ZERO DAY ATTACKS

Micro.ai™

Asset-Centric Zero-Day Attack Protection

It is estimated that there are ~ 1.2 million new IoT devices and machines being activated every day. This explosion of devices and endpoints has significantly increased the cyber risk to business-critical assets around the globe. Zero-day attacks are increasingly sophisticated and destructive. A new approach to IoT asset security is needed.

- **Data:** Intellectual property, PII
- **Network Infrastructure:** DMZ, Servers
- **Endpoints:** IoT

Security is a critical piece of any business, and an ongoing concern, but find any CISO, CSO or CEO who is “at ease” about security in their environment because it is a moving target and there will always be new vulnerabilities. Skilled and stealthy hackers are constantly finding ways to infiltrate a network or device to compromise a business, steal data, and reap the financial benefits. Some even do it for fun. In either case, a security attack on a business costs money, reputation, value proposition, competitive advantage, and in some cases, the business.

Some of the biggest hacks and attacks, include the Petya malware virus that has been responsible for several attacks occurring in the Ukraine. NotPetya, in 2017 also targeted the Ukraine and was successful in that it took out the electric grid, stopping public transportation dependent on electricity, bank ATMs, rendering the country helpless. NotPetya didn’t only affect Ukraine, but global shipping company lost $300 million due to its entire network taken out with more recent estimates that this attack caused $10 billion in damage.

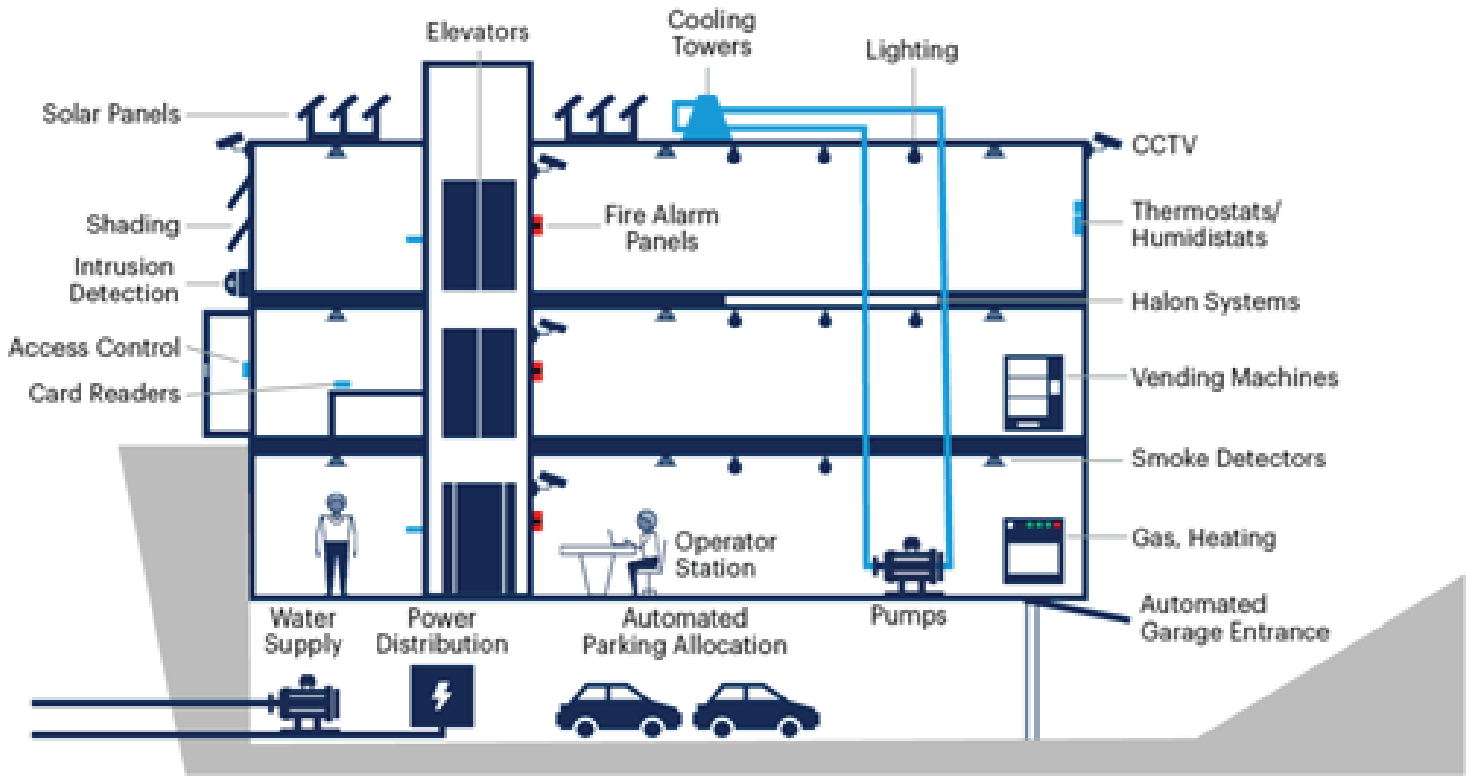
Hackers have not necessarily become more sophisticated. In fact, in 2021 they are using old techniques, targeting old systems, and through common mistakes made by individuals and businesses. To stop this from happening requires a combination of tactics, training, and technology. The Petya virus targeted old windows technology, so making sure software updates are conducted regularly is key. Stuxnet, a dangerous malware, while considered sophisticated attacked the uranium enrichment facility, Natanz in Iran. The facility, Natanz, was not connected to the internet, so the attackers used infected USBs to infiltrate the system and impose damage on the industrial control system. Stuxnet also has the potential to kill millions of people.

