ISG Thought Leadership Paper

Advanced Persistent Threats

The ZTA Imperative in a Mid-COVID World

January 2021

ISG Research™

Tech Mahindra

About ISG

ISG (Information Services Group) (Nasdaq: **III**) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data.

For more information, visit **www.isg-one.com**

ISG Research™

About This Report

ISG is solely responsible for the content of this report. Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by, and are the sole property of, ISG.

The research and analysis presented in this report includes research from ongoing ISG research programs, including our global survey and interview work with user enterprise business and IT leaders, briefings with providers, and analysis of publicly available market information from multiple sources.

Research conducted for this report, and publication of this report, were sponsored by Tech Mahindra.

imagine your future®

Contents

SYNOPSIS

This ISG Thought Leadership Report examines the factors behind the growth in advanced persistent threats (APTs) in a mid-COVID-19 world.
It explores how the increase in number of remote workers has made businesses more vulnerable to cyber attackers, and how nation states and criminal groups sponsored by them are increasingly being recognized as major threats. A complete list of recent attacks is also provided.

The report looks at the anatomy of an APT attack, the benefits afforded by the adoption of a Zero Trust Architecture (ZTA) and at the key elements of a ZTA.

It then examines the many advantages of a ZTA, many of which are beyond the world of cyber security.

Finally, it provides a checklist of recommendations for use by ICT professionals to act upon to mitigate the effects of an APT.

> *“Cyber security is not just the role of the cyber security team. It’s everybody’s job, right up to board level. If there is an incident it focuses people’s minds. User education is everything. You need to get buy in across the organization, and make everyone cyber aware.”*
>
> – CISO Interview

EXECUTIVE SUMMARY

Cyber criminals are taking substantial effort and using highly sophisticated methods to breach network infrastructures. They are using APTs to access sensitive data over a long period of time, but without being detected. Many APTs are initiated by nation states or hacking organizations sponsored by them.

The COVID-19 pandemic has increased APTs, primarily as a large number of people are working remotely, often from their homes. Many organizations have recognized the many advantages of remote working, including (in many cases) increased employee productivity, curtailed costs related to office space and travel and improved collaboration. But these advantages come with increased vulnerability to cyberattacks through the use of networks that are less secure. In this context, the importance of maintaining a culture of cyber resilience has never been more important.

Effective defense against APTs requires highly skilled cyber security practitioners, with the abilities and resources to defend corporate and even national level infrastructure. This means upskilling cyber security resources and establishing security as a core value throughout the workforce.

Unlike cyberattacks, APTs are not isolated incidents — they typically take the form of a sustained campaign, employing many types of attacks and technologies. Therefore, a "security first" mindset is critical in establishing new behavioral patterns within an organization. Also important are continuous improvements in an organization's cyber security architecture, with complete awareness of recent trends in security services and technologies.

APTs come in many forms and so do the types of protection — a combination of technology and human factors that fall into four main categories — prevention, detection, response and analysis. Ideally, enterprises should maintain a ZTA to fight cyberattacks and, in particular, APTs.

In a ZTA, as the name suggests, no component of a corporate network is trusted; every access (or identity), by each component and at each stage, must be verified. This is very different from the traditional paradigm of perimeter security. With a ZTA, there is no such perimeter within which transactions are trusted, and which serve as a barrier against cyberattacks.

This report shows the benefits of adopting a broader and more holistic perspective toward cyber security through the adoption of ZTA practices and philosophies. A ZTA enforces more robust security practices and has many benefits for the more effective implementation of digital transformation, at all levels. It shows that a ZTA is the most effective form of cyber hygiene an organization can adopt.

The most effective methods of protection are listed in the "Recommended Actions" section of this report.

THE EVOLUTION OF CYBER SECURITY IN A MID-COVID-19 WORLD

The COVID-19 pandemic has changed the world in many ways, where the human and economic costs have been enormous; it has changed the way we do business and the way we go about our daily lives. Many more people are now working remotely, usually from home. This is being perceived as a permanent change and is having a significant effect on the cyber security landscape.

With a large number of remote workers, the number of pain points and vulnerabilities, in corporate networks, have increased, making it easier for entities with malicious intent to breach the networks. In recent years, an increasing number of these attacks are originating from nation states, or cyber attackers, which are often criminal groups sponsored by nation states.

This paper highlights some of the recent attacks that can be traced directly to end-point vulnerabilities exposed by the pandemic. At the end of the day, cyber security is dependent on the human factor — irrespective of the technology employed, its effectiveness is dependent on human behavior.

COVID-19 has seen a significant increase in the number of phishing and ransomware attacks, many of which are taking advantage of user fears and insecurities over the pandemic. At times, the many kinds of attacks and risks are related to the carelessness of an organization's own employees. Therefore, enterprises need to implement more stringent systems/codes than in the past — in short, focus on building a security culture within the organization.

Attackers are increasingly using highly sophisticated methods to intrude into a network infrastructure; an APT is an insidious form of cyberattack, often initiated by nation states, and used to breach and eventually influence the political or economic environment of a target. They are often initiated by organized criminal networks that are sponsored or work in tandem with nation states. APTs access sensitive data over a long period of time and cannot be easily detected.

> *"COVID has greatly increased phishing, exploiting people's anxiety and thirst for knowledge. Now, with various Incentives coming through from different areas of government, there are many different channels which look bona fide but which are malicious. We try to weed those out, but it's a challenge."*
>
> – CISO Interview

ISG research partner, DataDriven, recently conducted a global survey involving approximately 300 CIOs and senior ICT decision makers across nine countries. The survey focused on digital transformation (DX), revealing specific ICT challenges, current status of DX and other technology initiatives and implementation plans, including cyber security. The following charts examine some of the key findings.

Fig 1

ICT Strategic Challenges

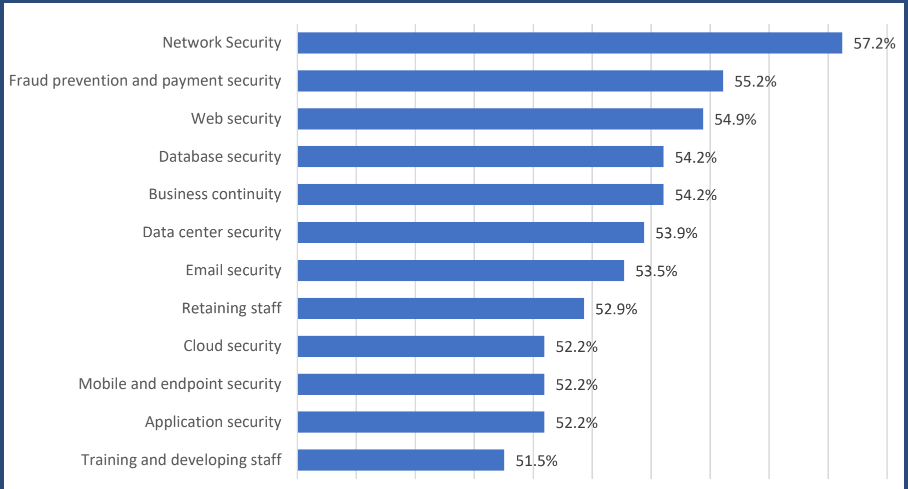
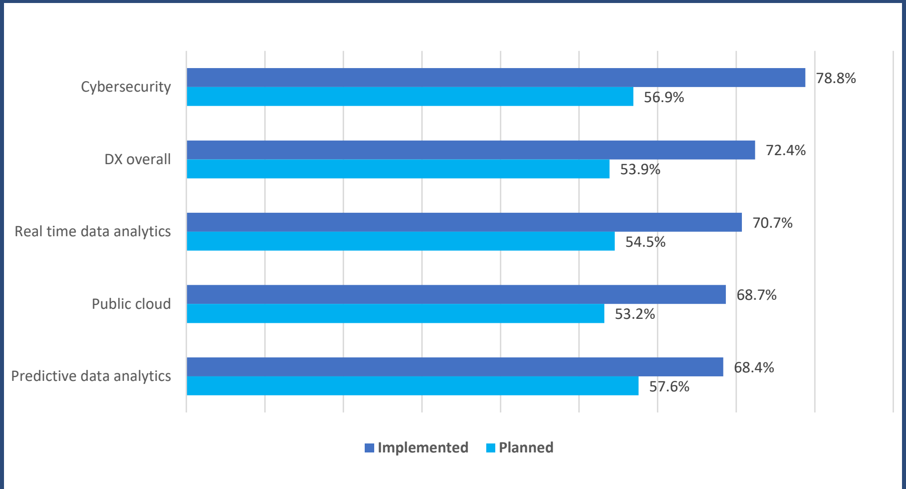


