WHITE PAPER

ENSURING AVAILABILITY AND SECURITY OF CRITICAL BUSINESS SYSTEMS IN THE AGE OF IOT

EXECUTIVE SUMMARY

The Problem

By 2020 there will be 20 billion connected devices in the world. Nearly one-quarter of them will be deployed in businesses, as integral parts of critical systems intended to optimize operations, increase profits, and provide competitive differentiation. In 2016 alone, 52% of global enterprises had or were planning to utilize Internet of Things (IoT) solutions to move their business forward.

Simply having more devices in and of themselves aren't the problem. The issue is that these devices are a massive conduit for security vulnerabilities to enter your company. Security vulnerabilities, if exploited, can have direct impact on the availability of critical business systems. In fact, Hewlett Packard (HP) research found that 70% of IoT devices are vulnerable, and a Dark Reading study found that IoT devices contain an average of 25 vulnerabilities. Not only are connected devices exposing an entirely new attack surface, their integration in key business systems and infrastructure--patient management, manufacturing controls and processing, utilities management, etc--elevates the risk of that attack surface beyond data breach to include financial loss, business reputation and physical safety.

The Solution

Secure adoption of the Internet of Things requires a new approach—one that accounts for a couple of basic facts: first, that IoT projects are being adopted at a rate and scale that make agent-based management solutions completely unrealistic. Second, *older,* previously isolated networks and systems are being retro-fitted to interconnect with other business systems to promote efficiencies in productivity and revenue. These older systems tend to be extremely sensitive, such that any kind of intrusive security scans could render the system inoperable.

Pwnie Express' solution is based on the simple premise that a deep understanding of devices, the networks upon which they communicate and the relationships between them is fundamental to gaining and maintaining control of the critical systems which run your business.

This is done through passive, non-intrusive surveillance of the network, device profiling, real-time threat detection and automated risk scoring, without having to capture and store packets, install agents or rely on intrusive scanning like existing solutions. This allows you to

see the world the way an attacker, not the helpdesk, would see it.

These are the core components of the Pwnie Express solution:

+ **Data Collection:** Pwnie provides hardware sensors to continuously and passively monitor the environment, devices and how they move through the network. The sensors are hardened and encrypted. This data is sent to a cloud-based management console called Pulse which analyzes all of the data.
+ **Policy Specification:** Quickly and simply define the acceptable network, system and device behaviors, both on and off-network. This allows you to instantly generate a system baseline of *your things* without having to pre-populate a list of assets or networks.
+ **Critical System Monitoring & Threat Analytics:** Systems are made up of device components. Pwnie Express automatically builds these correlations and gives you the ability to assign the business function and criticality of these systems. Then, we monitor them for changes in how they are configured, how they are communicating and how devices are moving between low-trust and critical networks.
+ **Response:** If any device puts the system at risk of sabotage, compromise or denial of service, Pwnie offers multiple alert options including to your incident response system and gives you the ability to take instant corrective action. The Pulse sensors also house a complete suite of remediation capabilities so you can fully act without the need to be physically on site.
+ **APIs & Integrations:** Push the insights you get from Pwnie Express into your larger security stack with our SIEM adapters, proactively respond to policy violations via your existing control plane or build your own applications through our RESTful API.

• • •

ENTERPRISE MISSION ASSURANCE WITH PWNIE EXPRESS

ABSTRACT

This paper is intended for those organizations and enterprises with a need to assure critical system availability and security who are planning, designing and implementing solutions which require minimal downtime for implementation. In understanding the issues with current solutions, we describe the critical requirements of the ideal platform to include deployment and management scenarios.

THE IoT SECURITY GAP

Historically, the technologies running our business have been highly segmented and isolated from each other. IT and security teams have been focused on securing the laptops, infrastructure, servers and applications which optimize employee productivity, but have not been responsible for the really critical operational systems—manufacturing production, point of sale terminals, medical devices, physical security components—which run the business.

Those days are over. To gain competitive advantage, to streamline business processes, and to drive down costs, businesses are connecting parts of their business that have never been connected before. Not just to each other, but even to Internet-facing, third-party (vendors and contractors) organizations to leverage big data analytics, drive smart automation and realize cost savings across previously segmented functions.

These newly connected systems introduce a huge new diversity of devices into the environment which we can bucket in four ways:

- ***Traditional IT Devices****:* These are the laptops, printers, network infrastructure, phones, etc… that IT security professionals are accustomed to monitoring, managing, securing, etc.