As “smart” grows (smart office, home, etc.) most automation systems are vulnerable to attacks as the automation systems are built on common Operation Systems Windows and/or Linux. Hackers have been using a combination of old and new methods, however, mainly old. For example, something as simple as the Shodan search engine that searches for devices connected to the internet as well as details of devices with great granularity leaving them extremely vulnerable to exploitation. This could mean anything from medical devices such as insulin pumps to robotic or mechanical devices in a factory.

In a smart building each component or “thing” is connected to the IT/OT system, but operate individually meaning, it can be compromised as an individual component because it is connected to the internet and not just from a hacker getting in at the IT/OT level.

HACKERS STILL USE OLD TECHNIQUES. COMMON MISTAKES BY INDIVIDUALS AND BUSINESSES ARE THE LOW HANGING FRUIT FOR BAD ACTORS

Components of a Smart Building

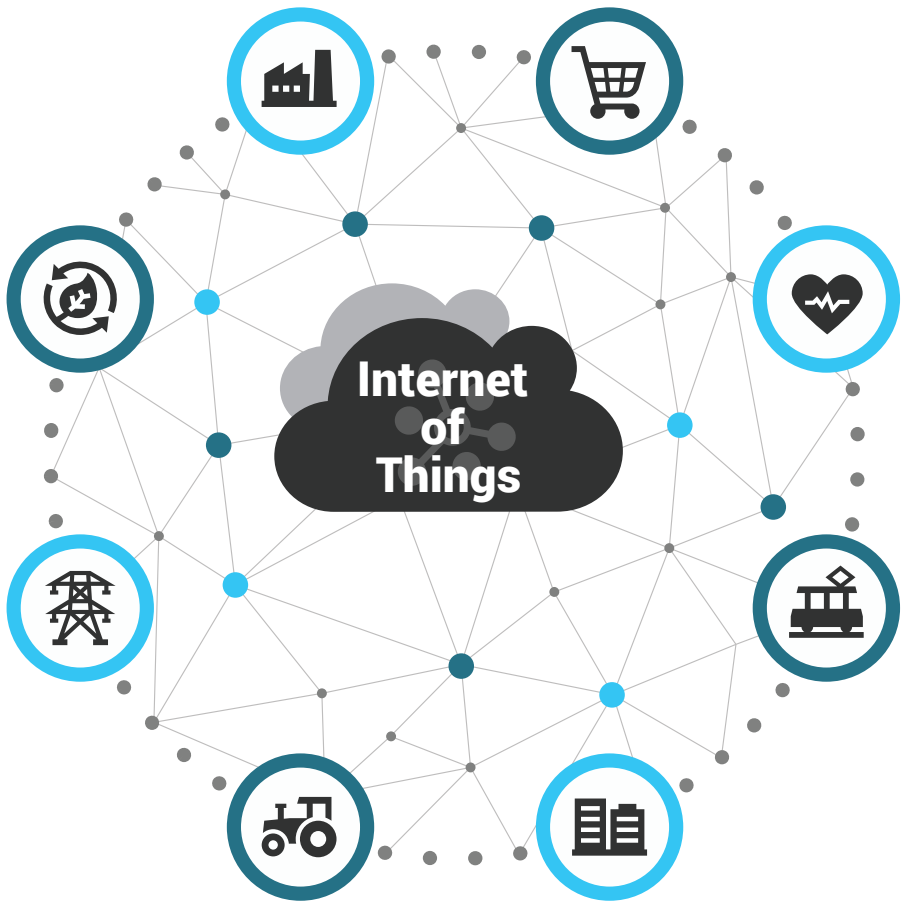


Source: Gartner

Growth in IoT Endpoints Exacerbates the Problem

The number of connected devices to the internet is growing. More and more things are getting connected beyond just devices – even animals. According to a Frost and Sullivan report, in 2019, there were more than 24.37 billion IoT devices in service and that by 2026, there will be approximately 66.82 billion IoT devices in service representing roughly 8 connected IoT devices per human being.

According to the Global Cyberattack Trends report by SonicWall, North America saw the biggest soar in IoT malware cases in 2020. In a year, IoT malware attacks leaped by an alarming 152%.



“Malware attacks on IoT devices spiked by 66% in 2020 compared to 2019.”

- SonicWall

They expand the attack surface and businesses are challenged to track, update, or maintain the security of them. According to a Ponemon survey in 2020, 68% of organizations experienced one or more successful endpoint attacks in 2019 and that by early 2020, around 80% of successful network breaches fell into the Zero Day category. In addition, Trend Micro’s Zero Day Initiative, in 2018 discovered nearly 400 new vulnerabilities, up from 49 in 2017, and predicted that a new Zero Day attack will be discovered every day by the end of 2021.

The Threat Landscape

Attacks and hacks present in a variety of form factors. Every day organizations are faced with attack types and through a combination of strategy, policy and investments in software tools aiming to help combat against them. Some of the most common attack types to create a Zero Day Attack (see Table 1) and characteristics thereof, have been happening for years with some notable success and costly outcomes.

Common Attacks and Threats	Overview
DDoS Attacks	▶ Hackers penetrates network and shuts down vital resources, machines, or systems ▶ Victim originates from many different sources ▶ Attackers overwhelm the victim using hundreds and thousands of devices infected with malicious code creating a "botnet"