Fig 2

Digital Transformation (DX) Strategies Implemented vs Planned

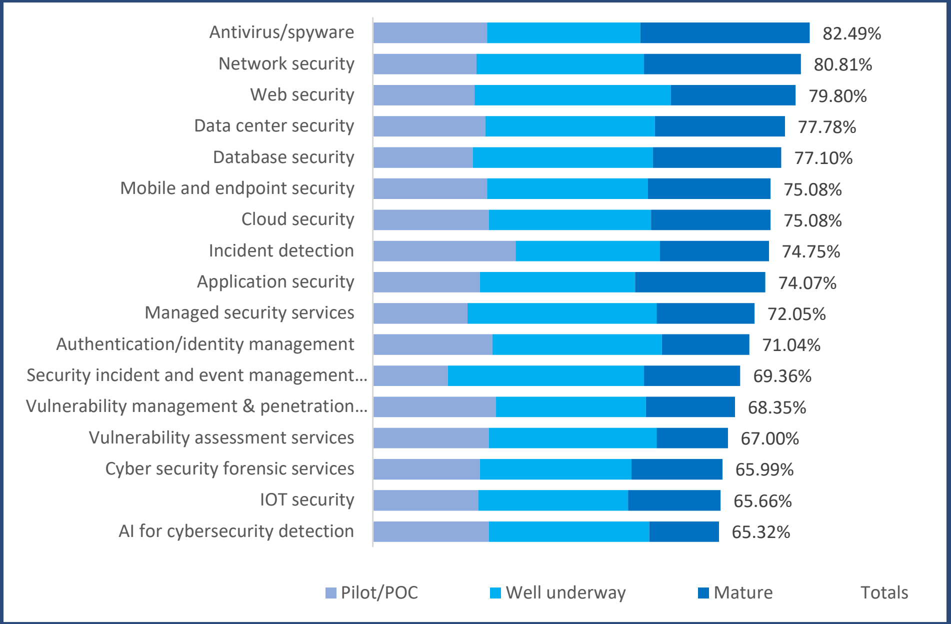


ICT Strategic Challenges. The first chart above (Fig. 1) lists the ICT strategic challenges faced by organizations. Of the 22 technologies and initiatives covered in this part of the survey, respondents indicated that 10 of the top 12 ICT strategic challenges are related to security.

Digital Transformation (DX) Strategies. Among the list of 22 potential technology initiatives for digital transformation strategies currently implemented or planned in the next twelve months (Fig.2), cyber security was at the top or was indicated as a priority in both categories.

Fig 3

Cybersecurity Implementation



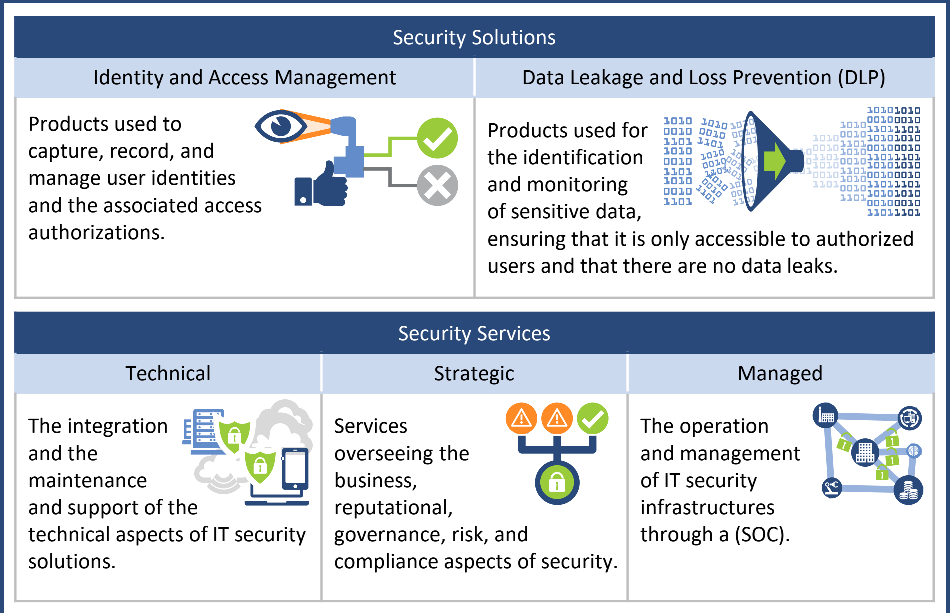
Cybersecurity Implementation: Regarding the maturity of implementation of various cyber security tools and techniques, the survey revealed that anti-virus tools and spyware were most likely to have been implemented, followed by network, web security, data center security and database security (Fig. 3).

Respondents have comparatively low levels of implementation of more sophisticated approaches such as Security Incident and Event Management (SIEM) and the use of artificial intelligence (AI) for threat detection, indicating potential gaps in overall defense.

The survey shows that the majority of respondents have signiciant levels of implementation across a wide range of cyber security and related technonologies.

Fig 4

Cyber Security Solutions and Services



Security Solutions

Identity and Access Management

Products used to capture, record, and manage user identities and the associated access authorizations.

Data Leakage and Loss Prevention (DLP)

Products used for the identification and monitoring of sensitive data, ensuring that it is only accessible to authorized users and that there are no data leaks.

Security Services

Technical

The integration and the maintenance and support of the technical aspects of IT security solutions.

Strategic

Services overseeing the business, reputational, governance, risk, and compliance aspects of security.

Managed

The operation and management of IT security infrastructures through a (SOC).

CYBER SECURITY TRENDS AND CHALLENGES

In August 2020, ISG Research conducted an extensive evaluation of cyber security solutions and service providers across seven countries, namely, the U.S., the U.K., Germany, Switzerland, France, Brazil and Australia. Based on hundreds of interviews with providers, users and ISG advisors.

These reports (published as *ISG Provider Lens (IPL) – Cybersecurity Services & Solutions <Country> 2020*), also contain a significant and detailed analysis of global cyber security trends.

