campus. However, due to the pandemic the whole system is shifted to virtual learning. Hence, the attack surface has multi-folded. We need to consider breaches and in turn risks associated with thousands of connections outside BITS premises to WILP resources.

There are numerous breaches in online education in previous years. Some of them are enumerated below:-

- **January 2022**, two reported cyberattacks targeting ed tech providers have resulted in the breach of **private information of more than 3.5 million U.S.** K–12 students. Such data breaches even if they don't include a social security number are very dangerous for students and can impact their financial futures for many years to come, as per Doug Levin, national director of K12 Security Information Exchange.

- Details of more than 400 students were leaked after a spreadsheet containing personal information (DOB, contact information and Student ID etc) was **accidentally** attached to an email at **the University of Essex, UK** on **23 March 2022**. [2]

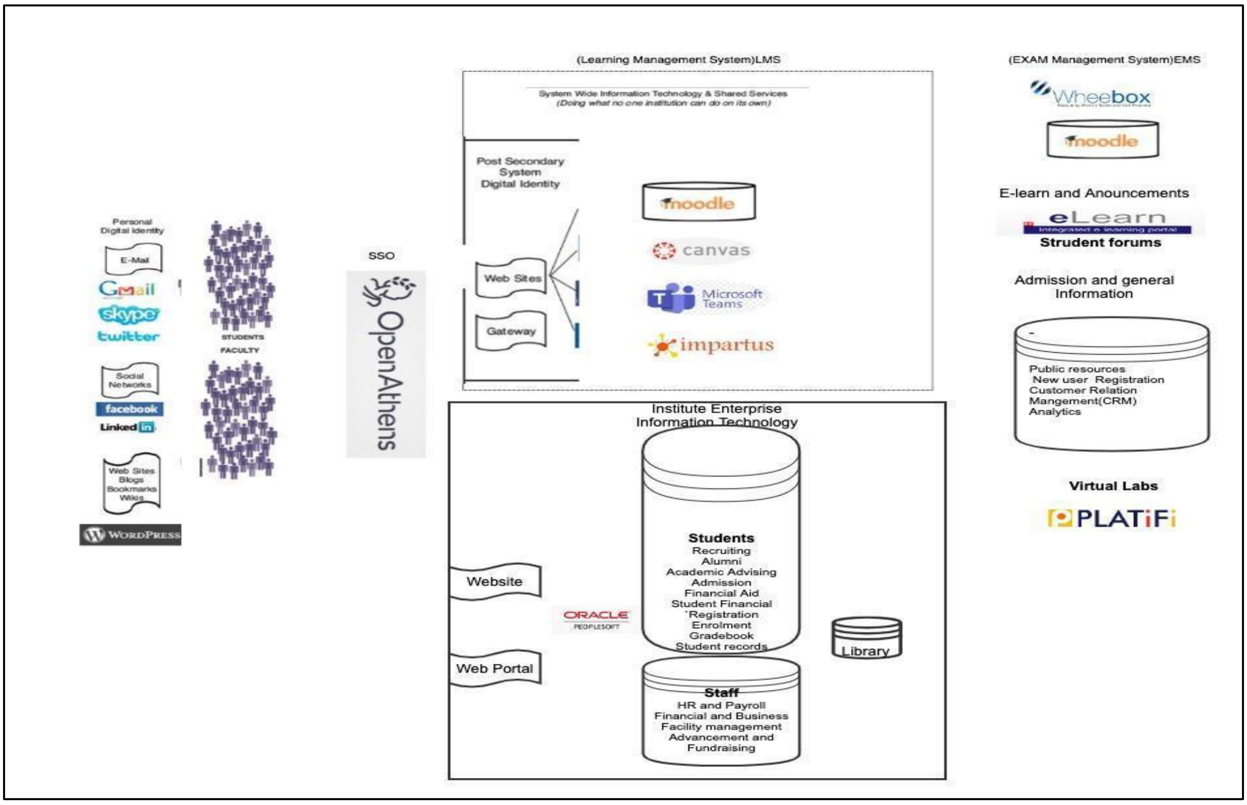
- A prominent school in **Kolkata, India** ditched online classes after hackers sneaked into several lectures and displayed obscene videos on the screen and **threatened the students** and teachers. As a result, teachers had to suspend the online classes.

- On **9th June 2022, Simpson University in Redding California** confirmed that the company experienced a data breach involving unauthorized **access to employee email accounts**. According to Simpson University, the breach resulted in the names, Social Security numbers, financial information (bank account, credit card, and debit card numbers), and protected health information of **6,175 students** being compromised. Simpson University has filed official notice of the breach and sent out data breach letters to all affected parties.

- JEE candidate in Assam who got 99.8 percentile arrested along with father for using proxy Assam Police has written to the National Testing Agency (NTA), which conducts the exam, seeking CCTV footage from the examination centre in Borjhar, Guwahati, for analysis and investigation. [4]

Use cases and /or Business processes

Above breaches provide a baseline for security requirements for WILP system. BITS also has highly educated staff and consultants that understand the importance of investing in best in class proactive security. BITS WILP uses tools and technologies developed in house as well as from different vendors such as moodle, Oracle etc for a modern better learning experience.



Existing module structure of WILP Portal: Central Office [5]

Use cases

The salient features requirements of the architecture of WILP is described below to include payroll, fees, admission, financial process, studies management and examination procedure. The architecture has limited capability for enterprise security and must be robust for day to day cyber and security attacks. The details of are as follows:-

(a) Staff payroll data should be confidential. MFA - OTP based authentication is needed in addition to password-based authentication for administrative operations and for managers/finance department support staff to access employee data.

(b) Students admission process will need degree certificates, photos, mentor forms, Aadhar card, email id and phone numbers etc - most of it will be PII.

(c) Fee payment process needs to support credit cards, net banking, UPI options from all majority banks/vendors securely.

(d) Financial information - payment gateway etc should be protected (C-I-A). Multi Factor authentication for financial transactions.

(e) Loans/EMIs facility (3rd Party finance providers) should be from an authorised and trusted list only. There should be a well-defined contract and agreement that the third-party products comply with security standards like PCI DSS.

(f) Exam papers administration/download should only be available to authorized staff - OTP based authentication should be added to ensure confidentiality.

(g) Data center servers should be only protected with PKI, TPM, Certificates based trust mechanism to ensure integrity.

(h) Course content - Students from worldwide (may not be near HO/RO/RC) so need caching servers for performance and availability.

(i) Streaming across countries following different privacy and compliance policies - GDPR, ISO27001 etc

(j) Grades information should be accessible only to student and staff - each student should be able to access only their own grades/records. Only authorized and current staff like course instructor/ teaching assistants, IT support assigned to any related support case in case of technical error, should be able to modify the records. Other course instructors and few more staff members in the hierarchy may have view access.

(k) Courseware - access only chosen electives and core subject material. Students will not have access to course material outside the enrolled courses as it may be protected to be distributed only for educational purposes under restricted license, copyright/intellectual property laws etc. Digital library/lab subscriptions will be for limited period covered by appropriate licenses.

(l) Data retention policy – Alumnus educational, payment status data needs to be maintained even after course completion as per local and global data retention policy. Financial account information needs to be purged/shredded carefully once the transaction is complete unless instructed and permitted specifically to be saved for future use.

(m) Almost zero Budget constraints - There is no compromise while allocating funds as it has lobby of sponsors like prominent businessmen and alumni association, interested in providing better quality and affordable education.

(n) Secure access to lab – lab resources should be only available upon authentication and authorization from current students. It should be isolated from production environment /rest of the data centre. Lab maintenance schedules may differ from data centre maintenance. That way even insider attack cannot extend using this window to penetrate into rest of the system.

(o) Online lectures - susceptible to MITM/DDoS - Rogue students/hackers may target to disrupt the classes either by overwhelming the network with large amounts of requests or may send inappropriate content during the lectures. System should be prepared in advance to handle and protect from such incidents.

(p) Data protection from natural calamities, accidental damage as well as intentional attacks - Fault detection and recovery should be provided using features like RAID/encryption at storage layer, https SSL/TLS1.2 while in transit, DLP for email servers (e.g. payroll info should not leave the RO), Backup and Disaster Recovery to formulate and mitigate impact of ransomware attack etc.

(q) BYOD - staff/students can access courses and accounts using mobile/laptops/tablets. So, policies should be clearly defined for safe and ethical use of such devices.

(r) Exam process - certain information like hall ticket, exam schedules, grade sheet needs to be accurate, highly available and immutable. Data Integrity also should be maintained for question papers need to be tamperproof.

(s) Adequate training to staff and students to protect from social engineering, Phishing, Vishing attacks etc.

Compliance Requirements

While the majority of compliance revolves around student/staff/end users personal and financial information and data protection/retention, some amount of PHI available also warrants health related standards compliance. Example of PHI -

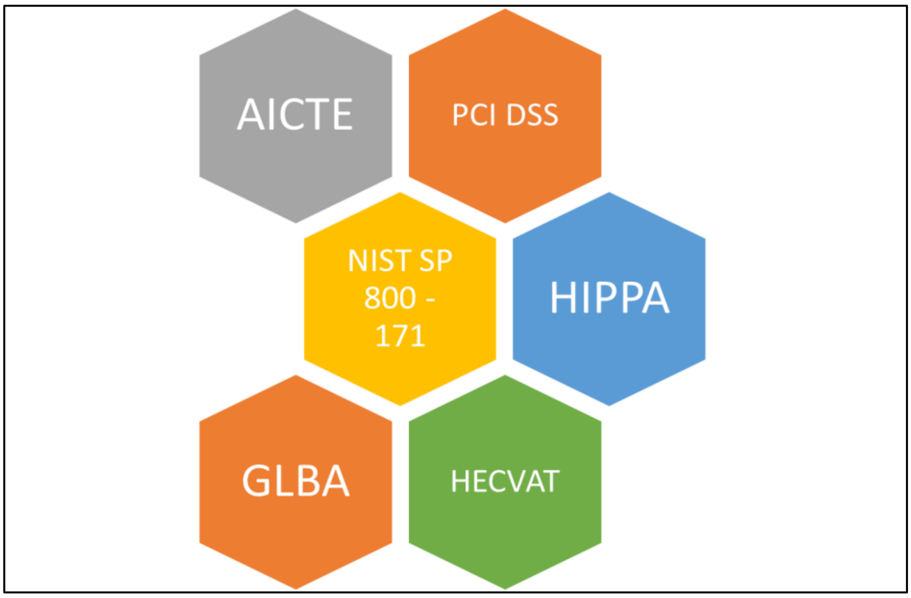
(a) Disabilities information for fee concessions.

(b) Medical certificates in case of missing regular exams.

(c) Medical information of staff for medical insurance related process.

(d) Disability information of staff for priority parking pass.

As an international higher education institution, WILP needs to comply with following worldwide standards. This is important not just to avoid financial losses but to protect the organization's reputation. Please note this is a growing/changing list that needs to be reviewed and revised at least annually.



Compliance requirements for Enterprise Security

(a) AICTE Cyber security strategy for higher education institutes in India covers 360 degrees aspects of security like infrastructure, network, data privacy protection as well as data retention, processes and last but not the least - incident response.[6]

(b) NIST SP 800 - 171- These guidelines, issued by the National Institute of Standards and Technology in 2015, are intended to secure federal information stored in non-federal databases. It includes broad requirements covering a variety of data security threats that apply to higher education and is required for higher educational institutions that process Controlled Unclassified Information (CUI). Though this originated in the US, the standard is used as a measure of security worldwide.

(c) The Gramm-Leach-Bliley Act (GLBA) Signed into US law more than twenty years ago, this compliance standard requires financial institutions to disclose their procedures for sharing and securing customers' personal data.

(d) WILP provides flexible payment options like credit, debit or prepaid card used for all financial transactions - registration, annual fee payment, WILP merchandise and donations etc. Compliance with the Payment Card Industry Data Security Standard (**PCI DSS**) is required of all university departments and offices that accept payment cards for financial transactions. Any third-party vendor engaged by University Merchants to process payment card transactions on their behalf, or who is engaged in payment card financial services on WILP campus, must also comply with the PCI DSS.

(e) **Health Insurance Portability and Accountability Act (HIPAA)**. This privacy regulation has been around for more than two decades, and it sets data privacy and security parameters for organizations managing peoples' protected health information (PHI). In addition to outlining specific compliance standards, HIPAA includes financial penalties for companies that can't secure this critical information.