Malware	▶ Blocks access to key components of the network (ransomware) ▶ Malware or additional harmful software installed through phishing or opening email ▶ Covertly obtains information by transmitting data from the hard drive (spyware) ▶ Disrupts certain components and renders the system inoperable
Phishing	▶ Confidential information is obtained and used to access sensitive data ▶ Victim is "tricked" into clicking links allowing hacker access
Insiders	▶ Associate with harmful intent leverages access privileges to obtain documents or plant malicious software ▶ Negligence due to wilful ignoring of policy ▶ Inadvertent loss through careless users or falling victim to phishing attack causing accidental breach
Cloud Breach	▶ Hackers successfully breaches cloud infrastructure to obtain sensitive information
Man-in-the-Middle Attack	▶ Enters through unsecure public Wi-Fi install malware onto victim's device ▶ Attacker (once inside) can install software that steals victim's information

While it is not particularly good to be a victim of any of them, many – to some extent – can be identified and potentially stopped in their tracks, with hopeful learning lessons toward prevention, but there are still no guarantees.

Denial of Service/Distributed Denial of Service

Denial of Service/Distributed Denial of Service (DoS/DDoS) attacks, a major disruption and will bring any business to a screeching halt when successful. It starts with malware infected devices, or “bots” which can quickly become a group of bots, also known as a “botnet”. They happen using the following methods; by volume, at the application layer or as a protocol attack. Attackers, are often successful using all three methods spreading the bots and botnets across multiple assets in turn overpowering network defenses increasing the difficulty in stopping the attack. DDoS attack are typically combatted through firewalls, VPN, anti-spam, content filtering solutions.

Malware

Malware, or malicious software, is a very common attack method, comes in a variety of form factors, and has made headlines often. It includes spyware, ransomware, viruses and worms. Each type of malware can be delivered to create a Zero Day Attack which makes this a very compelling threat with extreme consequences in terms of individual and business reputations, financial loss (through litigation, regulatory fines and fees, the ransomware price), reduced credibility, loss of competitive advantage (intellectual property (IP) theft), loss of trust, and can limit business growth. In some cases, everyday life can be affected. A recent example of a malware attack is the Colonial Pipeline in May of 2021, where nearly the entire east coast of the United States experienced a gas shortage due to a ransomware attack. Ransomware attacks are usually combatted through antivirus software.