The reports are structured according to ISG's Cyber Security Solutions and Services taxonomy shown here, and include:

- Identity and Access Management
- Data Leakage and Loss Prevention (DLP)
- Technical Security Services
- Strategics Security Services
- Managed Security Services

THE EVOLUTION OF APTS

The ISG IPL reports, and other research related to actual user engagements, indicate that increased digitalization has pushed corporate security out of its comfort zone. Many new challenges are confronting enterprises and their chief information security officers (CISOs) at a time when there is an acute shortage of cyber security experts in the market. In addition technically sound resources in areas such as threat exploration, malware analysis and intrusion detection are scarce.

Until recently, many enterprises regarded cyber security initiatives as a necessity, but not as one that added value. It was just seen as an add-on to business functions that promised revenue growth or cost reduction. But with the increasing use of digital technologies in an organization, both for internal and external functions, cyber security is now essential to risk management.

The days of relying solely on perimeter security are gone. Enterprises of all sizes and in all industries need to incorporate security by design and default.

At the same time, cyber criminals, driven by commercial or political interests, have been intensifying their efforts and honing their capabilities. They are using advanced technologies, many based on AI, to infiltrate the targeted organizations.

Such advances have led to the emergence of what is currently being identified as APTs, that are insidious attacks that often stay below the radar for a long time before being detected.

Cyber security is one of the fastest evolving areas of information technology (IT), both in terms of products and in practice.

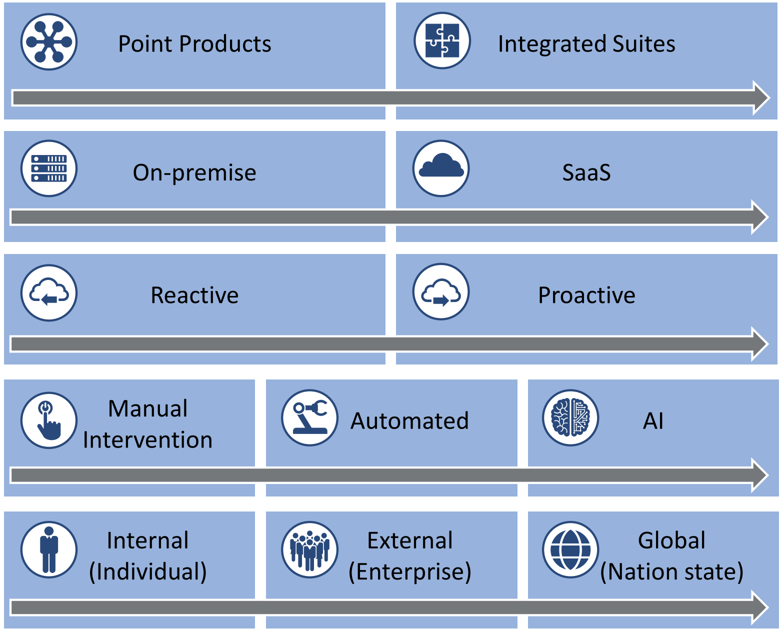
In many ways, the threat landscape can be likened to an arms race, with the attackers and the attacked constantly looking for new ways to achieve their aims/objectives.

> *"We transitioned from an on-premise model to working from home quite seamlessly. COVID-19 has changed the dynamic. People don't have the same controls at home as they have in the office. We have to provide awareness to people."*
>
> *"The controls on the devices need to be enhanced as well. We did a lot of work in areas like endpoint security, data leakage controls, and behavioral analytics to identify any sort of anomalous activity on the network. We really tightened the screw on endpoint computing"*
>
> – CISO Interview

One way to understand this evolution is to look at the cyber security environment in terms of a number of different continuums. These underlying trends explain many of the key dynamics in the market:

Fig 5

Cyber Security Evolution Continuum



Point Products to Integrated Suites. Growing awareness of the importance of cyber security has led to an explosion of products and services from a range of vendors. The high velocity of change means that the market is in a constant state of flux, with the entry of new players and high mergers and acquisition activity. A consistent trend is the move toward integrated cyber security product suites over best-of-breed point solutions.

On-premise to Saas. The growth of cloud computing and Software-as-a-Service (SaaS) has seen the availability of cyber security solutions provided as web-based services, even for organizations that have many on premise applications and processes. All user organizations now live in a hybrid world, where SaaS cyber security is highly relevant.

Reactive to Proactive. Early implementations of cyber security products have primarily been based on detection and then reaction. At present, an increasing number of tools and techniques are aimed at preventing attacks through the use of predictive analytics.

Manual to AI. In recent years, cyber security products and services have made increased use of AI. The growing complexity of the landscape has made manual interventions in solutions increasingly difficult, making the solutions somewhat unmanageable. At the same time, AI which is the technology of choice for many vendor offerings, has become much more sophisticated.

Internal to Global. As the technology has evolved so has the nature of the attackers. Cyber security was initially concerned with the activities of hackers or disgruntled employees, but ubiquitous networking opened the field to an organization's competitors, and to organized crime.

RECENT APT ATTACKS BY NATION STATES

The damage that can be caused by APTs and other attacks can be quite extreme and far reaching. The Centre for Strategic and International Studies (CSIS) tracks cyberattacks on government agencies, defense and high-tech companies, and on economic crimes, with losses of more than a million dollars. Some recent attacks by nation states or criminals associated with them have been listed below:

Fig 6 Recent APT Attacks

Date	Target	Origin	Details
Sept 2020	Govt agencies in NATO countries	Russia	NATO training material as bait for a phishing scheme that infects target computers with malware that creates a persistent backdoor
Sept 2020	US IT, Govt, healthcare, finance, and media companies	Iran	The FBI and CISA announced that Iran-based hackers had been exploiting publicly known vulnerabilities
Sept 2020	US Govt agencies and private companies	China	CISA revealed that hackers associated with the Chinese Ministry of State Security, had been scanning networks for over a year in searching for devices that could be compromised.
August 2020	US and Israel IT, Govt, defense, and healthcare organizations	Iran	Hackers for hire suspected of operating on behalf of the Iranian government were found to have been working to gain access to sensitive information
June 2020	Over 5 million businesses and individuals in Singapore, Japan, USA, South Korea, India and the U.K.	North Korea	State-backed hackers sent COVID-19-themed phishing emails in an attempt to steal personal and financial data.
June 2020	Australia Govt agencies and businesses	China (susp.)	Unnamed state actor targeted a range of organizations with large-scale DDOS attacks
May 2020	US Govt agencies and private companies	Russia	The NSA announced that hackers associated with the Govt intelligence agency GRU had been exploiting a bug that could allow them to take remote control of U.S. servers.
March 2020	Manufacturing, media, healthcare and non-profit organizations	China	Chinese hackers targeted over 75 organizations around the world as a part of a broad-ranging cyber espionage campaign.

Source: Centre for Strategic and International Studies
https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

(A more complete list is contained in the Appendix)

THE ANATOMY OF AN APT ATTACK

In recent years, nation states have emerged as serious players, introducing the concepts of cyber warfare as well as theft of intellectual property. Such attacks, usually aimed at the operations of governments and their agencies, political parties and major corporations, often use many techniques and increasingly take the form of sustained campaigns designed to disrupt, intimidate and interfere.