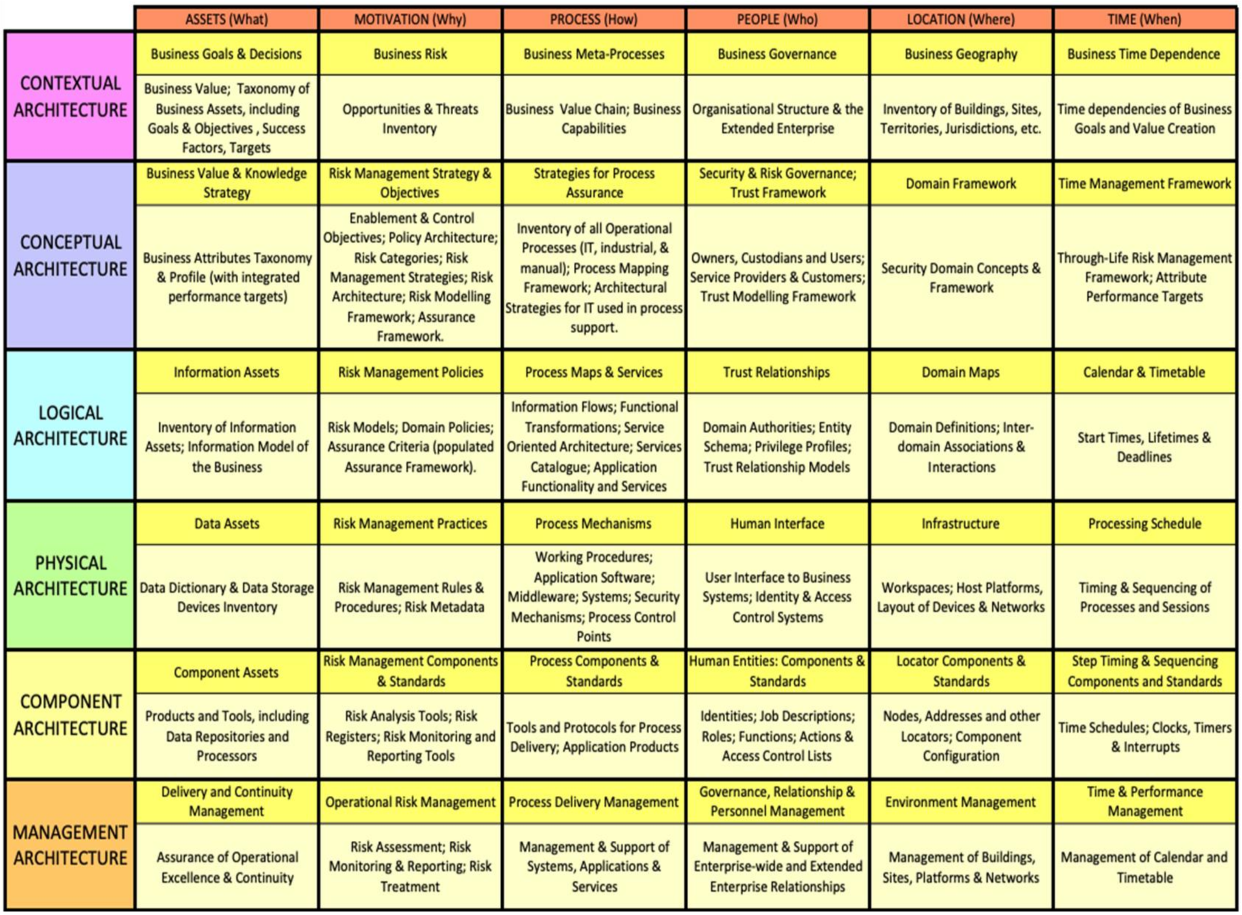
(f) Third party vendors are now subject to the same Security Rule requirements as Covered Entities and are also subject to relevant sections of the Privacy Rule and the **HITECH Breach Notification Rule**. In order to protect university confidential and highly confidential data, the risk and compliance team assesses the security and practices of all third-party vendor server applications and cloud services.

(g) Majority of current tools are developed inhouse or third party on premise (Moodle/Impartus) or SaaS cloud-based tools like MS Teams. In future as more and more technology will be catered via cloud-based software - it will need to comply to **HECVAT.** The higher education information security community, EDUCAUSE, Internet2, and the Research & Education Networks Information Sharing & Analysis Center (REN-ISAC) created the Higher Education Cloud Vendor Assessment Toolkit (HECVAT), a self-assessment that attempts to standardize higher education information security and data protection requirements around cloud service providers. The assessment helps higher education institutions ensure that cloud services are appropriately assessed for security and privacy needs, and allows a consistent, easily adopted methodology for those who want to use cloud services.

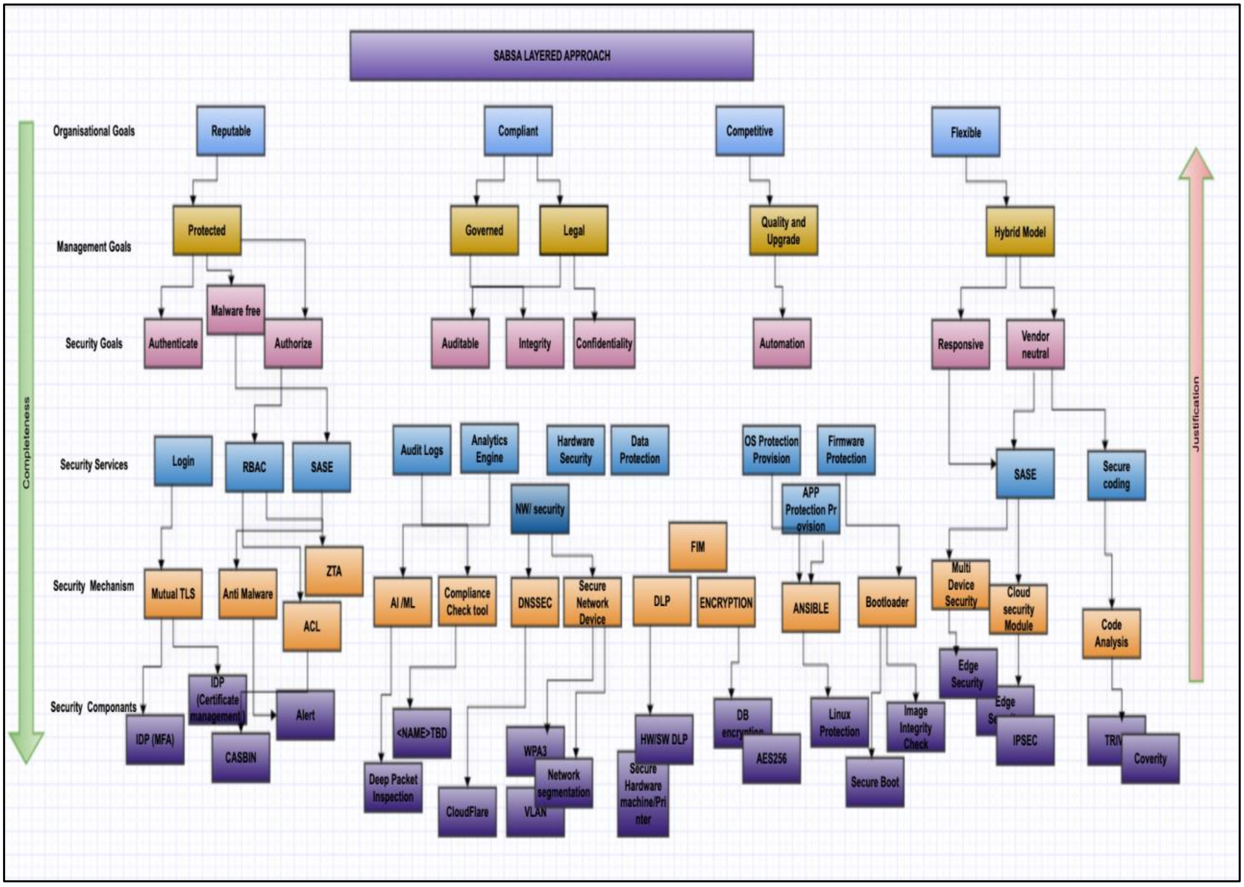
(h) ISO27001 also covers some security guidelines for educational institutes.

Security Architecture - High Level

WILP practices **SABSA Architectural Framework** as described below. SABSA layers and framework create and define a top-down architecture for every requirement, control and process available.



	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Goals & Decisions	Business Risk	Business Meta-Processes	Business Governance	Business Geography	Business Time Dependence
	Business Value; Taxonomy of Business Assets, including Goals & Objectives , Success Factors, Targets	Opportunities & Threats Inventory	Business Value Chain; Business Capabilities	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of Business Goals and Value Creation
CONCEPTUAL ARCHITECTURE	Business Value & Knowledge Strategy	Risk Management Strategy & Objectives	Strategies for Process Assurance	Security & Risk Governance; Trust Framework	Domain Framework	Time Management Framework
	Business Attributes Taxonomy & Profile (with integrated performance targets)	Enablement & Control Objectives; Policy Architecture; Risk Categories; Risk Management Strategies; Risk Architecture; Risk Modelling Framework; Assurance Framework.	Inventory of all Operational Processes (IT, industrial, & manual); Process Mapping Framework; Architectural Strategies for IT used in process support.	Owners, Custodians and Users; Service Providers & Customers; Trust Modelling Framework	Security Domain Concepts & Framework	Through-Life Risk Management Framework; Attribute Performance Targets
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Trust Relationships	Domain Maps	Calendar & Timetable
	Inventory of Information Assets; Information Model of the Business	Risk Models; Domain Policies; Assurance Criteria (populated Assurance Framework).	Information Flows; Functional Transformations; Service Oriented Architecture; Services Catalogue; Application Functionality and Services	Domain Authorities; Entity Schema; Privilege Profiles; Trust Relationship Models	Domain Definitions; Inter-domain Associations & Interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	Infrastructure	Processing Schedule
	Data Dictionary & Data Storage Devices Inventory	Risk Management Rules & Procedures; Risk Metadata	Working Procedures; Application Software; Middleware; Systems; Security Mechanisms; Process Control Points	User Interface to Business Systems; Identity & Access Control Systems	Workspaces; Host Platforms, Layout of Devices & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	Component Assets	Risk Management Components & Standards	Process Components & Standards	Human Entities: Components & Standards	Locator Components & Standards	Step Timing & Sequencing Components and Standards
	Products and Tools, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery; Application Products	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators; Component Configuration	Time Schedules; Clocks, Timers & Interrupts
MANAGEMENT ARCHITECTURE	Delivery and Continuity Management	Operational Risk Management	Process Delivery Management	Governance, Relationship & Personnel Management	Environment Management	Time & Performance Management
	Assurance of Operational Excellence & Continuity	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Management & Support of Enterprise-wide and Extended Enterprise Relationships	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable



Architectural Framework[31]

Define Roles

Data-Centric Architecture needs well-defined users/roles. Given below is the lists of main roles, more users can be added in later phases like design/implementation of Head Office Data Centre/Infrastructure:-

(a) Administrator

(b) Database Administrator

(c) Security Officer

(d) Storage Administrator

(e) Network administrator

(f) Operator

WILP eLearning Web Application User Roles can be further divided into following roles as per roles and tasks. This can be further articulated as per the requirements as day-to-day need. The details are:-