Phishing

Phishing is all too common, happens on a daily basis, and has enjoyed quite a bit of success in terms of an entry point. These are designed to trick a user into clicking a link on what looks like a legitimate email sending them to a fake website and automatically infecting the machine with a virus. It requires a combination of adopting companywide two-factor or multi-factor authentication, secure email gateways, anti-spam, and end user security awareness training so they can identify what a phishing email looks like, what to look for in an email. At a time where individuals are experiencing high productivity, phishing preys on individuals who are extremely busy with short attention spans.

Insider Threats

Insider threats are also very common and any business can be subject to data loss or theft by employees. Overall, there are three types of insider threats; malicious insiders such as a disgruntled employee/ex-employee wishing to inflict harm on a business, insiders who circumvent or intentionally ignore policy (sometimes just to get their job done), use personal email to transport sensitive information, don't encrypt files or folders leaving sensitive data on the table for bad outside actors to obtain, and truly accidental data loss by victims of a phishing attack. Insider threats can be mitigated through use of data loss prevention (DLP), enterprise digital rights management (EDRM), and user <and entity> behavior analytics (UBA/UEBA) tools.

Cloud Breaches

Cloud breaches are just another way bad actors gain access to sensitive data and are long debated as to whose responsibility it is to protect said data, the cloud provider or the enterprise. Either way, cloud breaches usually occur because of a configuration error or through stolen credentials (e.g. phishing attack or poor password management) therefore, attackers exploit errors or vulnerabilities without using malware. Essentially, they land and expand, their access across weakly configured or protected interfaces to locate valuable data, then store the data at their own location. Common tools to mitigate cloud breaches include cloud access security brokers (CASBs), cloud security posture management (CSPM), and cloud workload protection platforms (CWPPs).

Man-in-the-Middle Attacks (MitM)

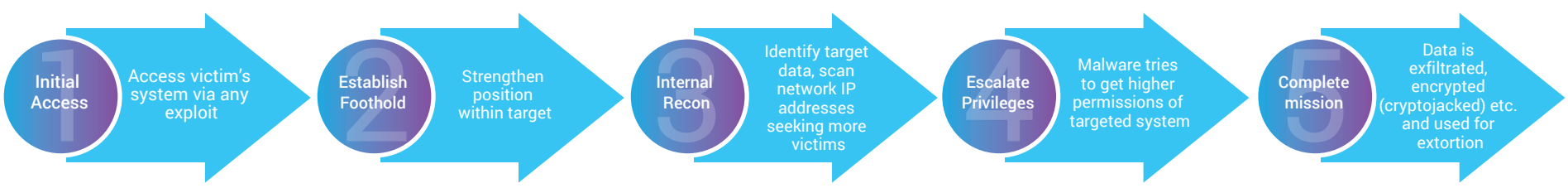
MITM attacks are also known as "eavesdropping" attacks and can be used to steal data. They don't tend to get as much publicity as Malware, Phishing or bugs such as Heartbleed, but they can be just as damaging. They typically happen through unsecure public Wi-Fi and directly onto a user's device. But they can happen on websites and across social networks. A MitM attack can expose a multitude of information including email addresses, passwords, and read and sent messages between parties. Attackers can also impersonate a user or edit a social media profile for malicious use such as catfishing. Common tools used to mitigate MitM attacks include use of virtual private network (VPN) tunnels, an intrusion detection system (IDS), security awareness training, and antivirus software.

Zero-Day Attacks

The Zero-day attack. The king of the unknown because it is just that - unknown. About the same as not being aware that the door lock on your house is broken, you would have no way of preventing a burglar from breaking in. A zero-day attack can come to any enterprise in any form, from phishing to malware because they based on software flaws and vulnerabilities detected by the attacker. Security teams being unaware of the flaw or vulnerability, means that they have zero days to fix the weakness before an attack occurs. Even more alarming, it can take days, weeks, or months for users or security teams to detect.

Zero-day attacks are on the rise, largely due to the growth in remote workforces where employees do not have the same protection as they would in the office. The increase in smart home technology with connected doorbells, smart appliances, and televisions sharing the same network makes them particularly vulnerable. The supply chain for zero-day attacks is interesting in that the finder of a network vulnerability will often sell that information to the tactile hacker, for example, in early 2020, a Zoom vulnerability sold for $500K. Combatting against zero-day attacks are time consuming and require frequent software patches and constant upgrading.