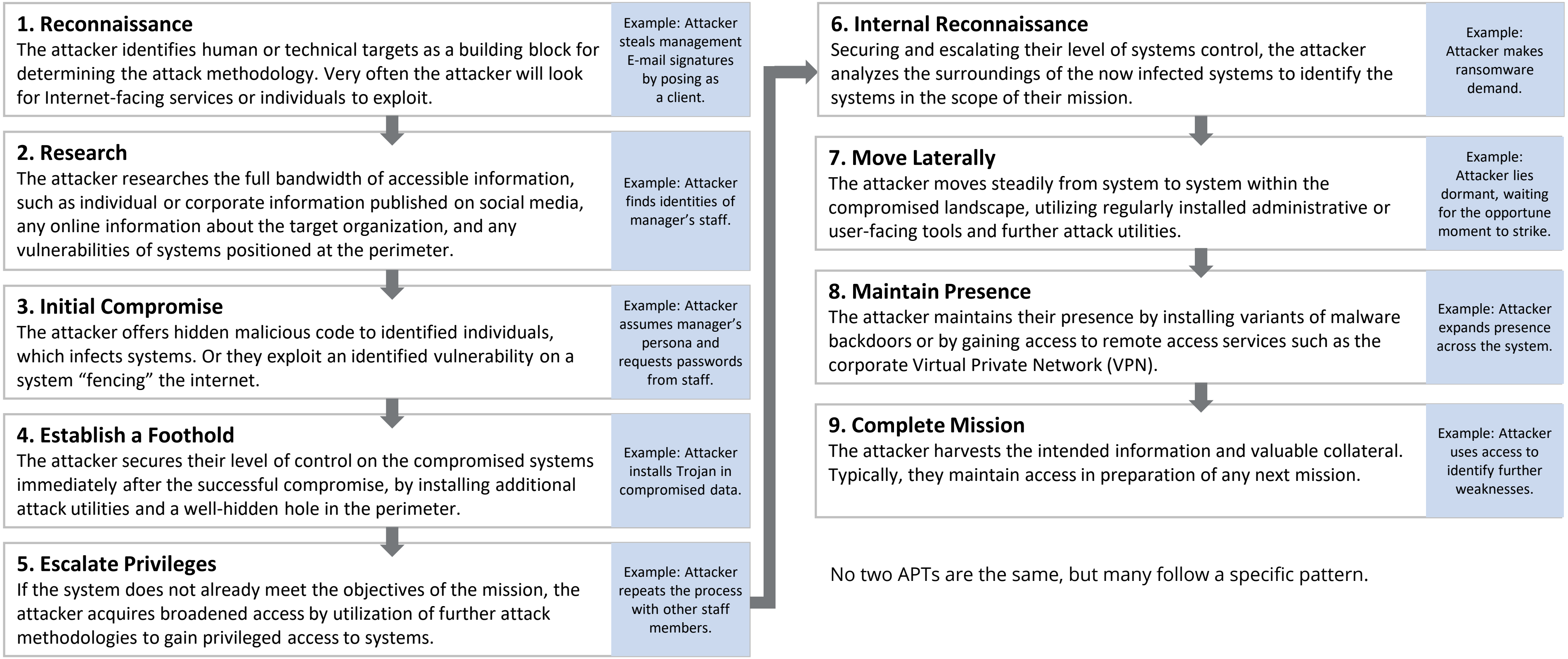
APTs, are cyberattacks that persist over a period of time, and may be countered with the use of Advanced Threat Protection or Advanced Threat Management. As mentioned earlier, APTs are not isolated incidents but sustained campaigns employing many attack types and technologies. They are common occurrences in recent years, garnering substantial publicity, especially as strategies of cyber warfare between nation states, where they take the form of attacks on enterprises primarily by cyber criminals working hand in glove with the perpetrator nation states.

Traditional cyber security tools enabled enterprises to protect the office perimeter. Cyberattacks are now aimed at the weaker elements in the overall corporate security chain. In the post COVID-19 world, employees are identified as the weakest link as an increasing number of them are working remotely, beyond the office perimeters.

In these circumstances, The enforcement of 'security first' corporate culture has become critical. A change in employee behavior patterns is as important as continuous improvements in the existing cyber security architecture in keeping with the recent trends in security services and technologies.

Fig 7

TYPICAL APT ATTACK PROCESS



1. Reconnaissance
The attacker identifies human or technical targets as a building block for determining the attack methodology. Very often the attacker will look for Internet-facing services or individuals to exploit.

Example: Attacker steals management E-mail signatures by posing as a client.

2. Research
The attacker researches the full bandwidth of accessible information, such as individual or corporate information published on social media, any online information about the target organization, and any vulnerabilities of systems positioned at the perimeter.

Example: Attacker finds identities of manager's staff.

3. Initial Compromise
The attacker offers hidden malicious code to identified individuals, which infects systems. Or they exploit an identified vulnerability on a system "fencing" the internet.

Example: Attacker assumes manager's persona and requests passwords from staff.

4. Establish a Foothold
The attacker secures their level of control on the compromised systems immediately after the successful compromise, by installing additional attack utilities and a well-hidden hole in the perimeter.

Example: Attacker installs Trojan in compromised data.

5. Escalate Privileges
If the system does not already meet the objectives of the mission, the attacker acquires broadened access by utilization of further attack methodologies to gain privileged access to systems.

Example: Attacker repeats the process with other staff members.

6. Internal Reconnaissance
Securing and escalating their level of systems control, the attacker analyzes the surroundings of the now infected systems to identify the systems in the scope of their mission.

Example: Attacker makes ransomware demand.

7. Move Laterally
The attacker moves steadily from system to system within the compromised landscape, utilizing regularly installed administrative or user-facing tools and further attack utilities.

Example: Attacker lies dormant, waiting for the opportune moment to strike.

8. Maintain Presence
The attacker maintains their presence by installing variants of malware backdoors or by gaining access to remote access services such as the corporate Virtual Private Network (VPN).

Example: Attacker expands presence across the system.

9. Complete Mission
The attacker harvests the intended information and valuable collateral. Typically, they maintain access in preparation of any next mission.

Example: Attacker uses access to identify further weaknesses.

No two APTs are the same, but many follow a specific pattern.

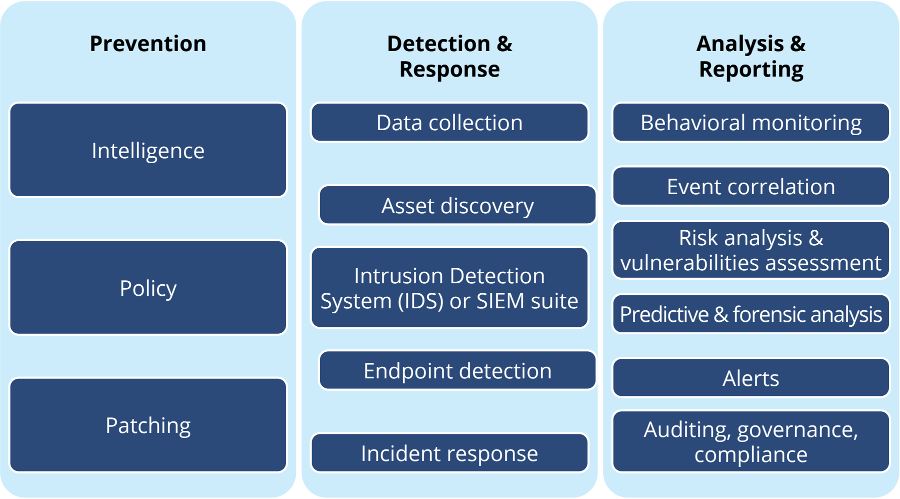
DEALING WITH APTS

A combination of technology and human intervention are deployed in dealing with the wide variety of APTs. These fall into four main categories:

1. Prevention
2. Detection
3. Response
4. Analysis (which includes reporting)

Note: Many taxonomies combine Detection and Response.

