Google Cloud

Trends in security: Artificial Intelligence (AI), machine learning (ML), and Internet of things (IoT)

So far, you've learned that new trends are emerging in digital security. Artificial Intelligence (AI) and its subset, machine learning (ML) are emerging as important trends in security. The Internet of Things (IoT) is also emerging, where home appliances like refrigerators and home security systems can connect to the internet and communicate over the cloud.

In this reading, you'll learn more about the implications of the AI, ML, and IoT technology trends. You'll also gain insights into how organizations can prepare for the future of cybersecurity with vulnerability and threat management, including a few examples of emerging security trends.

AI and ML

AI enables computers to perform advanced functions, including the ability to analyze data. Remember that ML is a subset of artificial intelligence that uses algorithms to train data.

There are three models of ML:

1. **Supervised learning:** This model maps a specific input to an output using structured data that's labeled. For example, if you feed the algorithm labeled pictures of cows, you can train it to recognize pictures of cows.
2. **Unsupervised learning:** This model learns patterns based on data that's not labeled. The algorithm can do things like matching patterns and descriptive modeling. The end result is not known ahead of time.
3. **Reinforcement learning:** This model is described as "learn by doing." The machine or "agent" uses trial and error as a feedback loop to perform a defined task.

AI and ML are constantly evolving, so they'll likely become more common in cloud computing tasks like security. As they evolve, they'll take on more duties, like searching for vulnerabilities and analyzing data. AI and ML might also become able to make helpful security recommendations.

AI also has its disadvantages. Currently, using AI requires many resources, like memory, power, and data. To train AI models, security teams need to find many different sets of data, like malicious codes, anomalies, and malware codes, which can be hard to find.

IoT

IoT enables devices to exchange data over the internet through sensors, software, and various technologies. For example, IoT enables you to use your mobile device to change the temperature of your home using a thermostat connected to the internet. There are billions of devices connected to the internet this way, and IoT connected devices have become a major part of internet traffic.

Pro tip: Think about IoT device security the same way you think about all other forms of security.

Note: Remember, malicious attackers use AI. They can also use it to test random data and identify vulnerabilities.

IoT effective practices

IoT is an evolving technology, so some providers of IoT devices do not yet apply appropriate security standards when designing their products. As a cloud security professional, it's important to be aware and take particular care when integrating IoT devices into your system environment. There are many best practices to be aware of when integrating IoT devices.