Five Stages of a Zero-Day Attack

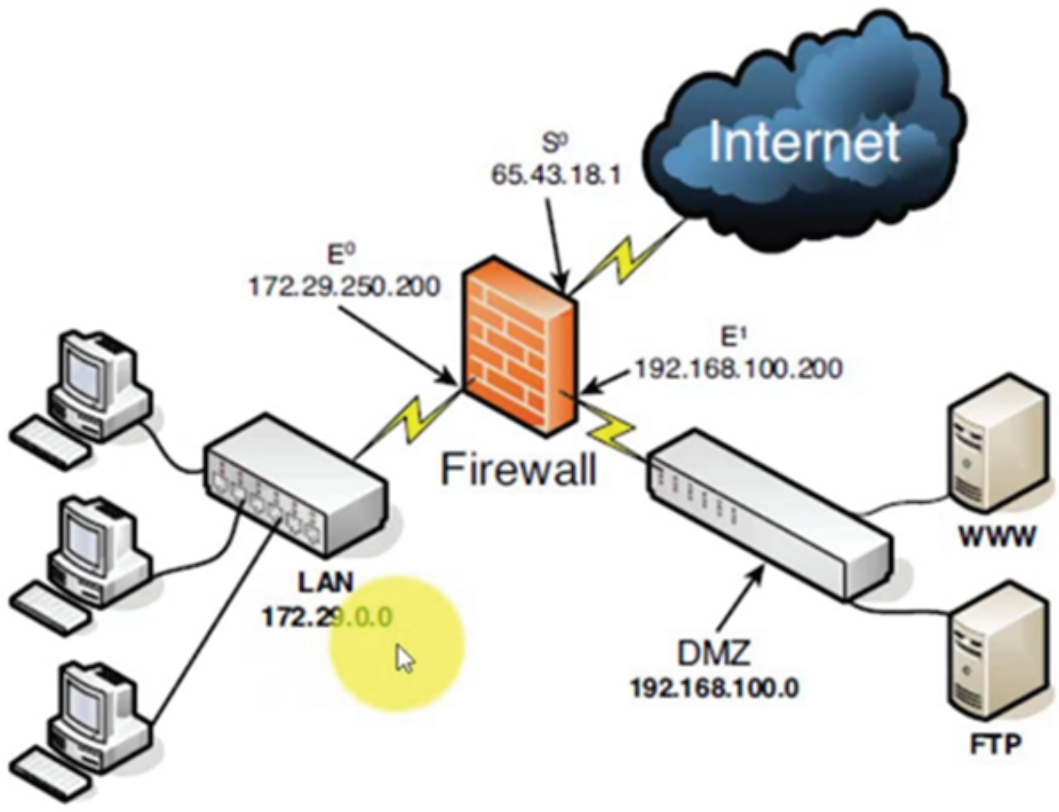


As flaws or vulnerabilities are discovered by the attacker, they will deliver a variety of common attack types to create the Zero Day.

Fighting the Good Fight

Organizations build security architectures to protect their assets, close common weaknesses, and reduce risk of cybercrime from common and Zero Day attacks through have logical and physical security architecture. Each layer, Operations, Identity and Access Control, Data, Hosts, and Network include components and software designed to satisfy a particular function, for example, a firewall inside the Demilitarized Zone (DMZ) monitors and controls incoming and outgoing traffic and acts as the barrier between the trusted and untrusted networks.

Common Security Architecture



Demilitarized Zone

The DMZ is the interface to the untrusted external network (the internet), aiming to keep the internal corporate network isolated. The area where the most vulnerable attack targets such as e-mail, web and domain name system (DNS) and even VoIP servers reside and protected by a firewall (both inside and outside) that filters traffic between the DMZ and the external network and between the DMZ and the local area or private network (LAN). The DMZ is designed to allow access to untrusted network resources while securing the private network.

Mitigating threats against a business also include encryption, use of passwords and password management, and a host of other tools such as those mentioned above (DLP, Antivirus, CASBs IDS etc.), and each have evolved to provide stronger security capabilities. This is particularly necessary as devices themselves expanded in capability such as becoming application rich, more mobile, move visible, and ultimately more vulnerable. Some techniques enjoy a certain level of success but there is no one size fits all when it comes to security.

Passwords and Password Management

A common problem across multiple organizations is poor password management. Between end users using simple and common passwords to security teams not changing a password on network elements such as routers and gateways. In fact, many studies have revealed that most people don’t use passphrases, or a series of special characters, numbers, and letters. Rather they keep default passwords, or use simple, easy to guess passwords (see Table 2).