Fig 8 Dealing with APTs



Prevention

- Intelligence
- Policy
- Patching

Detection & Response

- Data collection
- Asset discovery
- Intrusion Detection System (IDS) or SIEM suite
- Endpoint detection
- Incident response

Analysis & Reporting

- Behavioral monitoring
- Event correlation
- Risk analysis & vulnerabilities assessment
- Predictive & forensic analysis
- Alerts
- Auditing, governance, compliance

Prevention

Intelligence. The more information available about the threat environment, the better the chances of anticipating threats. There is ample information available about the global threat landscape and an enterprise must develop a comprehensive understanding of the various types of threats and who might carry them out. Enterprises need to gain visibility of potential threats beyond the organization. This knowledge enables them to develop appropriate policies and implement the right procedures and technologies as a safeguard against possible threats.

Policy. As part of the protection against APTs, an organization must ascertain the following:

- Identify the assets they wish to protect
- Define the access rights to those assets
- Decide on the procedures for handling and storing sensitive data
- Determine acceptable use
- Establish password and verification practices
- Select e-mail practices
- Choose the patch procedures
- Prioritize the protection of mobile devices, including USB drives
- Determine appropriate usage of social media by staff
- Define the cyber incident reporting strategy

Patching. Vendors constantly update their software, not just to fix bugs but also to guard against the new security weaknesses. An organization needs a thorough and systemic patch implementation system, across all systems, including all end-user devices. This can include the practice of virtual patching, which protects applications by shielding them from known vulnerabilities.

Detection and response

Data collection. Successful defense is based on data. All information systems generate large volumes of data. These include syslogs; Simple Network Management Protocol (SNMP) traps; perimeter detection systems such as firewalls, applications monitors and hardware monitors; VPNs; and proxy servers. Many tools can be used to gather data from network traffic.

Asset Discovery. An organization cannot protect its assets without knowing the nature of the assets, in terms of what they are and what they do. Many systems and networks contain important hidden elements. Asset discovery identifies devices and software assets, monitors them for problems and helps with patch management.

Intrusion Detection Systems (IDS) or SIEM suite. An IDS is a hardware or software-based monitor, usually employed for a specific part of an organization's system — host processing, internal and external networks and cloud processing. The different technologies and techniques that are used are often collectively referred to as SIEM, and are available as a single integrated suite of tools.

Endpoint detection and response. APTs often use the weaker defenses of end-user devices in the initial attacks. Endpoint detection and response tools monitor all end-user devices and activities and their interaction with the cloud and the host.

Incident response. A standard cyber security incident response methodology is the OODA loop, first developed by U.S. military. OODA stands for Observe (your system and the wider environment), Orient (assess the operational issues and the risks), Decide (prioritize your responses and remediation strategies) and Act (implement your strategy).

Analysis and Reporting

Behavioral monitoring. Unusual activity by system users may be an indicator of a potential security issue. For example, an unexplained increase in traffic by a discrete group of end users might be an indication of intrusion attempts.

Event correlation. Individual events may be significant in themselves. But patterns of events, or a repetition of similar events, may indicate a potential security breach. Real-time data analytics identifies such patterns.

Risk analysis and vulnerabilities assessment. Conventional risk analysis identifies the likelihood and the severity of various factors in an attempt to quantify the degree of risk. Cyber security risk analysis is no different, and involves weighing the likelihood of various attacks by their probable effects and the vulnerabilities of various system components. This is an essential step to developing a cyber security strategy.

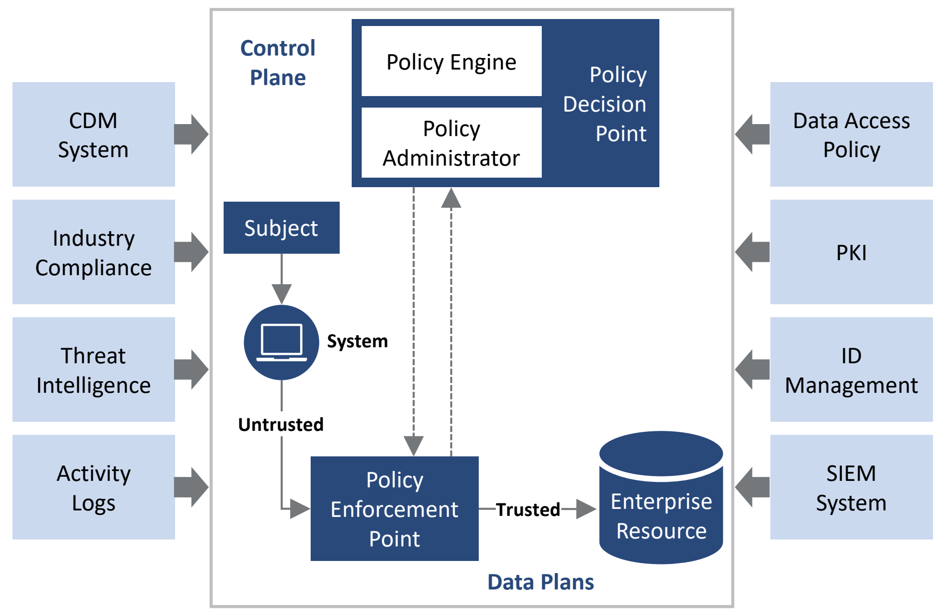
Predictive and forensic analysis. Sophisticated big data analysis tools enable potential security events to be predicted, based on patterns of past behavior. Forensic analysis involves the detailed examination of syslog and other records to determine the causes of data breaches and other events.

Alerts. A good cyber security system should have a comprehensive alert system for reporting potential threats. These can include dashboards for monitoring and summarizing activities and SMS and e-mail alerts.

Auditing, governance and compliance. Data collection and reporting capabilities are essential for auditing system performance. Compliance to certain security standards is increasingly a statutory obligation, with most jurisdictions introducing new compliance and reporting obligations.

Fig 9

Core Zero Trust Logical Components



Source: NIST https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

ZERO TRUST ARCHITECTURE (ZTA)

Ideally, enterprises should maintain a ZTA to fight, or even prevent, a cyberattack and, in particular, APTs. A ZTA, as the name suggests, implies that no component of a corporate network is trusted, and that every access by every component must be verified. This is a very different concept to the traditional paradigm of perimeter security.

With a ZTA, the old concept of 'trust and verify' is replaced with the new concept of 'never trust and always verify'. A ZTA is enabled by the verification of a user's identity at every stage — no user is trusted by default and verification is required at every step. This makes it easier to track any attempt of intrusion. In traditional perimeter based cyber defense systems, it was difficult, or even impossible, to track an intruder's path through the system.

There is no standard method for implementing a ZTA. It could involve many products and services. But, any ZTA is built around three fundamental levels of verification: the verification of the identity of the user, the verification of the user's device and the verification of the user's access privileges. There are various methods for verifying and authenticating user access. These include encryption, behavioral profiling and two-factor or multifactor authentication.

In August 2020, the National Institute of Standards and Technology (NIST), a part of the US Department of Commerce, published a detailed overview of the core logical components that make up a ZTA network strategy as shown in Fig 5.