(a) Professors

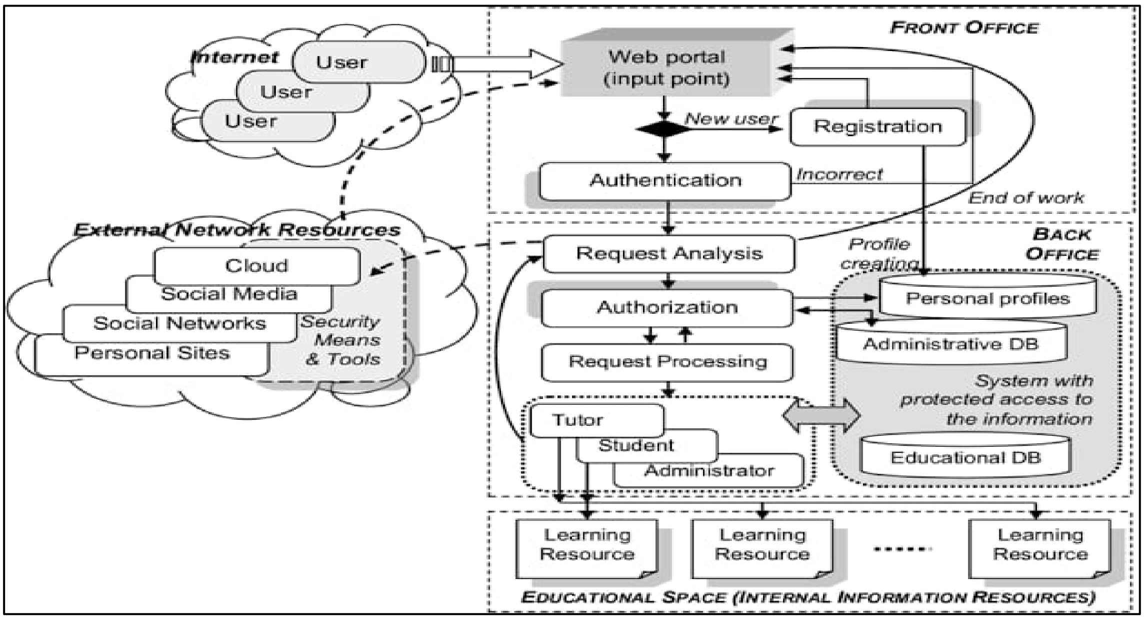
(b) Students

(c) Finance Staff

(d) Teaching assistants

(e) IT Administrator

(f) Contractors



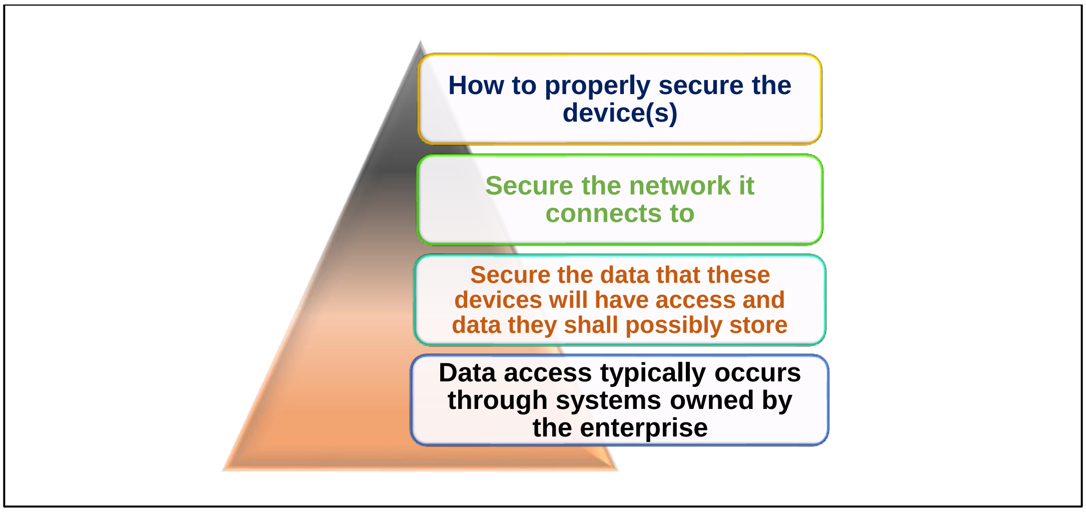
Define Processes

As there are hundreds of staff members and thousands of students as well as many supporting third parties/ sponsors and other stake holders, trusted processes become a backbone for smooth and secure operation of WILP. Only BYOD process is explained below for brevity of this document. Similar processes will be designed for ensuring 360 degrees security encompassing diverse aspects like acceptable use, data retention and protection, system lifecycle and purging, compliance to standards and regulations etc

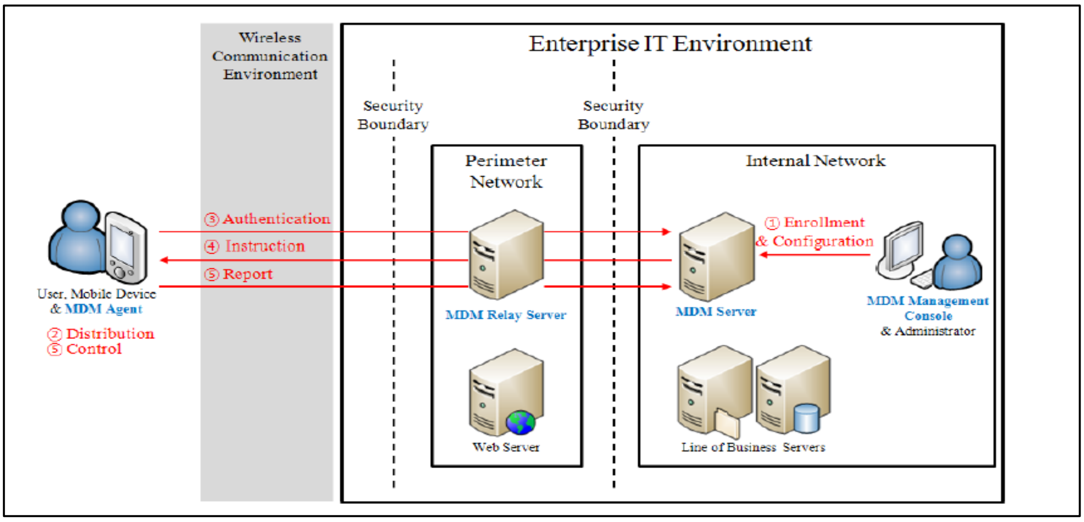
BYOD.

(a) Students/Professors allowed to bring/use their own laptops or can also join from home or anywhere using valid credentials. Support/ Head office Staff will be allowed only to use WILP provided laptop/workstation and personal mobile.

(b) Enterprise Security Architecture factors related to BYOD aspects are depicted in diagram below:-

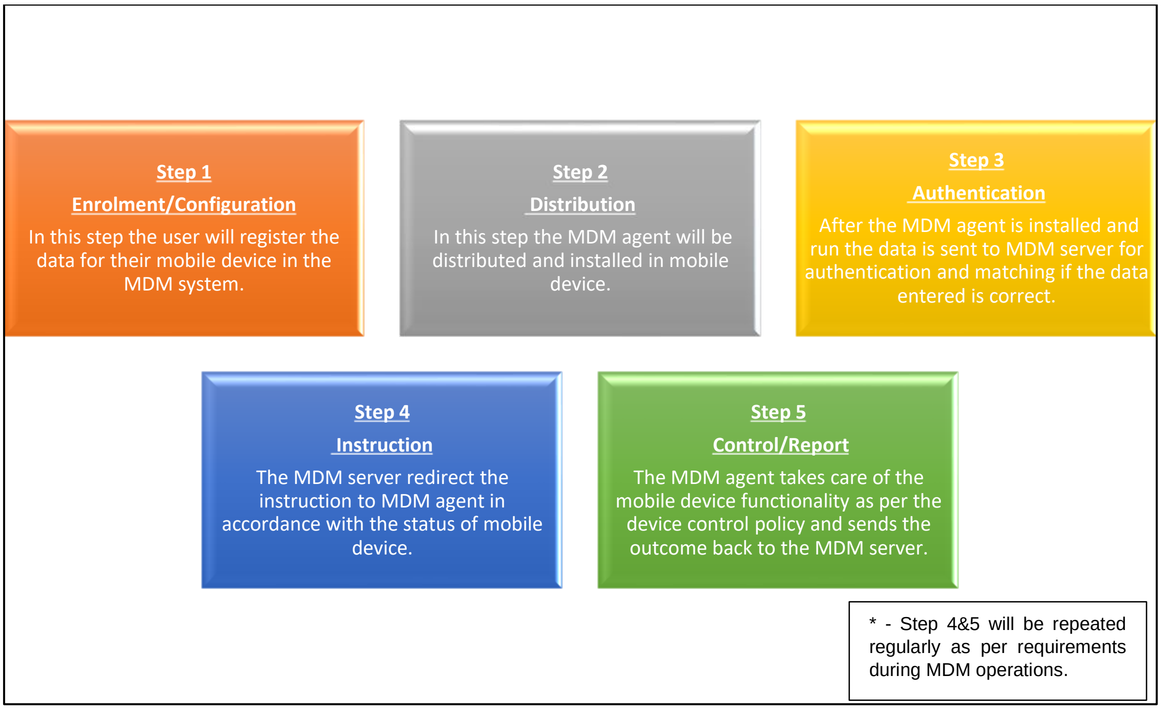

How to properly secure the device(s)
Secure the network it connects to
Secure the data that these devices will have access and data they shall possibly store
Data access typically occurs through systems owned by the enterprise

(c) Commonly implemented security measures include using a Mobile Device Management (MDM) solution. It is Generic platform for determining what exact data the device has access to will be up to WILP to decide. WILP will have to map the interaction to a defined trust model or develop one to meet this request.



BYOD MDM diagram [7]

(d) The basic operation steps for MDM architecture is described below:-



Step 1
Enrolment/Configuration
In this step the user will register the data for their mobile device in the MDM system.

Step 2
Distribution
In this step the MDM agent will be distributed and installed in mobile device.

Step 3
Authentication
After the MDM agent is installed and run the data is sent to MDM server for authentication and matching if the data entered is correct.

Step 4
Instruction
The MDM server redirect the instruction to MDM agent in accordance with the status of mobile device.

Step 5
Control/Report
The MDM agent takes care of the mobile device functionality as per the device control policy and sends the outcome back to the MDM server.

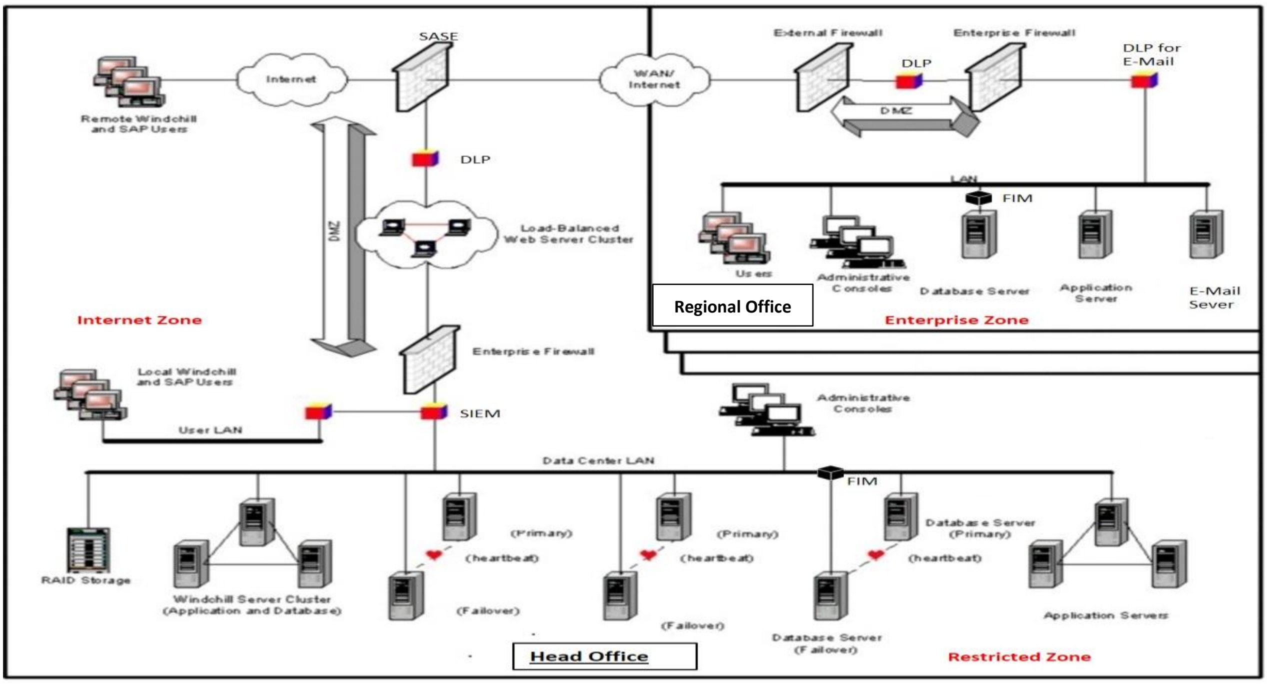
* - Step 4&5 will be repeated regularly as per requirements during MDM operations.

Deployment Security Architecture (Defense in Depth)

WILP systems needs multifaceted, multi-layered security best described by following quote.