	10 Most Common Passwords
1	123456
2	123456789
3	qwerty
4	password
5	12345
6	qwerty124
7	1q2w3e
8	12345678
9	111111
10	1234567890

Most organizations suffer from poor password hygiene.
It is a major open highway into the entire organization.

Zero Trust Network Access (ZTNA)

Zero Trust Network Architecture (ZTNA) is an IT security model that provides secure remote access to an organization's network, applications, data, and services based on clearly defined access control policies. It works by allowing access to specific applications or network resources only after the user has been authenticated to the network and requires ongoing or frequent authentication to applications and other resources within the organization. While the endpoint initiated ZTNA authenticates access to applications from an endpoint connected devices, it does not monitor and alert to the health of a compromised device nor does it prevent a device from being compromised.
Vendors in a wide variety of security tools market their products are as part of the ZTNA ecosystem, however building the architecture is mostly adopted by large enterprise and can be cost prohibitive to the SMB market. Therefore, it is not a one size fits all, nor is it a silver bullet for device security.

Evolution of Tools: The Road to Unified Endpoint Security

As the number of mobile endpoints grew, tools designed to assist in managing and increase visibility of company owned devices developed. Over the years, vendors have enhanced and evolved products as requirements expanded.

Mobile Device Management

As one of the first iterations of endpoint protection, Mobile Device Management (MDM) software is designed to secure, monitor, manage and enforce policies on employee devices such as laptops, smartphones and tablets.

Enterprise Mobility Management

Enterprise mobility management (EMM) builds on MDM in that it has more capabilities that MDM such as mobile application management and containment of data, but also allows for more flexible management of employee mobile technology. EMM became particularly popular when the bring your own device (BYOD) notion came about where more employees wanted to bring their own device for use in the workplace. EMM gives the organization more visibility over devices used for corporate business, and this trend continues. As more devices or connected things to the internet continued to grow, naturally existing MDM platforms and EMM suites needed to evolve.

Unified Endpoint Management

While managing and securing devices is important, the market continues to evolve. Unified Endpoint Security (UES) is the next step toward stronger endpoint security. According to Gartner, Unified endpoint security is a modern type of endpoint security, not meant to replace endpoint protection platforms, but provide a version that aligns with modern endpoint management and unmanaged devices. It provides a dashboard giving visibility of all endpoints and allows for prioritization of alerts and warnings and can inform the user of potential suspicious activity leading to resolution of the event (e.g. remote wiping, quarantining, isolating). Unified endpoint management (UEM) is the evolution of MDM and EMM and manages all endpoints including the internet of things (IoT) and wearables.

UEBA/UBA/SIEM

User behavior analytics (UBA), aka, user entity behavior analytics (UEBA) are designed to help security teams identify and respond to potential insider threats. It uses machine learning and artificial intelligence (ML/AI) to follow user behaviors and detect anomalies based on what it learns from the user's "normal" activities. Over time, UBA/UEBA integrated with security information and event management (SIEM) tools, which initially started out as a solution for security event log management.

These tools are necessary and all serve a purpose -- to protect the assets and integrity of the business. With successful breaches happening on a daily basis, these are simply not enough because none of them are monitoring the device itself.

Security Skill Sets Have Not Kept Pace with Threats

As threats and attacks are on the rise, the skill set for security teams is on the decline and has been for years. Particularly as organizations continue their path to digital transformation. As organizations become more digital, security becomes more critical and skill sets are challenged to keep pace with the threat landscape. This is largely why vendors are continuously developing products and solutions to automate specific functions and detect anomalies that potentially can harm business operations.

A survey by Information Systems Security Association (ISSA) and industry analyst firm Enterprise Strategy Group (ESG) revealed the areas where security skills are lacking include cloud computing security, security analysis and investigations, and application security. And that 95% of respondents state the cybersecurity skills shortage and its associated impacts have not improved over the past few years and 44% say it has only gotten worse.