- ***Employee-owned****:* The devices and technology of employees also have access to privileged systems. They are connecting to our networks, and integrated in our businesses as deeply as any corporate device. In fact in 2017, 50% of devices in the enterprise are employee owned.

Each of these, in their own way, can expose the business to dangers through uncontrolled interactions of connected systems which can directly impact physical safety, revenue, public perception, or degrade the customer experience.

- ***Operational:*** The biggest disruption from IoT/IIoT is in the operational technology (OT) world. These formerly isolated environments are now being connected. These sensors, medical devices, HVAC, building management systems and others are now being connected to the Internet, to corporate networks, to privileged third-parties all of which expose the business to significant new risks.

- ***Public:*** Much like employee technology is invading the enterprise, so is public wireless and other technology that now exists *around* our own enterprises.

Each of these, in their own way, can expose the business to dangers through uncontrolled interactions of connected systems which can directly impact physical safety, revenue, public perception, or degrade the customer experience.

All of this points to a major gap in the security team's ability to see, track and monitor these new types of devices. We call this the IoT Security Gap. Existing security solutions struggle with this gap:

- Endpoint Security /MDM– Works great for traditional IT security devices, but agents don't work on employee, or operational devices. The diversity of devices and the limited resources of operational devices severely limit the ability to actually install agents on IoT and Industrial IoT (IIoT) components.

- NAC – Network Asset Control is great at controlling initial access to the traditional IT networks, but it doesn't provide the continual assessment, doesn't identify IoT devices, and introduces too much of an availability risk when it comes to OT environments.

- Vulnerability Management – Traditional vulnerability management solutions introduce too much risk to the availability of these new devices. Their heavy weight scans can take devices, especially operational devices, offline or worse, render them inoperable. Newer vulnerability scanners have the ability to do

- Passive packet capture – sniffing network traffic is great for both traditional as well as OT networks typically because it allows for visibility of device communications without having to be intrusive or utilize agents. The fundamental flaw here, however, is twofold: first, interpreting industrial or even proprietary protocols requires either a robust library of pre-built signatures to identify anomalous traffic, or a domain expert who is able to conduct deep protocol analysis on proprietary traffic on the fly. Second, packet capture by its own nature is only effective *when the device is communicating on the network*. Increasingly, IoT networks operate completely wirelessly, communicating over protocols like Bluetooth, ZigBee and cellular. Enterprise-class detection solutions for this simply don't exist.

MINIMUM REQUIREMENTS TO CONFRONT THE GAP

The solution to deal with the IoT Security Gap must meet the following requirements:

1. Cannot require the use of agents to operate.

2. Must offer completely passive detection of all device types including extended spectrum (wireless, Bluetooth, etc) and non-traditional networks.
3. Can proactively generate a device and network inventory, construct a baseline and alert on deviations from it.
4. Automatic and continuous correlation of interfaces to devices; devices to systems; systems to operational functions.
5. Provides context of security events which can cause negative impact to critical business operations.
6. Must remain independent of the network architecture—nothing that could render the network or associated devices unavailable.
7. Assumes zero-trust of the environment: allows for granular definition and customization of acceptable behaviors, devices, networks and enforcement actions in accordance with local policies or industry standards.
8. Proactive detection and flagging of any/all events or behaviors which could render a critical system unavailable or vulnerable to sabotage.
9. Offers centralized control with decentralized execution of remediation tasks.
10. Findings and analytics are accessible by other parts of an existing security framework or can be used as the basis of new applications.

With these requirements in mind, we present Pwnie Express. Pwnie Express' solution is based on the simple premise that a deep understanding of devices, the networks through which they communicate and the relationships between them is fundamental to gaining and maintaining control of the critical systems which run your business.