“There’s no silver bullet solution with cyber security, a layered defense is the only viable defense.” - James Scott, Institute for Critical Infrastructure Technology

All offices/sites/data centres and regional campuses need to employ appropriate security mechanisms to ensure even the weakest link is not left vulnerable.



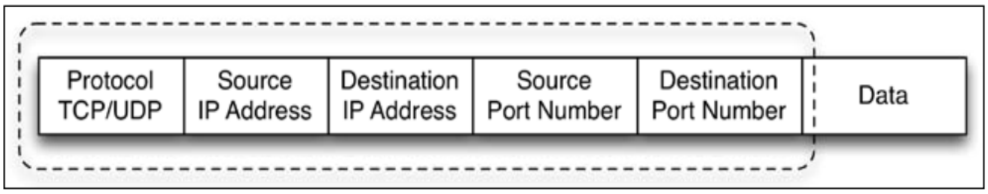
SASE for Branch Network Security

Secure access service edge (SASE), a relatively new security concept, is the convergence of WAN/SD-WAN and network security services like CASB, FWaaS and Zero Trust into a single, cloud-delivered service model. A SASE solution offers a consistent way to deliver and manage security at branch offices while also providing a uniform way to securely connect users to applications. With a cloud-based infrastructure, branch offices forward traffic into the cloud service, where security policy is centrally enforced. This eliminates the need for IT to physically go to sites to manually update appliances or mitigate issues. This will include security equipment, networking devices, storage systems, management tools, operational components for the detailed security architecture.

(a) **Next-generation firewall (NGFW)**. restricts access to other locations. Unlike legacy stateful firewalls, NGFW will provide application awareness and control to protect against the spread of malware and other application-layer attacks. NGFW can be delivered as an on-premises solution or from the cloud in which case its a firewall as a service (FWaaS).

(i) NGFW will be installed at endpoints of Regional Campus RC, Regional Office and Head Office and will monitor data packets when RC to RO or RO to HO transmission is carried out. It performs more deep packet Analysis to mitigate malicious traffic masquerading as legitimate.

(ii) (NGFW would be able to detect the anomaly behaviour in such network transactions, alerting security staff of a potential network breach. The most significant benefit of the NGFW is awareness. The NGFW no longer makes packet permit and deny decisions using only the simple network portions of the communication, such as source and destination IP and port pairings; it can look into the traffic flow and decode the exact application that makes up the communication flow. This is rather special from a security perspective. The technology is aware of what the traffic is, and not just how the traffic is communicating. Having the application awareness capability, NGFW is able to perform deep packet inspection to also decode and inspect the application data in network communication.



Simplified TCP packet with IP header with header inspection only

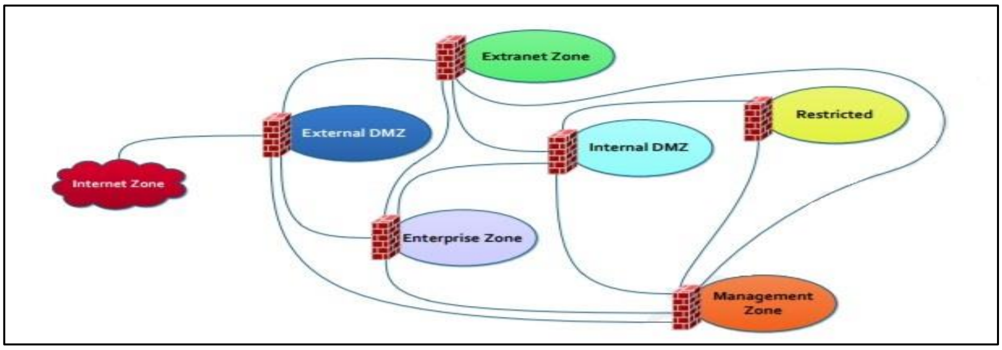
(b) **Devices for Network segmentation - DNS zoning** [8]

(i) A network can have the most sophisticated security mechanisms implemented but without network segmentation. Their value will be greatly undermined, if not invalidated. Internal segmentation is often overlooked, because focus is on the external threat. Unfortunately, the external threat is counting on weak internal network segmentation to spread malware throughout the enterprise and gain a foothold for exfiltration of critical enterprise data. Significant investment has been made in network access control (NAC) and perimeter technologies, meanwhile the latest threat introduced to the network through a trusted host is wreaking havoc on internal client systems and the most critical systems in the enterprise.

(ii) The main intention of network segmentation is to divide networks into different zones via subnets and putting checkpoints within zones of the network, thus preventing spread of attack by following the strategy of Internal Network Segmentation.

(iii) Before network segmentation it is important to identify critical data, resources, processes, applications and systems. This activity helps in determining complexities of moving assets to network segments separated by a firewall.

(iv) Recommended security monitoring tools can be SIEM security Information and Event Management along with FIM file Integrity Monitoring which gives early detection and timely incident response.



Security Zoning in Network Architecture

(c) **Secure Web Gateway (SWG)**. restricts access to Internet and cloud resources and provides advanced threat protection against malware in user-initiated Web/Internet traffic. All SWGs will inspect HTTP/HTTPs traffic, but some will also include all ports and protocols.

(d) **Software Defined Perimeter (SDP)**. **It is also called zero trust network access (ZTNA)** restricts access to applications based on identity and real-time context. While thought of as applying to remote and mobile users, SDP/ZTNA extends to network users as well. Rather than connecting to network, users of SDP/ZTNA first authenticate with a broker who then provides a portal of permitted applications and network resources. As such, users have application access but not general network access, preventing minimizing lateral movement across the network.

(e) **Intrusion Detection/Prevention Systems (IDS/IPS)**. This analyses network flows for signatures of known cyberattacks. IDSs detect attacks, IPSs stop attacks. Because IPSs impact the flow, not merely monitor it, enterprises need to be particularly careful that adding signatures won't result in false positives, unnecessarily interfering with user workflows.

(f) **Remote Browser Isolation (RBI)**. This protects users from Web-based attacks by shielding them from Internet. An RBI system sits between the users and the websites they browse, sending a user's browser an image of the browsed site. No content is executed on user machines, protecting them from most Web threats.

(g) **Cloud Access Service Brokers (CASBs)**. This identify and protect data in the cloud. CASBs provide a central point to enforce policies and provide visibility into user activities. It generally includes DLP to enforce policies, threat protection to prevent users from accessing specific cloud services and compliance capabilities.

(h) **Web Application and API Protection**. This delivers multiple security modules for inspecting and protecting at the Web layer. WAAP's core features include WAF, bot mitigation, protection against DDoS and API protection with a variable depth of security available for these for each module.

(i) **Data Loss Prevention (DLP)**. It identifies and prevents the use of sensitive information such as social security numbers or meta-data within data streams. DLP systems inspect content and analyse user actions to identify activity involving confidential information out of compliance within company guidelines and regulations.

(j) **Data Masking**. It goes a step further than DLP that masks data for reasons of privacy or compliance. Data Masking is a one-way process that hides sensitive data such as social security numbers with other realistic-looking data.

(k) **User and Entity behaviour Analytics (UEBA)**. It analyses user behaviour and apply advanced analytics to detect anomalies.

Other planning considerations for information, computer and network security

Contingency and Disaster Recovery planning considerations

(i) Protection in case of power outages.

(ii) Contingency planning in case of natural disasters.

(iii) Needs inventory of all resources along with classification relative to overall WILP - not just one office.

(iv) Incident response and intimation needs to be planned in case security incident still takes place.

Cost-Avoidance considerations in information security

Education is different from conventional business enterprises. It involves a service component and trust/reputation is paramount for educational institutes. Hence WILP security should be considered in each level from top to bottom. Security planning and architecture needs to be proactive and not wait until something bad happens and real cost for security gets visible.

Following worksheet which is a template to generate financial exposure amounts for different scenarios of data/information incidents. The worksheet should be filled out for each data type used in WILP, from the highest priority to the lowest priority. (Example: Data type: Student financial data. WILP students are professionals so may have higher credit limits and higher financial implications.)

Aspects	Issue: Data Released	Issue: Data Modified	Issue: Data Missing
Cost of Revelation			
Cost to Verify Information			
Cost Of Lost Availability			
Cost of Lost Work			
Legal Costs			
Cost of Lost Confidence			
Costs Cost to Repair Problem			
Fines & Penalties Other costs			
Notification			
Total Cost Exposure for this data type & issue			

To be filled by respective Department

Business policies related to information security and other topics

There are written policies to identify acceptable practices and expectations for business operations. This is not an exhaustive list but just a peek into type of policies at WILP:-

(a) Some policies are related to human resources, others will relate to expected employee/staff/student practices for using business resources, such as computers, file servers, printers, fax machines, and Internet access.

(b) Legal and regulatory requirements also require certain policies to be put in place and enforced.

(c) Policies for information, computer, network, and Internet security communicate clearly to staff and students the expectations that the WILP management has for appropriate use. For example, for sensitive student information a typical policy statement says, “All employee personal data shall be protected from viewing or changing by unauthorized persons." This policy statement identifies a particular type of information and then describes the protection expected to be provided for that information.

(d) Policies are clearly communicated clearly to each employee as well as students on the WILP website and all employees and students need to sign a statement agreeing that they have read the policies, that they will follow the policies, and that they understand the possible penalties for violating those policies. This helps to make them accountable for violation of the businesses policies. There are penalties for disregarding business policies.

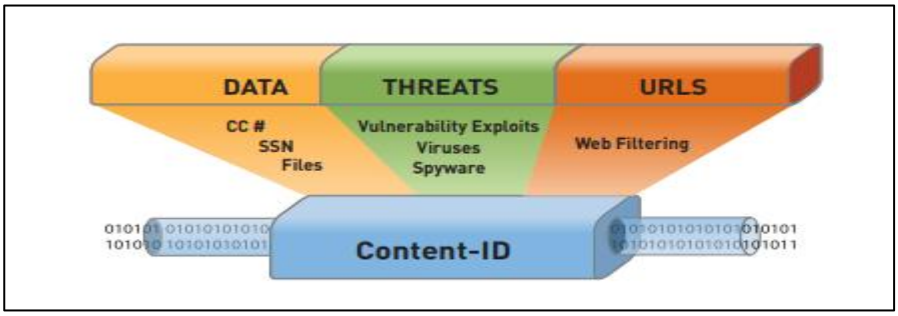
***** - Implementing the best practices described above will help your business cost-avoidance efforts and will be useful as a tool to market your business as one in which the safety and security of your customer's information is of highest importance.

Detailed Security Architecture & design for Offices

Head Office (HO)

Tools that enforce Architecture of Security in Head office: Advanced firewalls, Defence in Depth, Intrusion Detection and Prevention, Network Segmentation, SIEM and FIM monitoring.

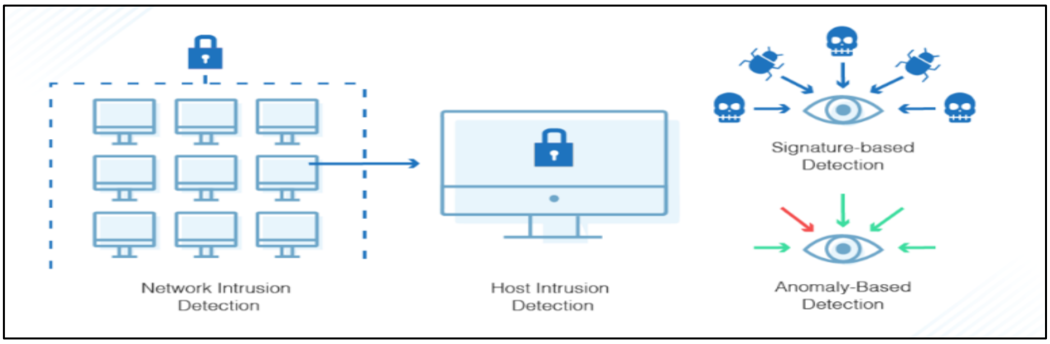
(a) **NGFW**. Next gen Firewall will be installed at endpoints of Regional Campus RC, Regional Office and Head Office and will monitor data packets when RC to RO or RO to HO transmission is carried out.