Goal of ZTA. The goal of a ZTA enabled system, says the report, should be to prevent unauthorized access to data and services, coupled with making the access control enforcement as granular as possible. Authorized users, applications, services or devices can access other components of the network to the exclusion of all other subjects. It makes the point that a ZTA applies equally to physical devices and the network, not just to access data.

ELEMENTS OF A ZTA

NIST definition of ZTA. "Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privelege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprises's cyber security plan that utilizes zero trust concepts and encompasses component relationships, workflow planning and access policies."

NIST identifies the following as the seven basic tenets of a ZTA:

1. **All data sources, computing services and devices** are considered resources, including IoT devices that send data to services within the network. An enterprise may decide to classify personally owned devices as resources if they can access enterprise-owned resources.
2. **All communication** is secured regardless of network location. Network location alone does not imply trust. Access requests from assets located within the network perimeter must meet the same security requirements as access requests and communication from any other external network.
3. **Access to individual enterprise resources** is granted on a per-session basis. Trust in the requester is evaluated before the access is granted. Access should also be granted with the least privileges needed to complete the task.
4. **Access to resources is determined by dynamic policy**—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes. An organization protects resources by defining what resources it has, who its members are (or ability to authenticate users from a federated community), and what access to resources those members need.
5. **The enterprise monitors and measures** the integrity and security posture of all owned and associated assets. No asset is inherently trusted. The enterprise evaluates the security posture of the asset when evaluating a resource request. An enterprise implementing a ZTA should establish a continuous diagnostics and mitigation (CDM) or similar system to monitor the state of devices and applications and should apply patches/fixes as needed.
6. **All resource authentication and authorization** are dynamic and strictly enforced before access is allowed. This is a constant cycle of obtaining access, scanning and assessing threats, adapting, and continually re-evaluating trust in ongoing communication.
7. **The enterprise collects as much information** as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. An enterprise should collect data about asset security posture, network traffic and access requests, process that data, and use any insight gained to improve policy creation and enforcement.

Source: NIST https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

ZTA AND ITS BENEFITS

ZTA concept

The concept of ZTA has evolved as traditional network security systems have been challenged by new cloud-based networking paradigms. A ZTA was once regarded as an unaffordable luxury. In the current cyber security landscape, it has become a necessity.

A ZTA has many advantages over the traditional perimeter security model, and the benefits go beyond improved cyber security. These include:

Improved asset discovery

Asset discovery is a necessary pre-condition to implementing a ZTA. Each device, resource and process needs to be identified and classified. This improves network visibility, making intrusion detection easier and response more effective.

Protection through micro-segmentation

A ZTA shifts emphasis from the perimeter of the network to the individual devices and services within the perimeter, each with its own access control. This practice is known as micro-segmentation. The creation of secure zones within the processing ecosystem enables processes and network components to be isolated from one another, ensuring that any security compromise can be localized.

Incident detection and resolution

The advantage of micro-segmentation is not limited to security; as discrete processes and assets are isolated from each other, performance issues can be easily identified and addressed.

Effective implementation through SASE

With the increasing adoption of SaaS applications and many more remote users, the increase in traffic within corporate networks, and the increasing use of the public cloud the earlier approaches to network security have been rendered untenable.

Many security providers have adopted the new concept of Secure Access Service Edge (SASE), that incorporates traditional wide area network (WAN) security with cloud-based services such as Cloud Access Security Brokers (CASBs) and other SaaS delivered security services, applying ZTA concepts and practices across an enterprise's entire ecosystem.

Aid to compliance

Inherent in the implementation of a ZTA is the compartmentalization of a corporate information ecosystem. This makes governance and compliance easier, and ultimately more cost-effective.

Facilitator of digital transformation

Digital transformation (DX) for an organization can be a difficult process. A ZTA makes it easier to adopt a building block approach to DX, making the transformation of business processes discrete and manageable.

Fig 10

CHECKLIST OF RECOMMENDED ACTIONS

Develop a comprehensive cyber action plan
If you do not already have one, you need to develop a cyber security action plan appropriate for your organization. You may wish to do this yourself, or you may wish to work with a cyber security services provider. There is no one size fits all approach, but you need to ensure that your plan takes into account all the relevant aspects of your situation.

Develop and maintain practical cyber defence policies
The first point on your action plan should be to develop an organization-wide cyber security policy covering all aspects of your operations, from staff awareness to prevention to detection through to remediation and reporting. The policy should be a living document, updated regularly to take into account the changing cyber security environment. It should inform everything you do.

Ensure your staff develop a cyber security mindset and culture
The human element is the most important part of cyber security, particularly in the mid-COVID-19 era characterized by many endpoints and extremely distributed networks. You need to keep your staff informed, aware and trained in the appropriate cyber security measures. You need to develop a cyber security culture.

Ensure you are fully informed of the cyber threat landscape
The world of cyber security is complex and is constantly evolving. You have responsibility to keep ahead of the developments so that you are able to plan for all types of threat as they develop. This is not a one-off project but is a continuous process.

Use virtual patching to shield against vulnerabilities
It is important to implement software patches as quickly as possible, but patch management can be a time-consuming process and can affect business continuity. The solution is virtual patching, a method of protecting applications by shielding them from known vulnerabilities.

Collect data from as many sources as possible
Successful cyber defense is based on data. All information systems generate a vast amount of data from a variety of sources. Use them all. Asset discovery is an important part of this process. Remember that all your data sources, services and devices are assets you need to protect. Refer to the NIST guidelines.

Ensure your Intrusion Prevention Systems are evolving to meet new threats
There are many potential intrusions to detect. Ensure your IDS tools are up-to-date and comprehensive. Endpoint detection is of particular importance. Remember the OODA loop: Observe, Orient, Decide, and Act.

Conduct contextual monitoring
Unusual user behavior and other out-of-context activity can be monitored and analyzed. There is a large range of analytical tools now available – make use of them.

Carry out thorough risk analysis and vulnerabilities assessment
Use your knowledge and your data to analyze your risks and vulnerabilities. This should be a continuous feedback loop with your policies and practices.

Conduct cyber security drills and red team/blue team simulation
Practice makes perfect. You should run drills to test your cyber security procedures and level of readiness. "War gaming" using red teams (attackers) and blue team (defenders) can be very effective in building practical skills.

Make thorough use of AI and ML based analytical tools
Don't just analyze past data for behavioral patterns and the like. Take it a step further with predictive analysis, using artificial intelligence and machine learning. Conduct a thorough forensic analyses of past incidents and activities.

Ensure your alerts, reporting, and metrics are first rate
You need a rigorous system of alerts so the right people are informed about and can act on any breach as soon as possible. This needs to be accompanied by systematic and comprehensive reporting. Build a cyber scorecard to ensure the effectiveness of your capabilities.

Maintain high governance and compliance standards
Develop and maintain the highest standards of information governance to ensure that your policies and procedures are followed and that your cyber security systems are operating at peak efficiency. Good governance also means high standards of audit and compliance. and conformance to statutory and regulatory requirements.

Automate your incident response capabilities
Many Automated Incident Response tools now exist. They trigger a range of actions when an intrusion is detected. These replace many manual processes and can significantly mitigate the immediate effects of a cyber attack.