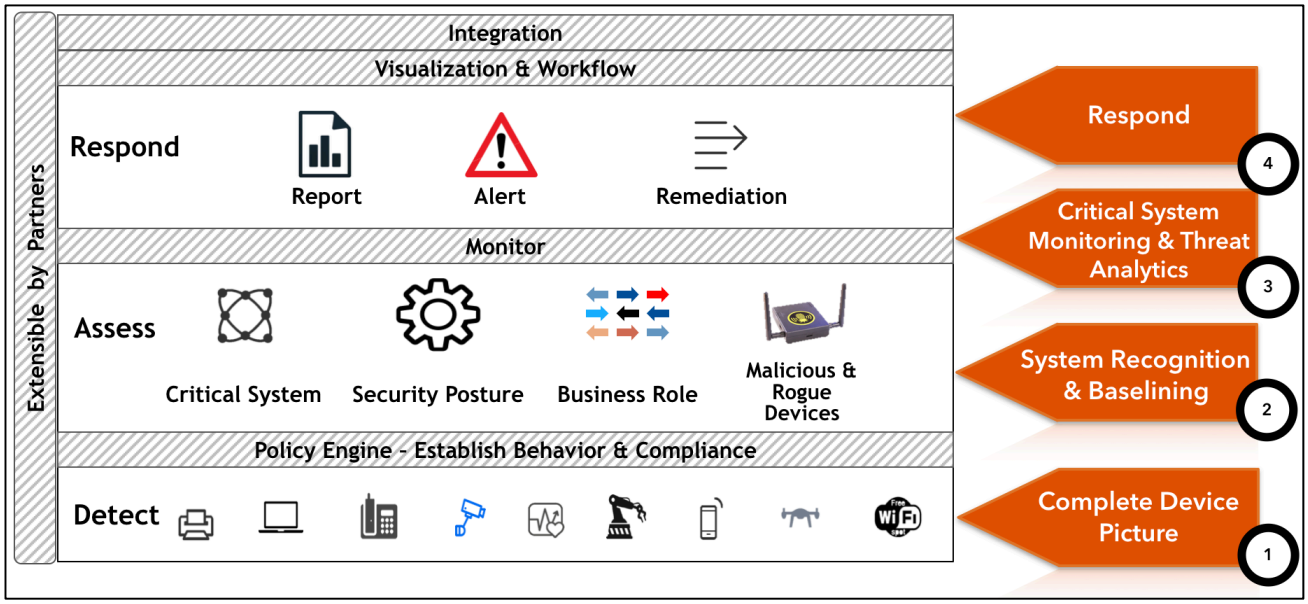


Figure 1: Pwnie Express Solution

This is done through passive, non-intrusive surveillance of the network, device profiling, real-time threat detection and automated risk scoring, without having to capture and store packets, install agents or rely on intrusive scanning like existing solutions. This allows you to see the world the way an attacker, not the helpdesk, would see it.

PWNIE EXPRESS PLATFORM COMPONENTS

The Pwnie Express platform was borne out of our experience as penetration testers. We know the cyber kill chain[1] because we actively participated in it. We know that reconnaissance, done with stealth and agility, is the prelude to any kind of engagement and that's really what we wanted to reflect in our platform. Like most hackers, we also took the approach of 'zero-previous-knowledge' of the environment, its architecture or its protections, so we knew that we needed to build a system which could operate independently of the network stack, while still contributing to it. Finally, we knew any hacker worth their salt would take the path of least resistance: why attack the highly fortified data center when you can upload your malware to the web camera's FTP server and move laterally through the network from there? We wanted to show people the information they needed to know to understand which devices could put their business at risk and what they should do about it. Here is how we've architected our system to do just that.

THE HARDWARE

Pwnie Express uses hardware sensors, known as Pwn Plugs, which connect to the network as unprivileged hosts and surveys the entire spectrum, wired and wireless environment continuously. The sensors also include bays for additional adapters to make it easy to extend spectrum visibility on an ad-hoc basis. Typically, you only need to have one sensor per location as they are capable of monitoring connection events across VLANs, though full wireless coverage may necessitate additional wireless sensors. The sensors communicate (outbound-only) over a secure connection back to the cloud-based Pulse Management Console.

COLLECTION

Collection is foundational to provide the information needed to develop a complete device picture. Collection is performed at the sensor level and is comprised of

[1] http://www.csoonline.com/article/2134037/strategic-planning-erm/the-practicality-of-the-cyber-kill-chain-approach-to-security.html

multiple services which continuously survey both the wireline and wireless spectrum gathering data on found devices, networks and their associated configuration.

There are multiple ways in which Pwnie Express collects device data, passive detection being foremost amongst them. The services running on the sensors passively listen for any and all indications of a device connection, whether that be new MAC address advertisements, new IP addresses appearing in a subnet or new wireless broadcasts appearing in the airspace. As new devices are discovered on the network, we can also perform a deep port, service and vulnerability scans, without the need for any agents to be installed or configured. The frequency and depth of this scan is user configurable from the Pulse Console. All of the information goes back to the Pulse Console for deeper analysis, fingerprinting and profiling.