Next Gen Firewall [10]

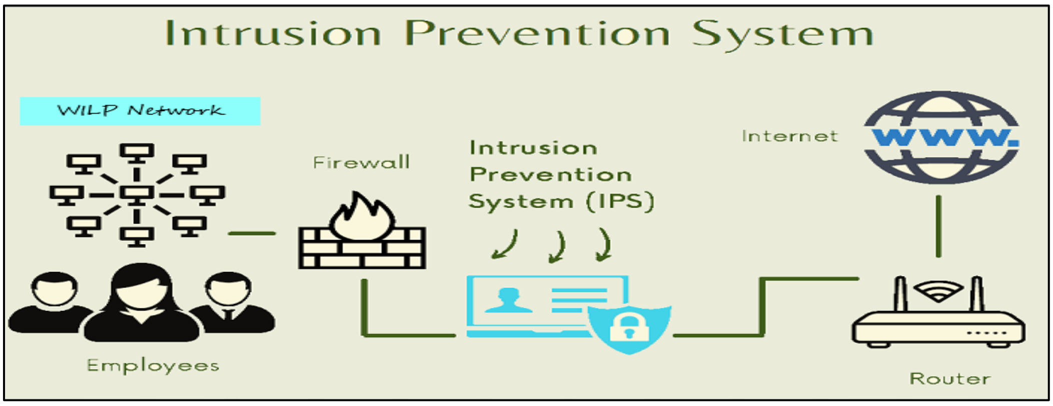
(b) **Devices for Network segmentation**. Divide networks onto different zones via subnets and put checkpoints within zones of the network, thus preventing spread of attack by following the strategy of Internal Network Segmentation. Security monitoring tools SIEM security Information and Event Management along with FIM file Integrity Monitoring which gives early detection and timely incident response used in Critical zones.

(c) **Network Intrusion Detection**. Placed in HO network parameters and internal server endpoints to detect anomalies and traffic analysis. Capable of detection using 3 methods: Behaviour, Anomaly & Signature.



Network Intrusion Detection [11]

(d) **Network Intrusion Prevention**. Capacity to disrupt and mitigate malicious traffic by blocking and using other methods. Built-in DDOS mitigation technology helps protect critical assets in the Internal Network.


Intrusion Prevention System
WILP Network
Firewall
Intrusion Prevention System (IPS)
Internet
www.
Employees
Router

Network Intrusion Detection [12]

(e) **Securing Network Services**.

(i) DNSSEC which provides authenticity of DNS information and source of DNS records.

(ii) SPAM filtering @ Cloud which uses MX records to accept the legit mails from servers.

(iii) Secure file transfer techniques which includes FTP, SFTP, FTPS, SSH and SSL connection.

(iv) Network security via user authentication both local active directory and using Public Key (SPKI).

(v) Monitoring through Internet Proxy Servers for secured internet access for the head office.

(f) **Securing Enterprise Websites**.

(i) Secure coding by web application developers.

(ii) Application whitelisting for trusted applications to run on servers for layered mitigation implementation.

(g) **Securing Enterprise Servers**.

(i) TPM, Secure Boot for root of trust (Avoid rootkit attacks)

(ii) Application Whitelisting

(iii) Vulnerability Scanning

(iv) OS hardening - Secure default configuration

Regional Offices (RO)

Regional office network security represents the means to secure internet traffic branch to branch as well as between branches and data centres, headquarters or remote employees. Keeping data secure @ rest (for payroll information security), in transit and ensuring proper access control are critical to protecting an organization as a whole. Branch Office Network Security requirements are as given below:-

(a) Establish complete visibility.

(b) Protect corporate resources.

(c) Secure access to internet and cloud apps.

(d) Prevent zero-day threats.

(e) Prevent user circumvention.

(f) The challenges while mitigating the same are as follows:-

(i) Keeping network speeds up and minimizing bandwidth interruptions.

(ii) Traditional technologies like wide area networks (WAN) and multiprotocol label switching (MPLS) can't keep up with the evolving network landscape or the addition of new services and applications that require more bandwidth.

(iii) The practice of sending internet traffic back to headquarters to be filtered and inspected can't realistically keep up with user demands and the types of data being accessed and sent.

(iv) Traditionally, firewalls have been placed on-premises at each location, requiring IT to be physically present for implementation, setup, maintenance and hardware troubleshooting. The more sites, the more hardware requirements, and the greater the number of granular rules and policies that must be created.

(v) Hackers know that the network edge is generally the weakest point in an organization and will exploit that to gain access into internal networks.

Regional Campus (RC)

Production network security will use similar infrastructure like HO, RO. Tools that enforce Architecture of Security in Regional Campuses are :-

(a) Anti-Virus, Intrusion Detection and Prevention, Network Segmentation, SIEM and FIM monitoring.

(b) Secure Printers as well as File servers - need authentication and authorization (including MFA for sensitive data)

(c) Audit logs should be in place for accountability.

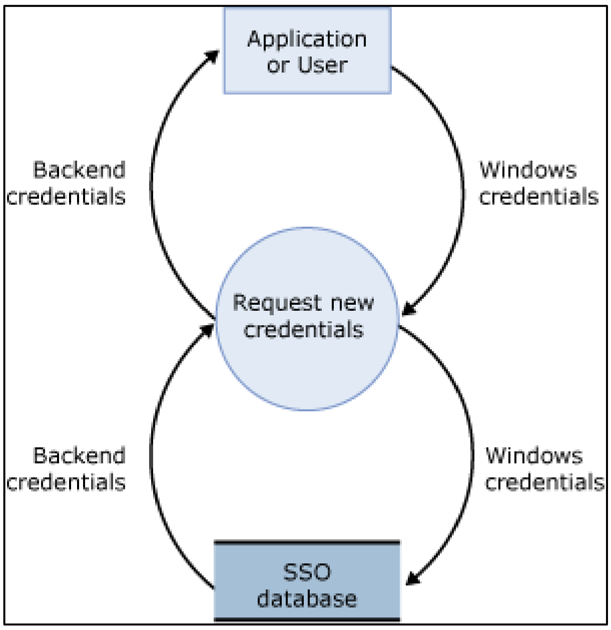
(d) Laboratory infrastructure should be virtualized and isolated (Firewalls/IDS/IPS, network segmentation, secure configuration, application whitelisting) from the production infrastructure.

(e) Workstations - Application blacklisting i.e. block malicious/suspicious applications automatically using applications like Zscaler.

(f) IOT - DNSSEC same as explained for RO above.

(g) All communication to and from RC should be using https/TLS1.2/SSL encryption.

(h) Mandatory security updates will be pushed time to time on all RC devices - they can be postponed only for a limited number of times. SSO is mandatory for all RC devices.



Data flow diagram for SSO

(i) **<u>Device authentication</u>**. IoT devices connect to each other, to servers, and to various other networked devices. Every connected device needs to be authenticated to ensure they do not accept inputs or requests from unauthorized parties (M2M networks, device certificates, PKI etc)

(j) Turning off unwanted features.

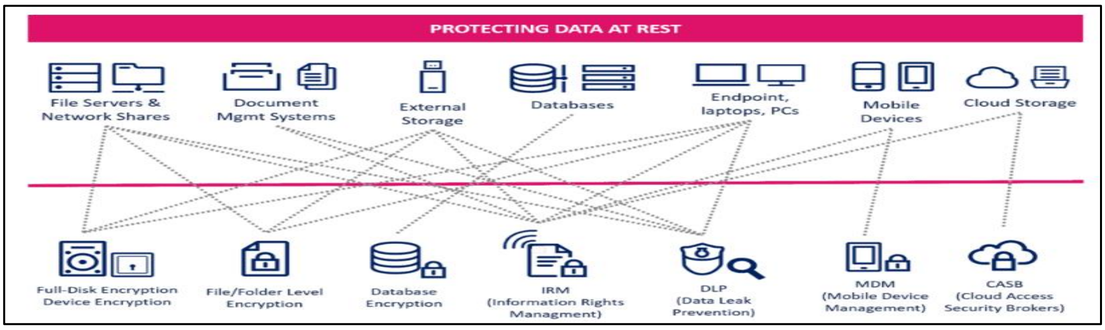
(k) **<u>DNS filtering</u>**. DNS filtering is the process of using the Domain Name System to block malicious websites. Adding DNS filtering as a security measure to a network with IoT devices prevents those devices from reaching out to places on the Internet they should not (i.e. an attacker's domain (example to prevent Dyn DNS service DDoS attack 2016)

Protecting Sensitive Data [13]

When it comes to protecting confidential information, we find that BITS WILP requires **different approaches or pose different protection needs**. Some need to protect the information on their mobile computers or laptops in case they are lost/stolen. Others wants to keep their documentation protected on file servers so that it can even be protected from improper access by Internal faculty/staff. Sometimes they need to protect documentation when it travels attached to an email because they use managed email servers or in the cloud. Also, to protect the documentation when it is sent to third parties or even internally in order to minimize the possibility of it being copied, unprotected or accessed by inappropriate users. We can **consider three states for information or data:-**

Data at rest

WILP File servers in RO, Payroll and Student information databases and flash drives. Hard disks etc. Documentation is considered secure at rest when it is encrypted and immune to a dictionary attack.


PROTECTING DATA AT REST
File Servers & Network Shares
Document Mgmt Systems
External Storage
Databases
Endpoint, laptops, PCs
Mobile Devices
Cloud Storage
Full-Disk Encryption Device Encryption
File/Folder Level Encryption
Database Encryption
IRM (Information Rights Managment)
DLP (Data Leak Prevention)
MDM (Mobile Device Management)
CASB (Cloud Access Security Brokers)

(i) **<u>Full disk encryption or device</u>**. In case of loss, the data contained in devices cannot be accessed by simply mounting the hard disk or device in another machine. However, if the computer or the file server is accessible by the administrator, nothing prevents a dishonest user from accessing the data, copying it, resending it, etc. The data is protected while residing on the device or hard disk but is no longer protected once it is extracted from the device.

(ii) **<u>File-level encryption</u>**. No partition or hard disk is encrypted, only individual files. Files are not only encrypted when they are stored on the disk, but can also be protected in transit, when they are sent for example as attachments in an email. In this case, transparent access by a user is lost, as well as transparent protection of the user. On the other hand, once the document has been decrypted by the recipient, it can be stored unprotected, resent unprotected etc.

(iii) **Database Encryption**. Database systems such as SQL Server or Oracle use Transparent Data Encryption (TDE) to protect data stored in databases. TDE technologies perform encryption and decryption operations on data and log files in real time. This type of encryption protects data at rest in the database but not when the data has already been accessed by the corresponding application and can be extracted.

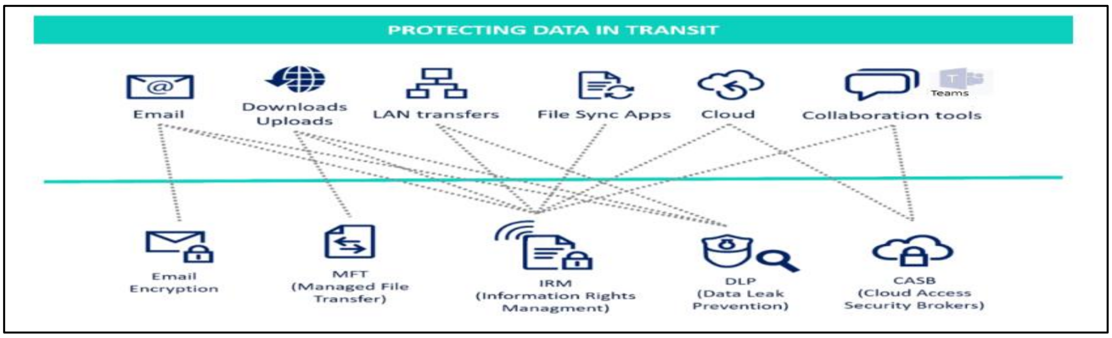
(iv) **Protection through Digital Rights Management (IRM)**. Data Rights Management technologies as SealPath (Information Rights Management) allow the encryption of documentation by applying persistent protection to it. The documentation at rest is encrypted and is only accessible to users who have access rights to it.

(v) **MDM (Mobile Device Management)**. MDM tools allow limiting access to certain corporate applications, blocking access to the device or encrypting data on the mobile or tablet. As with standard encryption, they are useful in the event that a device is lost, but when the data is sent to the outside of the device, it leaves unencrypted. This is discussed in depth in the hight level architecture section.

(vi) **DLPs (Data Leak Prevention)**. DLP enables a search or location of sensitive data on an endpoint or network repository. They are valid while the data is inside the organization, but they cannot act on it once it has left.

Data in transit

Data that travels through an email, web, collaborative work applications such as Slack or Microsoft Teams, instant messaging, or any type of private or public communication channel. It's information that is traveling from one point to another. We are in the age of digital collaboration and BITS WILP following the same, there are now plenty of ways to share our data with others. One of the most widely used has traditionally been email. However, we move data through other platforms such as collaborative work like Microsoft Teams, impartus for online class delivery, and share slides and recordings through cloud storage applications such as Box, OneDrive, Dropbox, moodle, etc.