Choose the right partner
You cannot do cyber security on your own. You need to find the most appropriate services provider – or providers – to complement your abilities. In most cases they will maintain a Security Operations Center (SOC) and work with you on implementing suitable products and services.

CONCLUSION – NEXTGEN CYBER SECURITY

- **The COVID-19 pandemic has increased APT attacks significantly.** The cyber security landscape has changed forever. The increase in number of employees working remotely has led to a significant number of endpoints in corporate networks.
- **Effective defense against state sponsored or sophisticated criminal** APTs requires cyber security practitioners with the skills and resources to defend corporate and even national infrastructure. This means upskilling the resources, and also establishing security as a core value throughout the workforce.
- **A ZTA has replaced the old concept of 'trust and verify'** with the new concept of 'never trust and always verify'. Once regarded as a luxury, a ZTA is increasingly becoming a necessity as an increasing number of security professionals recognizing it as the most appropriate option of dealing with APTs and other evolving cyber security threats.
- **The advantages of a ZTA go well beyond improved cyber security** — the nature of a ZTA that isolates system components from each other also enables digital transformation, compliance and good governance, and the effective management of distributed networks.
- **A ZTA can transform an organization's information infrastructure.** Its effective implementation requires the automation of many processes. It also enforces the implementation of policies and procedures that positively impact many aspects of an enterprise's operations.
- **As an increasing amount of processing is conducted in the cloud,** corporate networks are faced with the reality of a large, distributed workforce, and with this the concept of protecting the perimeter as a cyber security defence mechanism has become obsolete. A ZTA ensures security throughout the extended network.
- **Cyber security has moved to the next generation,** and so have those perpetrating cyberattacks. Fortunately, tools and techniques exist to enable organizations to move to this level. The landscape continues to evolve. Welcome to NextGen cyber security!

Welcome to the next generation of cyber security!!

> *"You need a strong partnership with a good security supplier. Some are too small to do it properly, but some are just too big to give you personalized service. You need someone who has the core competencies and who can also push the boundaries. And in our case they needed to be technology agnostic.*
>
> *You have to start with documenting your environment and what you want to do. Draw up a comprehensive RFP, but don't send it to too many suppliers. Spend time upfront finding out who can help you on your journey by doing some research, then go to three or four suppliers. You don't have time to look through 20 of them."*
>
> – CISO Interview

TECH MAHINDRA SPONSOR PERSPECTIVE

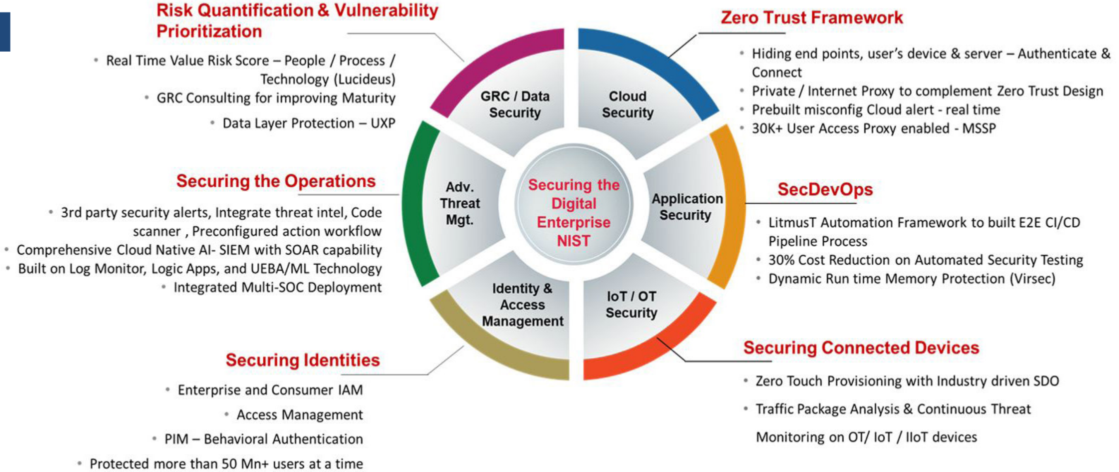
Securing Enterprises from NextGen Cyber Attacks

Cyber security threats and issues, further heightened during the pandemic, have taken precedence over many corporate and national security developments. There is a shift towards next generation safeguarding of the enterprise, from a basic NextGen firewall structure to AI-based cyber defense.Tech Mahindra recommends three goals:

Early Detection | Resilience Response | Efficient Redesign

Tech Mahindra's Enterprise Security and Risk Management (ESRM) capabilities enable its clients to mitigate threats by empowering security consultants and analysts with artificial intelligence platforms. Tech Mahindra offers cyber defense services in partnership with AT&T that ensure:

- **11%** increase in the productivity of SOC operations
- **80%** reduction in threat detection and response time
- **34%** reduction in risk of breach benefits
- **94%** reduction in compliance reporting efforts
- **7%** increase in savings with OTX threat Intelligence
- **6000 hours** of time savings each year with respect to compliance reporting
- **Less than three months** of reduced payback time
- **6X** times ROI guaranteed



Risk Quantification & Vulnerability Prioritization

- Real Time Value Risk Score – People / Process / Technology (Lucideus)
- GRC Consulting for improving Maturity
- Data Layer Protection – UXP

Zero Trust Framework

- Hiding end points, user's device & server – Authenticate & Connect
- Private / Internet Proxy to complement Zero Trust Design
- Prebuilt misconfig Cloud alert - real time
- 30K+ User Access Proxy enabled - MSSP

Securing the Operations

- 3rd party security alerts, Integrate threat intel, Code scanner , Preconfigured action workflow
- Comprehensive Cloud Native AI- SIEM with SOAR capability
- Built on Log Monitor, Logic Apps, and UEBA/ML Technology
- Integrated Multi-SOC Deployment

SecDevOps

- LitmusT Automation Framework to built E2E CI/CD Pipeline Process
- 30% Cost Reduction on Automated Security Testing
- Dynamic Run time Memory Protection (Virsec)

Securing Identities

- Enterprise and Consumer IAM
- Access Management
- PIM – Behavioral Authentication
- Protected more than 50 Mn+ users at a time

Securing Connected Devices

- Zero Touch Provisioning with Industry driven SDO
- Traffic Package Analysis & Continuous Threat Monitoring on OT/ IoT / IIoT devices

Empowered through a custom dashboard to assess the details of people, process and technology across the enterprise, Tech Mahindra's Cyber Defence Service integrates all elements with an AI-based cyber defense platform, thereby enabling clients with early intrusion detection, trend identification, external and internal threat intelligence followed by automated risk mitigation. We cater to each aspect of enterprise security – IT infrastructure, applications, connected devices, networks or transforming entire enterprises.