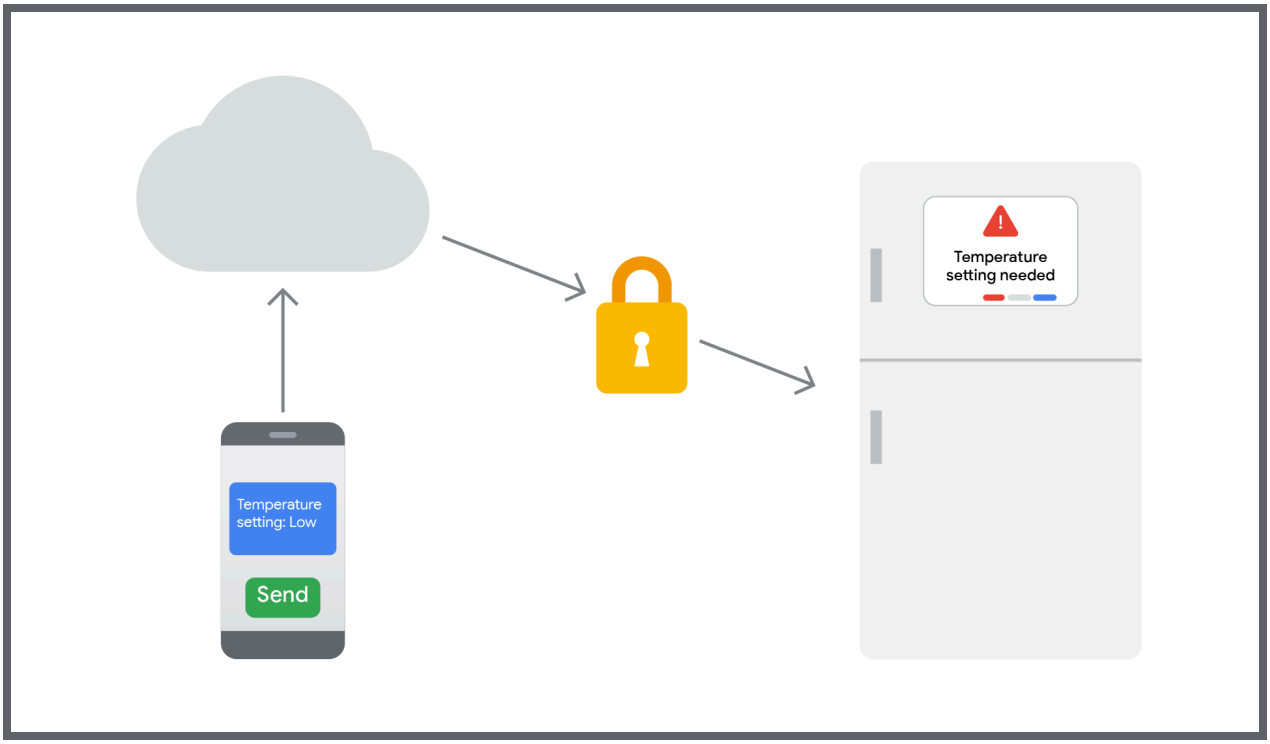
Best practices for IoT consumers

- Stay current with any OS updates.
- Apply strong passwords and credentials.
- Enable multi-factor authentication (MFA) if it's available.
- Disconnect any devices you're not using.

Best practices for organizations using IoT

- Implement an IoT policy for your organization.
- Keep an inventory of all IoT devices.
- Keep a security checkpoint, like a cloud access security broker.
- Monitor all your organization's devices.
- Encrypt all the data going through the organization's system.

This graphic shows how IoT works. In the graphic, a mobile phone is connected to the cloud. On the mobile phone is the option for setting the temperature of a refrigerator. The refrigerator is also connected to the cloud as an IoT equipped device. Between the cloud and the refrigerator is security to protect the device. This is represented by the lock. Because the IoT device is protected, you can safely use the mobile device to control the temperature of the refrigerator.



Implications for AI, ML, and IoT trends

The implications of AI, ML, and IoT trends on cloud security are significant. On the positive side, these technologies have the potential to significantly improve cloud security by automating many tasks. This helps improve visibility into security posture and helps enable faster and more effective response to security incidents.

On the negative side, these technologies also introduce new security risks. For example, AI and ML systems can be fooled by adversarial attacks and IoT devices can be used to launch attacks against cloud environments. It's important to be aware of these risks and to take steps to mitigate them.

How organizations can prepare for the future of cybersecurity

Now, you'll explore some practical, yet innovative AI, ML, and IoT examples that you can use for system integrations (SI) in cloud security.

- **AI-powered threat detection and prevention:** AI can help you analyze large amounts of data from cloud security tools to identify patterns and anomalies that may indicate a threat. With this information, you can prevent attacks from happening in the first place. For example, Google Cloud's Chronicle Security Operations platform uses AI to analyze data from a variety of sources, including security logs, network traffic, and user activity to help detect and respond to threats in real time.
- **ML-based security orchestration, automation, and response (SOAR):** ML can help you automate many of the tasks involved in responding to security incidents, like investigating alerts, triaging incidents, and taking corrective action. This can help security teams respond to incidents more quickly and effectively. For example, IBM Security SOAR uses ML to automate many of the tasks involved in incident response, like helping identify the root cause of an incident and recommend remediation steps.
- **IoT-based security monitoring and analytics:** IoT devices can help you collect data about the security posture of cloud environments. You can analyze this data to identify potential threats and vulnerabilities. For example, Cisco Secure Access by Duo uses IoT devices to help monitor the security posture of cloud environments and identify potential threats, such as unauthorized access and suspicious activity.

Key takeaways

AI and ML are constantly evolving, and as they do, there'll be more ways to use them to help with your security duties. For example, AI and ML might help you find vulnerabilities and analyze data.

IoT is another emerging technological trend. IoT can help you collect data about the security posture of cloud environments on devices connected to your systems and linked to the internet and the cloud. IoT can also help you communicate with other connected devices and individuals.

In your role as a cloud security professional, you'll find many ways to use AI, ML, and IoT to help you stay ahead of the threat actors that can compromise your system.