PROTECTING DATA IN TRANSIT
Email
Downloads Uploads
LAN transfers
File Sync Apps
Cloud
Collaboration tools
Teams
Email Encryption
MFT (Managed File Transfer)
IRM (Information Rights Managment)
DLP (Data Leak Prevention)
CASB (Cloud Access Security Brokers)

(i) **Email encryption**. Provides end-to-end protection for message bodies and attachments based on PKI (Public Key Infrastructure), a combination of a private key and a public key The email and attachments are protected using the recipients' public key, and on receipt, the recipient uses his or her private key to decrypt the content. Once the email or attachment has been decrypted, control over it is lost and it can be forwarded, copied, etc.

(ii) **Managed File Transfer (MFT)**. This is a secure alternative to transferring files via FTP for example. The file is uploaded to a platform and a link is generated to download it. This link is sent by email or other means to the recipient who makes the download via HTTPS. It is possible to set expiration dates for the link, password to access it, etc. As it happens with the e-mail encryption, once the file has been downloaded, it is unprotected and you can do whatever you want with it.

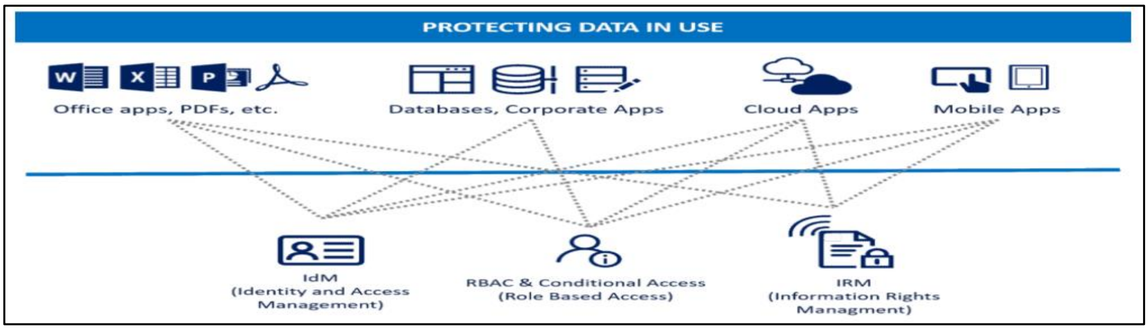
(iii) **DLP tools for data in transit**. DLP technologies provide in-transit or in-motion protection in that they are able to detect whether an attempt is being made to send confidential data outside the organization (e.g., credit card numbers) and block the sending of such data. They also allow for blocking copies of data to a USB drive, sending to network drives, uploading to web or cloud applications, etc.

(iv) **CASB (Cloud Access Security Brokers)**. With regard to data in transit, they can detect if a user tries to download sensitive data, and if he does not comply with certain security policy (e.g. is not a reliable user for this type of data) they can block the download. As with DLP, if the data has been downloaded, control over it is lost.

(v) **In-transit protection with digital rights**. Seal Path can be applied in the email to not only encrypt the body and attachments, but also to apply usage rights leaving only the content to be viewed, or to view and edit but not print, etc. They also allow for example to restrict the forwarding of the email to the recipients if desired. As a file protected with digital rights travels with the protection, protection in transit is offered via any medium. If a sensitive document is detected as coming out of the network or a confidential document is downloaded from a cloud application, they can automatically protect it depending on the security policy.

Data in use

When it is opened by one or more applications for its treatment or and consumed or accessed by users. user must be able to access the content decrypted (in the case that it was encrypted). To protect the data in use, controls should normally be put in place "before" accessing the content.

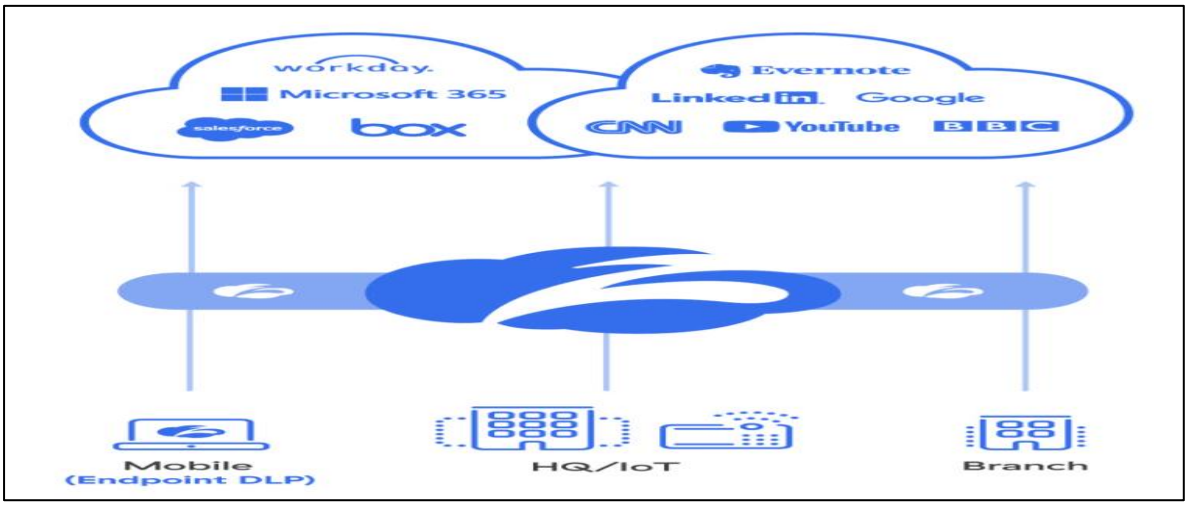

PROTECTING DATA IN USE
Office apps, PDFs, etc.
Databases, Corporate Apps
Cloud Apps
Mobile Apps
IdM
(Identity and Access Management)
RBAC & Conditional Access
(Role Based Access)
IRM
(Information Rights Managment)

(i) **Identity management tools**. To check that the user trying to access the data is who he says he is and there has been no identity theft. In these cases it is increasingly important to protect access to the data through a two-factor authentication, like for WILP teams setup implemented using -

(aa) **Conditional Access or Role Based Access Control (RBAC) tools**. Allow access to data based on the user's role or other parameters such as IP, location, etc.

(ab) **Through digital rights protection or IRM**. Obtain effective protection in the use of the data to limit what actions the user can take once they have accessed the data. For example editing, printing, etc. With an IRM protection applied directly on the file (not on the document manager or collaboration platform itself) apply a protection that travels with the documents and limits the opening permissions wherever it goes. Whether the data is online or has been downloaded, IRM can get a user to see it, but not completely unprotect it, print it etc.

Cloud DLP



Cloud DLP [14]

WILP needs a high-performance platform that inspects all internet and SSL traffic, secures endpoint data, and provides users with fast, consistent security regardless of their locations. Cloud DLP, along with Endpoint DLP, is part of a complete security stack as a service, fulfilling the demands of SSE while eliminating the costs and complexity of disjointed point products In other words, Cloud DLP delivers:-

(a) Identical protection on and off the network.

(b) Inline and endpoint enforcement for real-time protection.

(c) Full TLS/SSL inspection of all traffic.

(d) A fully integrated security service edge.

(e) Storage arrays supporting encryption and deduplication.

Compliance

In house solution for continuous compliance check as the standards keep changing. This tool will provide flexible rule and policies configuration to add alerts/action (shut off non-compliant systems) etc. It may be possible to shift to cloud compliance tools (GCP compliance, AWS artifact etc) if WILP decides to leverage cloud in future.

Incident Response

The IT team should be having the required skill sets to respond to a security incident and avert active attacks. We need to maintain:-

(i) Redundant systems and load balancers are in place in the Data Centre in case of DDoS/DoS/Ping Flood kind of incidents to keep the systems highly available.

(ii) Alert for unusual activities and anomalies inside the Data Centre. SIEM, FIM are deployed for this purpose. SASE will also have an alerting/notification mechanism.

(iii) WILP developed applications should have enough audit logs to monitor security issues.

(iv) Network Security Group (NSG) capabilities for visibility into network activities on the Cloud platform (example Moodle/Impartus tools should provide APIs to get health and performance statistics).

(v) Vulnerability scans and Pen testing activity should happen frequently to detect the vulnerabilities in the system proactively.

(vi) Data protection (Encrypted Snapshot/Synchronous replication) and Backup tools are in place to mitigate the impact of Ransomware incidents and buy time for negotiation and calculated response.

(vii) Abide by best practices of incident response mentioned in best practices section and the link below https://learn.microsoft.com/en-us/security/compass/ incident-response-process.

Costing estimates

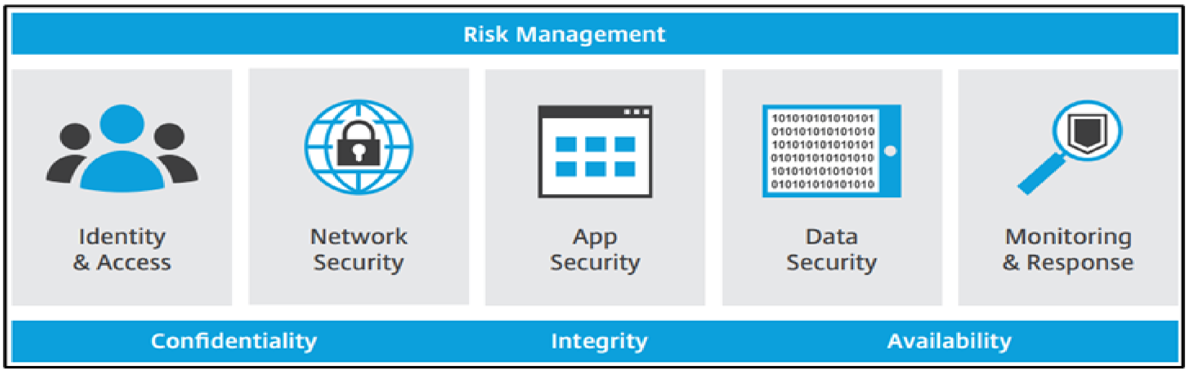
The cost estimates of all the services for enhancement if enterprise security are calculated base on costs available on internet. The same may be negotiated during purchase or tendering process by the OEM.

Ser No	**Solution**	**Cost**	**Source**	**Comments**
(a)	DLP [15]	$13500	Purplesec	
(b)	SASE [16] CASB ZTA DNS Security IPSec NGFW FWaaS NaaS SDWAN	8-12$/User /Month	Perimeter81	Although cost seems high but the solution reduces other cost such as Private WAN and MPLS using SD-WAN solution. We can use more comprehensive solution for critical data servers and network (Staff and Admins) and limited features for accessing Services with less

				importance (Forums and generic website)
(c)	IDP [17] (Mostly SASE provider is partnered with IDP)	If IDP solution is used separately 2$/User/ month	Netscope	
(d)	Hardware Cost	-	-	Not an additional cost with regular OS/Software patching
(e)	SecOps	3x12LPA	Glassdoor	3 dedicated secops professionals
(f)	Primary Storage supporting security features like encryption	$40,000 each	https://www.krgroup.com/pure-and-nimble-storage-cost/	Should support TPM, Secure Boot, Root of Trust, Encryption, 2FA etc
(g)	Secondary Storage Array for backup security license	Security license	https://storagepricing.org/hpe-storeonce-pricing/	Useful to restore data in case of ransomware attack/natural disasters. Array costs $35000 each