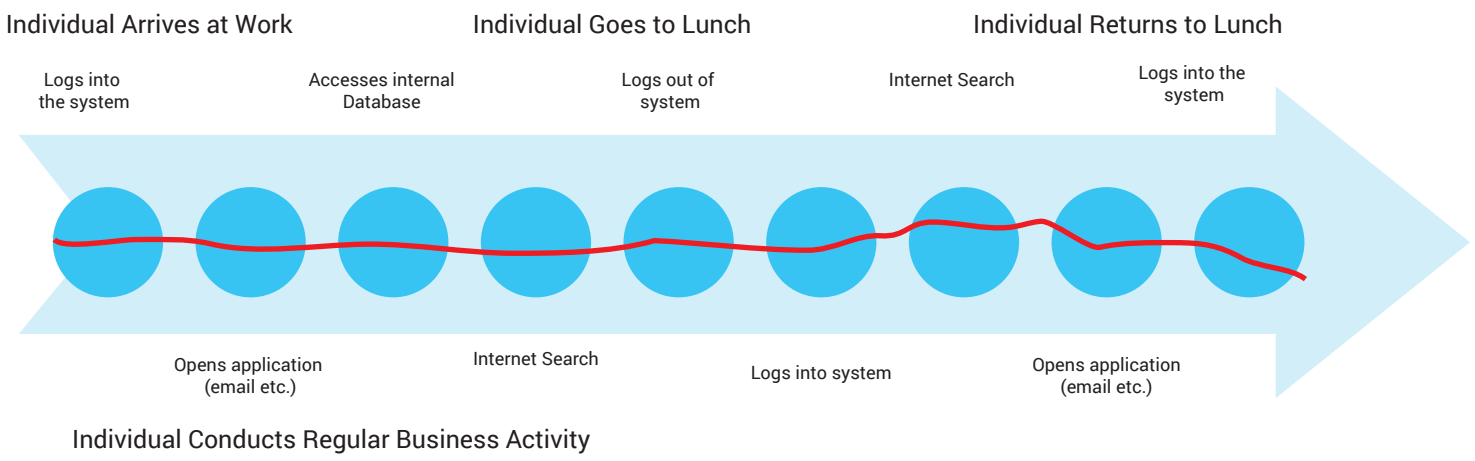
Security is more important now than ever before with the global pandemic forcing businesses to transition to remote workforce overnight. This meant that their digital transformation plans accelerated with security being a major component. Employees working from home could not benefit from the security architectures in the office environment. Personal printers, WiFi, external cameras and in some cases, personal laptops when company issued machines were not available are all at risk of exposure to cyber-criminal activity.

The Approach - Monitoring and Alerting at the Endpoint Level

Bad actors do things for fun, shock value, as a scare tactic, for financial gain, and for revenge. Ideally, security will be built into a device upon design, but even that is not guaranteed. And early versions of IoT devices which are largely still in operation weren't built with strong security as part of the DNA and most have none at all. Today, IoT devices and everyday items that are not generally thought about as being hackable are, in fact, being hacked. Examples include anything from manipulating the operation of brakes in a Jeep to eavesdropping through a lightbulb, not to mention the countless number of in-home smart devices like surveillance cameras, baby monitors, and virtual assistants that have been hacked. While scary and an invasion of privacy, other more critical security events have been a point of concern. Some of the most vulnerable medical devices to cyber-attacks are those that can be monitored remotely include insulin pumps and pacemakers. In the age of modern medicine, these devices are connected to the internet and can potentially be compromised, putting lives at risk. These are just a few examples of components of a network or devices that are inroads for potential security breaches.

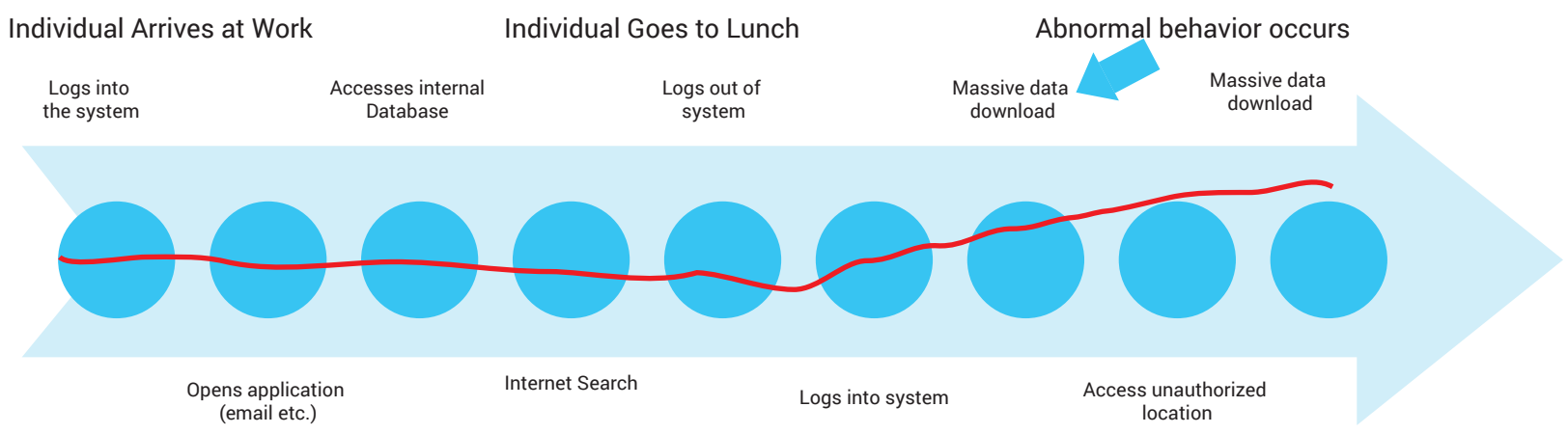
As these devices operate normally, the best way to know if an individual device or cluster of devices are exhibiting abnormal behavior is by monitoring them individually and in the event of an anomaly, the user or security team is alerted. The device can then be quarantined for further investigation to determine if the device has, in fact, been attacked or shut down completely further protecting the device, data, or user.