Having in-house Zero Trust and SASE implementation capabilities, we provide 360-degree protection to every enterprise. With a focus on addressing next-generation challenges and evolving attacks, we at Tech Mahindra are co-innovating with our clients as well as investing in strengthening future capabilities for redesigning and long-term resiliency. To find out more, please visit www.techmahindra.com/en-in/techmnxt/techbets/cyber-security/

APPENDIX - RECENT APT ATTACKS BY NATIONS STATES

- **October 2020:** The UN shipping agency, the International Maritime Organization (IMO), reported that its website and networks had been disrupted by a sophisticated cyberattack.
- **September 2020:** U.S.-based healthcare firm, Universal Health Systems, faced a ransomware attack that caused affected hospitals to revert to manual backups, divert ambulances and reschedule surgeries.
- **September 2020:** Russia-based hackers targeted government agencies in NATO member countries and nations that cooperate with NATO. The campaign used NATO training material as bait for a phishing scheme that infected target computers with malware to create a persistent backdoor.
- **September 2020:** Three hackers operating under the direction of Iran's Islamic Revolutionary Guard Corps were indicted by the U.S. for attacks against workers at aerospace and satellite technology companies, as well as international government organizations.
- **September 2020:** The US Department of Justice indicted five hackers from China with ties to China-based intelligence services for attacks on more than 100 organizations across government, IT, social media, academia, and other sectors.
- **September 2020:** The FBI and CISA announced that Iran-based hackers had been exploiting publicly known vulnerabilities to target U.S.-based organizations in the IT, Government, Healthcare, Finance, and Media sectors.
- **September 2020:** The CISA revealed that hackers associated with the Ministry of State Security, China had been scanning U.S. government and private networks for over a year in search of networking devices that could be compromised, using exploits for recently discovered vulnerabilities.
- **August 2020:** A North Korea- based hacking group targeted 28 UN officials in a spear-phishing campaign, including at least 11 individuals representing six members of the UN Security Council.
- **August 2020:** Hackers for hire, suspected of operating on behalf of the Government of Iran were found to have been working to gain access to sensitive information held by North American and Israeli entities across a range of sectors, including Technology, Government, Defense and Healthcare.
- **August 2020:** New Zealand's stock exchange faced several days of disruptions after a severe distributed denial of service (DDOS) attack was launched by unknown actors.
- **August 2020:** U.S. officials announced that hackers with the government of North Korea had been running a campaign focused on stealing money from ATMs around the world.
- **August 2020:** A China-based cyber espionage group targeted military and financial organizations across Eastern Europe.
- **August 2020:** The Defense Ministry of Israel announced that it had successfully defended against a cyberattack on Israel-based defense manufacturers; the attack was suspected to have been launched by a North Korea-based hacking group.
- **August 2020:** Russia-based hackers compromised news sites and replaced legitimate articles with falsified posts that used fabricated quotes from military and political officials to discredit NATO among Polish, Lithuanian, and Latvian audiences.
- **July 2020:** Chinese state-sponsored hackers broke into the networks of the Vatican to conduct espionage in the lead-up to negotiations about control over the appointment of bishops and the status of churches in China.
- **July 2020:** Canada, the U.K., and the U.S. announced that hackers associated with the intelligence in Russia had attempted to steal information related to COVID-19 vaccine development.

- **June 2020:** North Korea state hackers sent COVID-19-themed phishing emails to more than five million businesses and individuals in Singapore, Japan, the U.S., South Korea, India, and the U.K. in an attempt to steal personal and financial data.
- **June 2020:** The Prime Minister of Australia announced that an unnamed state actor had been targeting businesses and government agencies in Australia as part of a large-scale cyberattack.
- **May 2020:** Businesses in Japan, Italy, Germany, and the U.K. that supply equipment and software to industrial firms were attacked in a targeted and highly sophisticated campaign by an unknown group of hackers.
- **May 2020:** The NSA announced that Russia-based hackers associated with the government intelligence agency, GRU, had been exploiting a bug that could allow them to take remote control of U.S. servers.
- **May 2020:** Cyber criminals managed to siphon US$10 million from Norway's state investment fund in a business e-mail compromise scam that tricked an employee into transferring money into an account controlled by the hackers.
- **May 2020:** Iran-based hackers conducted a cyber espionage campaign targeting air transportation and government actors in Kuwait and Saudi Arabia.
- **May 2020:** China-based hackers accessed the travel records of nine million customers of U.K.-based airline group, EasyJet.
- **May 2020:** U.S. officials accused hackers linked to the Government of China of attempting to steal U.S. research into a coronavirus vaccine.
- **May 2020:** Suspected China-based hackers conducted a phishing campaign to compromise Vietnamese government officials involved in ongoing territorial disputes with China in the South China Sea.
- **May 2020:** Japan's Defense Ministry announced that it was investigating a large-scale cyberattack against Mitsubishi Electric that could have compromised details of new state-of-the-art missile designs.
- **May 2020:** A suspected PLA hacking group targeted government-owned companies, foreign affairs ministries, and science and technology ministries across Australia, Indonesia, the Philippines, Vietnam, Thailand, Myanmar and Brunei.
- **April 2020:** Suspected Vietnamese government hackers used malicious apps uploaded to the Google Play app store to infect users in South and Southeast Asia with spyware capable of monitoring the target's call logs, geolocation data and text messages.
- **April 2020:** Poland suggested that the Government of Russia was behind a series of cyberattacks on Poland's War Studies University; the attacks were meant to advance a disinformation campaign, undermining U.S.-Polish relations.
- **April 2020:** Suspected Iran-based hackers unsuccessfully targeted the command and control systems of water treatment plants, pumping stations and sewage in Israel.
- **April 2020:** U.S. officials reported seeing a surge of attacks by China-based hackers against healthcare providers, pharmaceutical manufacturers, and the U.S. Department of Health and Human services amidst the COVID-19 pandemic.
- **April 2020:** A Russia hacking group used forged diplomatic cables and planted articles on social media to undermine the governments of Estonia and the Republic of Georgia.
- **April 2020:** Iran-government-backed hackers attempted to break into the accounts of WHO staffers in the midst of the COVID-19 pandemic.
- **March 2020:** North Korea-based hackers targeted individuals involved with North Korean refugee issues as part of a cyber espionage campaign.
- **March 2020:** China-based hackers targeted over 75 organizations around the world in the Manufacturing, Media, Healthcare, and Non-profit sectors as a part of a broad-ranging cyber espionage campaign.

Source: Centre for Strategic and International Studies

https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

Author and Editor

Craig Baty, Author

Distinguished Lead Analyst at ISG

Craig Baty has extensive C-level executive, and research and advisory experience in global ICT markets. Craig is Principal and Founder of DataDriven an Asia/Pacific based global research and advisory firm. Craig has over 35 years of executive and board level experience in the ICT industry, including as a Group VP and Head of Gartner Research AP/J, CEO of Gartner Japan, Global VP Frost & Sullivan, and more recently as VP Global Strategy and VP Digital Services in Fujitsu Tokyo HQ. As a well know ICT commentator and analyst, Craig has written more than 200 research pieces, and presented at over 1500 events globally. He is also regularly quoted in regional media. Craig is actively involved in the ICT community as a board member of the Australian Information Industry Association (AIIA) and Vice Chair of the Australian Computer Society NSW (ACS), and National Council for Cybersecurity and Digital Trade.

Jan Erik Aase, Editor

Partner, Principal Analyst and Global Head – ISG Provider Lens/ISG Research

Jan Erik Aase brings extensive experience in the implementation and research of service integration and management of both IT and business processes. With over 35 years of experience, he is highly skilled at analyzing vendor governance trends and methodologies, identifying inefficiencies in current processes, and advising the industry. Jan Erik has experience on all four sides of the sourcing and vendor governance lifecycle - as a client, an industry analyst, a service provider and an advisor. Now as a research director, principal analyst and global head of ISG Provider Lens™, he is very well positioned to assess and report on the state of the industry and make recommendations for both enterprises and service provider clients.

ISG Insights | Advanced Persistent Threats

January 2021

Proprietary and Confidential

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.