Best Practices

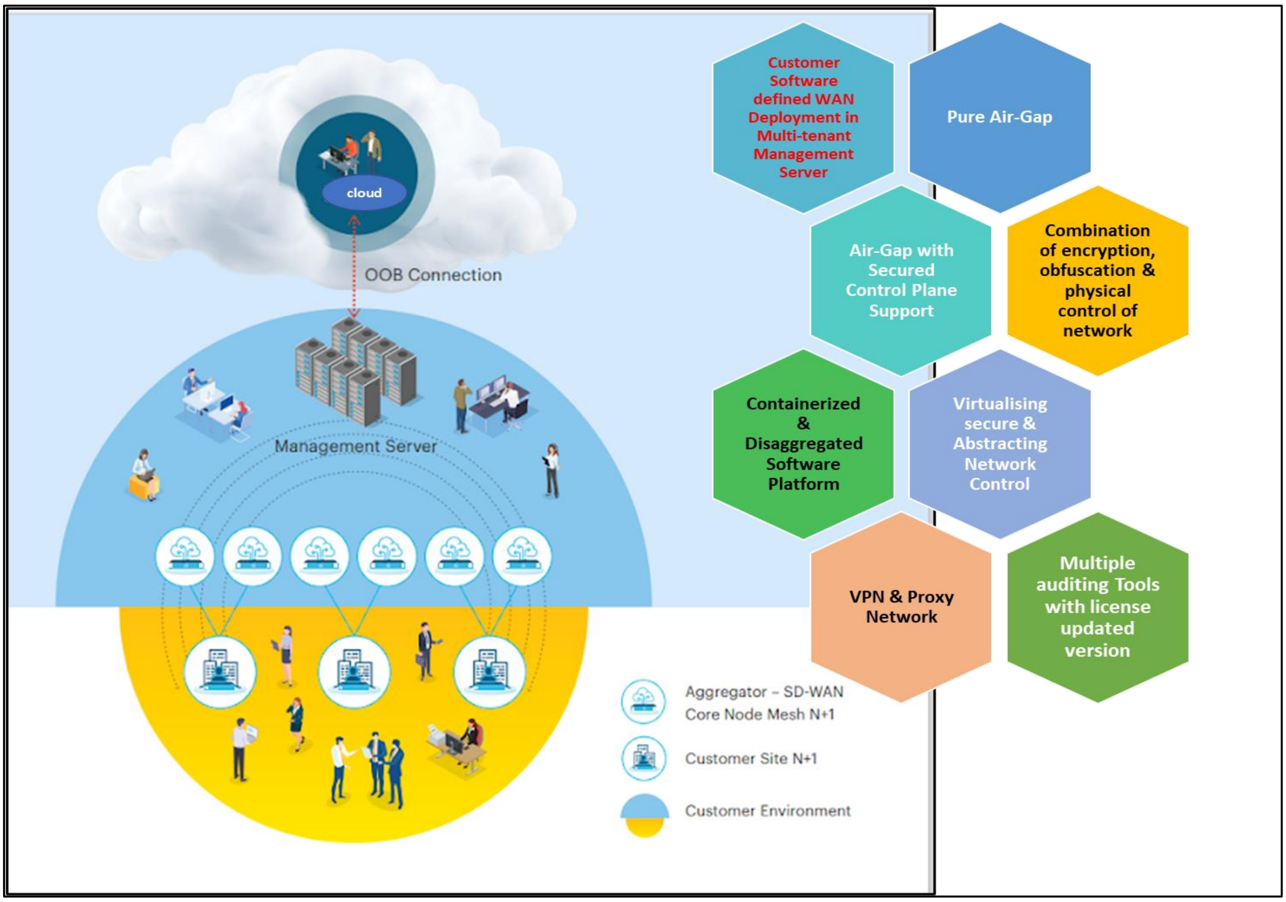
IT and security aspects face challenges of reducing risks to acceptable levels while ensuring ease of use and productivity. People should be able to work as per purposes, any location, device or network without being frustrated by an overly constrained or complex user experience. At the same time, it is essential to protect enterprise apps and data from being compromised by security threats, prevent loss and theft, and ensure full compliance with standards and regulations.



Three pillars of Security

Secure productivity in the modern enterprise

The security challenge facing today's enterprises is growing rapidly across two dimensions, exacerbated by both escalating levels of risk and the continued evolution and diversification. This must extend across every type of app we use over any network, on any device. Even as the requirements of the mobile workforce grow vastly more complex, IT must continue to strive for simplicity.


cloud
OOB Connection
Management Server
Aggregator – SD-WAN Core Node Mesh N+1
Customer Site N+1
Customer Environment
Customer Software defined WAN Deployment in Multi-tenant Management Server
Pure Air-Gap
Air-Gap with Secured Control Plane Support
Combination of encryption, obfuscation & physical control of network
Containerized & Disaggregated Software Platform
Virtualising secure & Abstracting Network Control
VPN & Proxy Network
Multiple auditing Tools with license updated version

The practices [17] are very important and should be implemented/followed all through the institution. Some of them are enlisted below and may be updated as per requirements and change of threats dimensions:-

(a) Hardware based security

(i) Use hardware from trusted vendors as it can be affected by crypto mining, ransomware attacks, steal data and intellectual property.

(ii) For servers and employee PCs, we need to use hardware from trusted vendors which has built in hardware security as these technologies are rooted in silicon and can be operated without being affected by corrupted software.

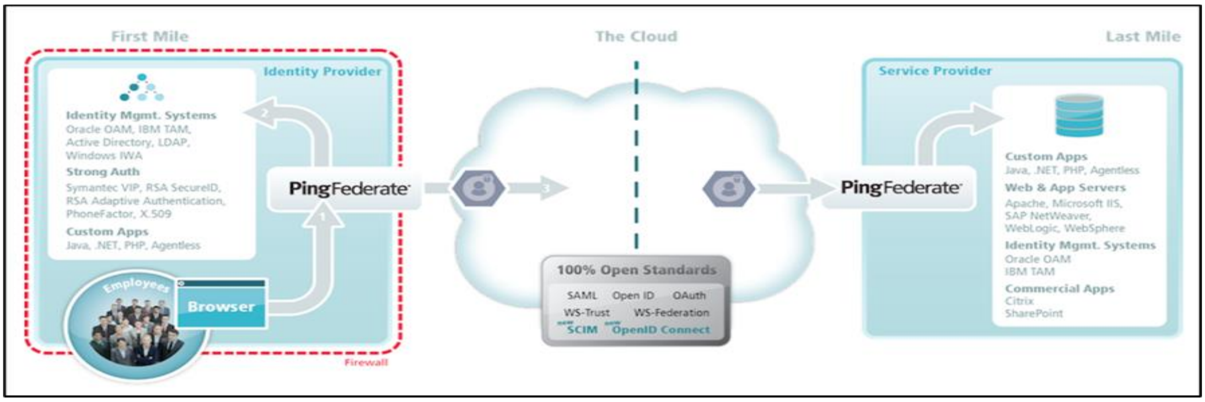
(iii) Application and data security to provide the hardware resources needed for virtualized workloads and reinforce virtualization-based security with hardware-based security features to protect applications at runtime and data in memory.

(iv) **Case Study**. Computer chips allowed the attackers to create a stealth doorway into any network that included the altered machines by China [19].

(b) Secure Internet-identity platform

(i) Use Enterprise identity bridge such as Ping federates to enable outbound and inbound solutions for single sign-on, federated identity management, student/staff identity and access management, mobile identity security, API security and social identity integration. Browser-based SSO extends employee, student etc identities across domains without passwords using only standard identity protocols.

(ii) All protocol definitions, public key infrastructure (PKI) keys, policies, profiles are managed in a single location, eliminating the need to maintain redundant copies of these configurations and trust relationships.



(iii) Encryption is a database security best practice no-brainer. Use strong encryption to protect databases in three ways:-

(a) Require all database connections to use TLS encryption to protect data in transit.

(b) Encrypt disks containing data stores to protect against their loss, theft or improper disposal.

(c) Use column-level encryption capabilities to protect the most sensitive fields against snooping.

(iv) **Case Study**. Griffith University which has over 50000 students and staff was seeking a solution that would serve as a centralized authentication service and provide its users with seamless authentication to the hundreds of apps they needed to access.[20]

(c) Security concerns about E-Mail

(i) Phishing is the most vulnerable for E-Mails. Simple practice of not to open email attachments unless you are expecting the email with the attachment and you trust the sender. Threats are attached to emails that pretend to be from someone you know but the “from” address has been altered and it only appears to be a legitimate message from a person you know.

(ii) The emails appears genuine but instead are sent by the computer when activated by the malicious code. Those malicious code on the computer of anyone who receives the email and opens the attachment will be affected.

(iii) Beware of emails which ask for sensitive personal or financial information regardless of who the email appears to be from. No responsible person will ask for sensitive information in an email.

(iv) **Case Study**. Email Inboxes belonging to the BBC were bombarded by about 50 million malicious email attacks between 1 October 21 and January 22 at an average rate of 3,83,278 a day. [21]

(d) Security concerns about web links in email, instant messages and social media

(i) Do not click on links in email messages as it can have embedded malicious links inside. Once a recipient clicks on the link, malicious software (for example, viruses or key stroke logging software) is installed on the user’s computer. Don’t do it unless you know what the web link connects to and you trust the person who sent the email to you.

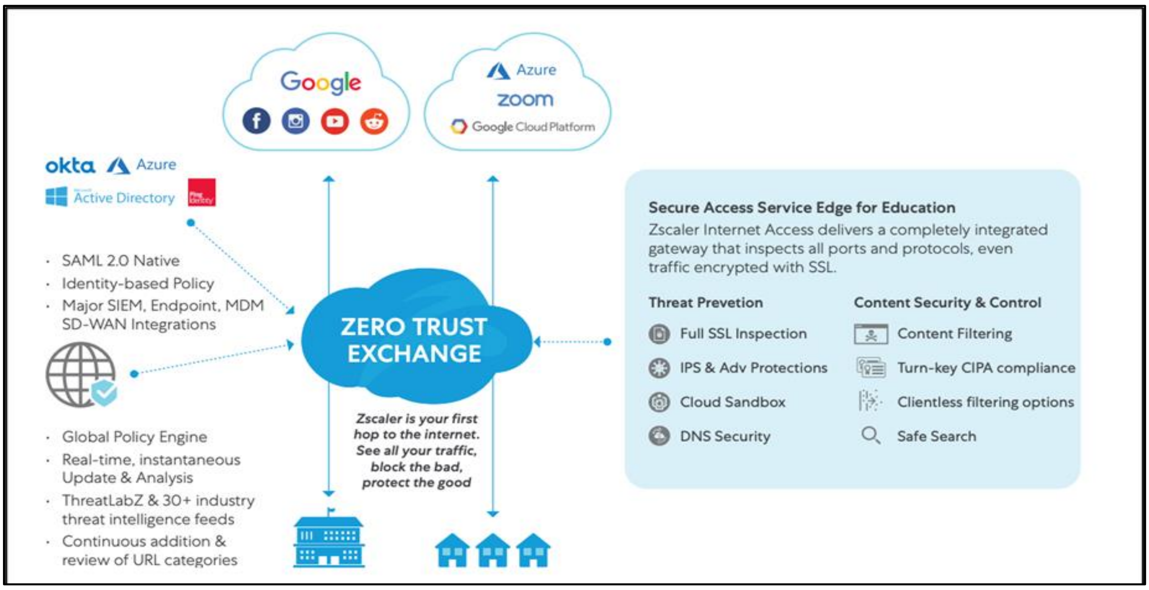
(ii) Always hold the mouse pointer over the link and look at the bottom of the browser window to ensure that the actual link (displayed there) matches the link description in the message. (The mouse pointer changes from an arrow to a tiny hand when placed over an active link)

(iii) **Case study**. Kent State University has to safeguard student and faculty data against cyber attacks and vulnerabilities. In 2020 and due to COVID-19 regulations, the university’s IT team had to move over 9,000 courses to online learning in two weeks.
DLP solutions. Azure Cloud Services, Azure Active Directory, Microsoft 356, Microsoft Intune, and Microsoft Teams.[29]

(e) Zero trust solution for incoming and outgoing traffic

(i) Securing cloud and on-premises systems is a complex balance to access resources to drive academic discovery while protecting critical data, Personally Identifiable Information (PII) and Intellectual Property (IP).

(ii) Zero Trust exchange provides customers a Zero Trust approach only allowing the right users to access to the right data while also enabling each department to manage its own environment as needed. Secure Access Service Edge (SASE) architecture delivers secure connections while ensuring users are only a short hop from their applications.



- SAML 2.0 Native
- Identity-based Policy
- Major SIEM, Endpoint, MDM SD-WAN Integrations

- Global Policy Engine
- Real-time, instantaneous Update & Analysis
- ThreatLabZ & 30+ industry threat intelligence feeds
- Continuous addition & review of URL categories

Zscaler is your first hop to the internet. See all your traffic, block the bad, protect the good

Secure Access Service Edge for Education

Zscaler Internet Access delivers a completely integrated gateway that inspects all ports and protocols, even traffic encrypted with SSL.