Much the same as Smart home devices, by monitoring average behaviors by the people using them, it is learned what time they are active in the morning, (e.g. movement around the house at varying times of the day and night) allows the device to adjust things like room lighting and temperatures. The aforementioned tools described (SIEM/UBA/UEBA) ultimately do the same from users in the workplace. They learn things like what time an individual typically logs into the system in the morning, the frequency of accessing internal systems, files and folders, how often they surf the internet. The figure below shows normal learned user activity with no anomalies detected.



Individual Conducts Regular Business Activity

Any deviation of the USERs behavior can trigger an alert as shown in the graphic below. The user in this case has potentially had their credentials stolen and information is being taken by a malicious source or the user is maliciously removing data.



Individual Conducts Regular Business Activity

But What is Protecting the Device?

In the above scenarios, nothing. Without insight into the devices – meaning human driven use and constantly learning the behavior of the device even without human driven use, organizations would never know if a device is about to fail, is malfunctioning for even a minor reason, or more seriously malfunctioning from a security compromise. The unknown can cause insurmountable damage to a business, financially and futuristically. Even asset management tools won't find anomalies at the endpoint level – they will locate the asset, but that's about it.

Security events happen every minute of every day and there is no shortage of events that make global news. As the growth in IoT devices continues, the level of visibility and management becomes near impossible, therefore any endpoint will need some level of security and monitoring. The consequences of cyber-attacks are costly. In fact, Gartner predicts that by 2023, the financial impact of cyber-physical system attacks as a result of fatal casualties will reach over $50 billion, 10 times higher than 2013 levels of data security breaches.

Knowing where devices reside and how they are operating can save both time and money through use of modeling and anomaly detection. And not just from security events. For example, an automobile manufacturing plant using robotics or mechanical devices assembling brakes is malfunctioning reversing an action so minute, but critical to the operation of the brakes. If it goes undetected, could cause the driver of the car to not brake causing an accident. Not only could there be negligence on the part of the manufacturer, but litigation could ensue costing millions of dollars in restitution and legal fees. The trickle-down effect is the costs associated with recalling the year, make and models and repairing them, not to mention long term effects such as loss of reputation. Modeling and baselining devices and constantly learning the behavior of the device assembling the brakes could have provided early detection and alerting of the malfunction, saving the company millions of dollars.

About MicroAI

MicroAI™ solutions are powered by proprietary algorithms making them small enough to live on a connected device. With MicroAI detects device behavior anomalies enabling asset owners to predict machine maintenance and prevent cybersecurity events.

MicroAI's Zero Day Attack Monitoring is a solution that through its artificial intelligence (AI) and machine learning (ML) capability, continually monitors and learns the behavior of the device to understand when an attack is being made through, anomaly detection. It keeps users and security teams one step ahead of vulnerabilities on their devices with predictive security algorithms that serves as a safety net in security architectures when hackers successfully locate and breach a network or device through an open patch.

MicroAI's solution is different from others in that it trains and runs fully local on the endpoint, saves cost on cloud transmission and is more secure as it can run full stack AI processing and visualize output within the local area network. Value is driven by its ability to identify specific machines and endpoints that are targeted or about to malfunction with alerts, triggers and notifications sent directly to the end user or security team.

With deployments in industries such as oil and gas, manufacturing, agriculture and telecom, MicroAI solutions help companies optimize the performance and security of their assets in a highly-connected world.

www.micro.ai advisor@micro.ai +1 (800) 852-0927

Visit www.micro.ai to access to our SDK. Send all technical inquiries to: support@micro.ai