Multiplying the Intelligence of Your Security Systems

The Enterprise Security of Things

We live in a connected world.

Twenty years ago security technicians were squinting at grainy video feed – reviewing thousands of pages of log files, hoping to decipher a threat. But, in reality, the best they could do was see what happened rather than identify a threat in progress.

Today, technology inspired by the Internet of Things (IoT), allows organizations to incorporate real-time and near real-time threat alerts into almost every aspect of their facilities and technology.

Is your organization responding fast enough to the threats created by new technology?

Traditional Physical/Logical Security Systems Can't Protect Against the Insider Threat – They Can Only React to the Loss of Data/Property.

While information systems are literally connecting every aspect of operations, most organizations still segment security into two, unconnected systems: physical security and logical security (also known as cybersecurity). While the logical security operations center focuses on IP theft, malware, viruses, network security, data at rest security, data in transit security, and so on; the physical security operations center is concerned with surveillance and access control.

The departments that manage the technology for these two types of security are usually entirely separate, and often do not even collaborate.

In most organizations, systems controlling physical access is a completely separate system and operations center from the logical security systems.

While organizations must be vigilant to protect against outside attacks, it is internal threats that are front-of-mind for most security professionals today. A nefarious character who gains physical access to a computer can almost always take advantage of that access to further their efforts.

That is why integrated systems are more imperative than ever before.

> "As long as organizations treat their physical and cyber domains as separate, there is little hope of securing either one. The convergence of cyber and physical security has already occurred at the technical level. It is long overdue at the organizational level."
>
> Scott Borg, Director of the U.S. Cyber Consequences Unit

It's Time For the Enterprise Security of Things

The Enterprise Security of Things (ESoT) builds on the principles of IoT to provide a smarter, fully-integrated security posture that can anticipate and identify threats faster and with more accuracy.

The technology is available to connect your physical and logical security operations safely and securely. Cameras are now IP-based; enterprise access control systems; and access lists, policies, and procedures are in databases. That means your systems can finally communicate with one another.

The Enterprise Security of Things provides an answer to the following types of challenges:

- Inability of security departments to communicate in order to accurately identify a person's identity
- Increased threat of data malice
- Best practices are not consistently applied across departments, geographic locations, and/or organizations
- Inability to physically monitor logical security devices
- Difficulty of detecting tampering and unauthorized access to a logical device console

In order to address these new threats, it is paramount that organizations have both the integration technology and a single, high-level individual or department responsible for a comprehensive security policy that covers both physical and logical security.

The Real-World Benefits of ESOT

Imagine a world in which logical and physical security are fully integrated and constantly learning from each other. Organizations are empowered to track threats and potential threats not only on individual devices but also across networks, systems, and geographic locations.

Cases for Use of an Integrated System:

Virginia: Virginia arrives at work at 6 a.m every morning. Her ID badge is swiped and a guard waves her through. Her entrance to the facility is recorded by surveillance video and her license plate is photographed. Today, Virginia arrives at 10 a.m. With traditional security methods, this information is nothing more than a data point that could be accessed after-the-fact to build a case against Virginia. With ESOT, an integrated system will identify this anomaly and notify a security personnel in real-time or close to real-time.

Tony: Tony is a network administrator at a secure facility who attempted to access a secure room after-hours but his access is rejected. An integrated security system recognizes both anomalies: He is in after-hours and his access was rejected. The system then notifies a security personnel in real-time or near real-time.

Christie: Christie is using a root username and password rather than her normal login to access a secure computer workstation. Only a fully integrated security system will recognize this anomaly and alert the proper security personnel.

Dale: Dale is logged into two workstations in two different geographic locations simultaneously. An integrated security system will alert security personnel while the infraction is occurring rather than days or weeks later.

ESOT integrated security systems process all of the information above, identify anomalies, and notify the proper authorities in near real time.

Not every one of these anomalies is an actual threat. There may be valid instances for most of the scenarios above. However, instances like these are the first indication of suspicious behavior that should be monitored and tracked. Creating universal integration of security across physical, network, and logical domains makes it easier for organizations to utilize security information to anticipate threats rather than simply responding to threats.

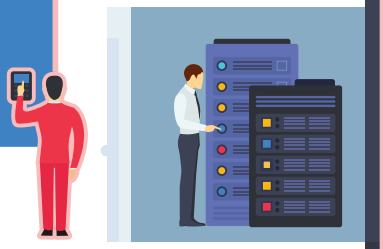
It's normal until it's NOT!

ESOT - The Perfect Marriage of Physical and Logical Security

Enterprise Security of Things searches for the piece or pieces of the puzzle that do not quite fit so you can identify a threat before it becomes a crisis.

- ID Check
- Badges
- Security Guard
- Video Surveillance
- Facial Recognition
- Voice Recognition
- License Plate Photo

- Fingerprint Scan
- Biometric Scan
- Card Scan
- Facial Recognition
- Facial Recognition
- Voice Recognition



- Password
- Pin Number
- CAC Card

- Geographic Monitoring

All security information is fed into the data repository which is constantly searching for anomalies in real-time.

Alert Virginia's license plate and badge clocked in two hours later than her normal arrival time.

Alert Tony attempted to access a secure room after-hours but his access was rejected.

Alert Christie logged into her computer station using a root username and password.

Alert Dale is logged into his account at two different geographic locations simultaneously.

Security officer investigates & responds to real-time threat alerts.

- ✔ Virginia... Attended a Funeral
- ✔ Tony... Working on Special Project
- ? Christie... Set Alert for Every Root Login
- ✖ Dale... It's Normal Until It's Not!

ARIEL TECHNOLOGIES

www.arielusa.com