Threat Prevetion	Content Security & Control
Full SSL Inspection	Content Filtering
IPS & Adv Protections	Turn-key CIPA compliance
Cloud Sandbox	Clientless filtering options
DNS Security	Safe Search

(iii) **Case Study**. Hong Kong International School enhances security posture to prevent cyberthreats and secure student data using NGFW. [22]

(f) Security concerns about web links in email, instant messages and social media

(i) Do not click on links in email messages. Some scams are in the form of embedded links in emails. Once a recipient clicks on the link, malicious software (for example, viruses or key stroke logging software) is installed on the user's computer. It is not a good idea to click on links in a Facebook or other social media page. Don't do it unless you know what the web link connects to and you trust the person who sent the email to you.

(ii) Always hold the mouse pointer over the link and look at the bottom of the browser window to ensure that the actual link (displayed there) matches the link description in the message. (The mouse pointer changes from an arrow to a tiny hand when placed over an active link)

(g) Security concerns about popup windows and other hacker tricks

(i) Do not respond to popup windows requesting that you click "ok" for anything. Close the popup window by selecting the X in the upper right corner of the popup window.

(ii) Do not respond to popup windows informing you that you have to have a new codec, driver or special program for something in the web page you are visiting. Close the popup window by selecting the 'X' in the upper right corner of the popup window.

(iii) Most of these popup windows are actually trying to trick you into clicking on "OK" to download and install spyware or other malicious code onto your computer.

(iv) Teach everyone not to bring USB drives into the office and plug them into your official computers (or to take them home and plug into their home systems). It is a good idea to disable the "AutoRun" feature for the USB ports on computers to help prevent such malicious programs from installing on your systems.

(v) **Case Study**. Your Windows 10 is infected with viruses scam. This scheme makes false claims about visitors devices being infected in order to gain and subsequently abuse users trust. Typically, such scams are used to endorse untrustworthy/harmful software and/or obtain funds through fraud. [23]

(h) Secure Online payments/EMI enrolment

(i) Online business/commerce/banking should only be done using a secure browser connection. Ensure not to save username or passwords.

(ii) After any online commerce or banking session, erase your web browser cache, temporary internet files, cookies and history so that if your system is compromised, that information will not be on your system to be stolen by the individual hacker or malware program.

(iii) **Case Study**. Multiple incidents of online fraud due to ATM fraud, UPI, Paytm etc. [24]

(i) Protection against Social Engineering attacks

(i) The social engineer researches the organization to learn names, titles, responsibilities and publically available personal identification information. Then the social engineer usually calls the organization's receptionist or help desk with a believable but made-up story designed to convince the person that the social engineer is someone in or associated with the organization and needs information or system access which the organization's employee can provide and will feel obligated to provide. To protect against social engineering techniques, employees must be taught to be helpful but vigilant when someone calls in for help and asks for information or special system access.

(ii) The employee must first authenticate the caller by asking for identification information that only the person who is in or associated with the organization would know. If the individual is not able to provide such information, then the employee should politely but firmly refuse to provide what has been requested by the social engineer. The employee should then notify management of the attempt to obtain information or system access.

(iii) **Case Study**. A new report of threat data collected for over 12 months across a section of media and entertainment customers including sports teams, talent agencies, celebrities, and streaming services reveals the kinds of unique vulnerabilities entertainment companies deal with at the hands of criminals. [25]

(j) Enforce the principle of least privilege

(i) Limiting users access to the smallest set of privileges necessary to carry out their job functions is usually the first piece of advice offered in any cybersecurity book. How well that theoretical goal maps to the reality of our enterprise databases is an important question. To assess this, enterprises should ask themselves several questions, including the following: -

(aa) Do developers have full access to production databases?

(ab) Do system engineers have access to the databases on the systems under their care?

(ac) Do database administrators have full access to all databases or just those that fall within their areas of responsibility?

(k) Security considerations for administrative privileges

(i) No one should surf the web using a user account which has administrative privileges. If you do surf the web using an administrative user account, then any malicious code ill have the same administrative rights as your user account has.

(ii) It is best to set up a special account with "guest" (limited) privileges to avoid this vulnerability.

(iii) **Case Study**. At least one in four IT security staff use their privileged login rights to look at confidential information, a survey has revealed.[26]

(l) Issues in downloading software from the Internet

(i) Do not download software from any unknown web page. Only those web pages belonging to businesses with which you have a trusted business relationship should be considered reasonably safe for downloading software.

(ii) Most other web pages should be viewed with suspicion. Be very careful if you decide to use freeware or shareware from a source on the web. Most of these do not come with technical support and some are deliberately crippled so that you do not have the full functionality you might be led to believe will be provided.

(iii) **Case Study**. Student's Download of 'Crack' Software Leads to Ransomware Attack on EU Research Institute.[27]

(n) Disposing of old computers and media

(i) When disposing of old business computers, remove the hard disks and destroy them. The destruction can be done by taking apart the disk and beating the hard disk platters with a hammer. You could also use a drill with a long drill bit and drill several holes through the hard disk and through the recording platters.

(ii) When disposing of old media (CDs, floppy disks, USB drives, etc), destroy any containing sensitive business or personal data.

(iii) Media also includes paper. When disposing of paper containing sensitive information, destroy it by using a crosscut shredder. Incinerate paper containing very sensitive information.

(iv) It is very common to discard old computers and media without destroying the computers' hard disks or the media.

(v) Sensitive business and personal information is found on computers purchased on online and thrift shops. This is a practice which can result in identity theft for the individuals whose information is retrieved from those systems. Destroy hard disks & media and recycle everything else.

(o) Conduct regular access reviews and monitoring database activity

(i) It is no secret that privilege creep affects virtually every technology organization. As technical and nontechnical staff move among job roles and project assignments, they accumulate new and different permissions each time their responsibilities change. New permissions are quickly sought and approved because the lack of permissions gets in the way of work. Old and unnecessary permissions may persist for months or years because they do not cause operational issues for the employee's everyday work. They do, however, expand the scope of an attack should that user become a malicious insider or fall victim to an account compromise.

(ii) Conduct regular, scheduled reviews of database access to ensure the principle of least privilege still applies. Pay particular attention to users who have direct access to the database, as this access may bypass application-level security controls.

(iii) Enable database monitoring on systems and ensure the logs are sent to a secure repository. Also, implement behaviour-based monitoring rules that watch for unusual user activity, particularly among users with administrative access.

(p) Harden, patch, configure

Follow good hardening and patching hygiene. This can play out in one of a few ways, depending on whether the database is managed by the organization or a service provider :-

(i) Organizations managing their own database nodes. For on-premises or workloads inside an IaaS ecosystem, ensure the OS is hardened and patched and that the database service itself is hardened and patched. Use a security technical implementation guide or other community configuration benchmarks to do this. Build for database instances you maintain. For example, by making sure they are segmented and that they follow good practices, such as not using production data for testing purposes.

(ii) Organizations using managed database services. The goal is the same, but the process is different. Patching and OS-level hardening are the managed service's responsibility. Ensure that the services are optimally configured from a security perspective. Enable any security posture optimization features available. This implies customers understand those features and how to enable and configure them.

(q) Documentation

(i) Documentation implicit in the above suggestions, including artifacts such as threat models and supporting data flow diagrams, access control matrices to support least privilege enforcement, data inventory and control implementations for example, which columns are encrypted and using what mechanisms.

(ii) Documentation of operational processes and procedures, as well as decision artifacts such as risk analyses.
(iii) Documentation is a bit like insurance. In the short term you might get away with not having it, but eventually you will get burned. Documentation is required in audits and it's also mandated under certain regulatory frameworks. What's more, having precise documentation that is regularly updated increases an organization's overall maturity and the resilience of its processes.

(iii) **Case Study**. Central National Bank of Waco is an attractive target for cyberattacks; it surpassed $1 billion USD in assets in 2021. They contacted CrowdStrike after an incident occurred in the middle of a forensics audit of the bank's security system. [28]

(r) DNS Security

(i) It ensures your DNS infrastructure is operating efficiently and reliably. This requires establishing redundant DNS servers, using security technologies like Domain Name System Security Extensions (DNSSEC), and mandating stringent DNS logging.

(ii) If a cybercriminal infiltrates a DNS system, they can send users to fake or malicious sites. They can also steal data, hijack websites, or inundate servers with requests, shutting them down eventually. DNS security is designed to prevent these kinds of attacks.

(iii) **Case Study**. Attackers took advantage of the pandemic by creating a slew of malicious NRD(newly registered domains) that masqueraded as official COVID-19 related resources.[33] The focus of the attackers shifted depending on current events related to the pandemic.

Conclusion

WILP being a reputed and top tier educational premium institute needs security architecture articulated with multifaceted approach and defence in depth. Business requirements and used cases encompassed student, staff as well as infrastructure requirements highlighting the need for proactive security and preventive approach with sufficient budget allocated. High level architecture is judiciously designed giving equal importance to Data, Processes, Hardware Infrastructure, Compliance and Incident response, not just for confidentiality, integrity and availability during normal operations but also planned for contingency and disaster recovery scenarios. Detailed security design for HO, RO and RC encompasses latest enterprise security trends like SASE, NGFW, DLP, BYOD etc. Though, cost is not a concern, tentative cost estimates are provided to prove expense of security in fact is beneficial for long term. Even with best quality security infrastructure and Hardware system is only as secure as its weakest link. Hence best practices are adopted to avoid well-known security incidents. All in all, this is a best-in-class security architecture suggested to address all aspects of a medium sized reputed multi-national educational institute providing safe and secure distance learning experience in this digital transformation and social network era.

References

[1] - https://bits-pilani-wilp.ac.in/

[2] - https://www.bbc.com/news/uk-england-essex-61312383

[3] - https://www.jdsupra.com/legalnews/simpson-university-confirms-data-breach-7498820/

[4] - https://www.news18.com/news/education-career/jee-main-scam-how-russian-hackers-rigged-engineering-exam-cbi-reveals-6104017.html

[5] - https://edusasha.com/the-guide-to-everything-elearning/elearning-infrastructure-and-architecture/

[6] - https://www.aicte-india.org/sites/default/files/cyber/AICTE%20Cyber%20 Security% 20Strategy%20for%20Higher %20Education%20Institutes.pdf

[7] - https://www.researchgate.net/publication/305380830_Mobile_Device_Management _MDM_in_Organizations

[8] - https://www.acunetix.com/blog/articles/dns-zone-transfers-axfr

[9] - https://medium.com/@aman.bansal93/security-zoning-in-network-architecture-ff7693b91556

[10] - paloaltonetworks.com

[11] - https://www.dnsstuff.com/ids-vs-ips

[12] - https://www.javatpoint.com/ips-intrusion-prevention-system

[13] - https://www.sealpath.com/blog/protecting-the-three-states-of-data/

[14] - https://www.zscaler.com/technology/data-loss-prevention

[15] - https://purplesec.us/best-data-loss-prevention-software/
https://www.somansatech.com/company/buy-online/

[16] - https://www.perimeter81.com/pricing

[17] - https://www.okta.com/pricing/
https://www.pingidentity.com/en/platform/pricing.html

[18] - https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/hardware-security-features.html
https://www.techtarget.com/searchsecurity/tip/4-enterprise-database-security-best-practices

[19]-https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-America-s-top-companies

[20] - https://www.pingidentity.com/en/customer-stories/3301-griffith-university.html

[21] - https://www.computerweekly.com/news/252514025/BBC-blasted-with-millions-of-malicious-emails

[22]- https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/customers/hong-kong-international-school.pdf

[23]- https://www.pcrisk.com/removal-guides/23228-your-windows-10-is-infected-with-viruses-pop-up-scam

[24] - https://www.instamojo.com/blog/online-payment-fraud-tips-to-prevent-them/

[25]- https://www.the420.in/10-celebrities-who-were-recently-attacked-by-the-hackers-on-social-media/

[26] - https://www.computerweekly.com/news/2240111956/One-in-four-IT-security-staff-abuse-admin-rights-survey-shows

[27]- https://vpnoverview.com/news/students-download-of-crack-software-leads-to-ransomware-attack-on-eu-research-institute/

[28]- https://www.crowdstrike.com/resources/case-studies/central-national-bank-of-waco/

[29] datamation.com/security/data-loss-prevention-use-cases/

[30] - https://www.securityweek.com/top-five-worst-dns-security-incidents

[31]- https://medium.com/@marioplatt/what-is-sabsa-enterprise-security-architecture-and-why-should-you-care-a649418b2742]

[32] - https://www.bpalermo.com/security-architecture.html

[33] - https://unit42.paloaltonetworks.com/covid-19-themed-phishing-attacks/