POLICY DEFINITION

Seeing what's abnormal means establishing a norm: a baseline. Pwnie Express allows you quickly and proactively specify the expected network configurations on the wire and off. Here, you can identify the corporate and guest networks, their expected encryption levels, manufacturers, authentication types. The policy engine gives users a means to define the corporate boundaries including which networks are fluid (such as guest networks) and which should be static (such as production networks).

CLASSIFICATION

Where the policy engine establishes acceptable behaviors, the classification engine is the mechanism to bucket the found devices and networks into specific definitions: corporate, non-corporate or guest; trusted or untrusted; crown-jewel or critical-network; rogue, misconfigured or malicious. Each network and device receives unique identifiers to classify their criticality and business role. Classifications are reassigned continuously as the device and network changes.

MONITOR FOR DEVIATIONS

During the monitoring phase, we look for deviations from the established policies as well as device and network classifications which could render the system vulnerable or inoperable. The product comes with over 100 out-of-the-box threat definitions and users have the ability to tailor them to suit their organizational threat models.

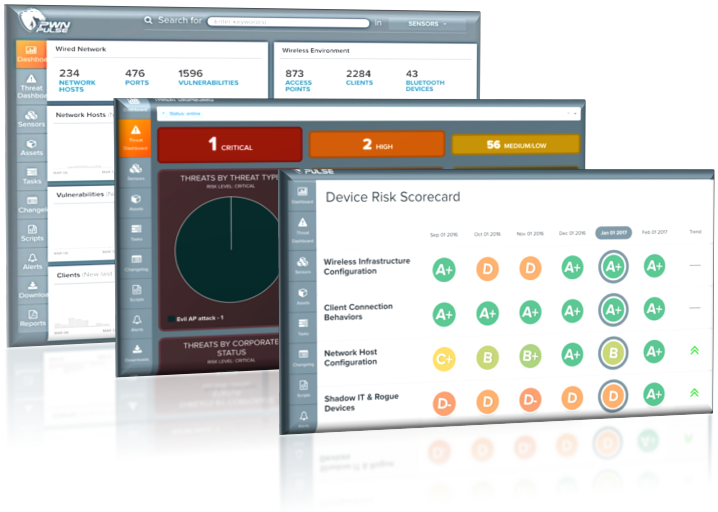
RESPOND TO THE EVENT

Pwnie Express provides three means to respond to devices and networks which put critical systems at risk:

+ **Report:** reports provide trending data on-demand, allowing you to quickly and visually determine whether or not the event is a one-time situation or if it is indicative of a larger, coordinated attack. The reports include recommended remediation steps.
+ **Alert:** Real-time notifications of a negative event or configuration which could put the system at risk of becoming unavailable.
+ **Remediate:** Corrective actions you can take immediately within the product to neutralize malicious actions which put the business at risk.

VISUALIZATION & WORKFLOWS

Traditional approaches would make sorting through all of the devices and networks and identifying which ones could put critical systems at risk a daunting and tedious task. Pwnie Express provides intuitive dashboards and filters which immediately identifies issues with the critical systems you actually care about.



Anomalous events are automatically organized in accordance with their user-defined criticality. All Pulse data is stored for 90-days by default (though longer data retention options are available) Investigators and incident responders can instantly identify how and when a device or network was used as an vector of an attack.

APIs & ADAPTERS

The Pulse Management Console includes an application programming interface (API) that makes it possible to leverage the Pwnie Express platform for custom applications. The full featured RESTful API allows for URI-based query language for data retrieval makes it possible to push Pulse data into any workflow, ticketing or incident management system. Additionally, the solution includes a syslog adapter which allows you to ingest network host, wireless client, Bluetooth, vulnerability and alert data into the SIEM of your choosing.

OUR ANALYTIC PROCESS

Though described in phases, in reality the process of data collection, classification, correlation, response and integration are continuous and fluid. The proliferation of devices leads, inevitably to a huge amount of data to sift through. The Pwnie Express Analytic process takes that raw data and converts it into finished device intelligence using both user-defined policies as well as automated device and system baselining to identify anomalous behaviors both on and off the network.

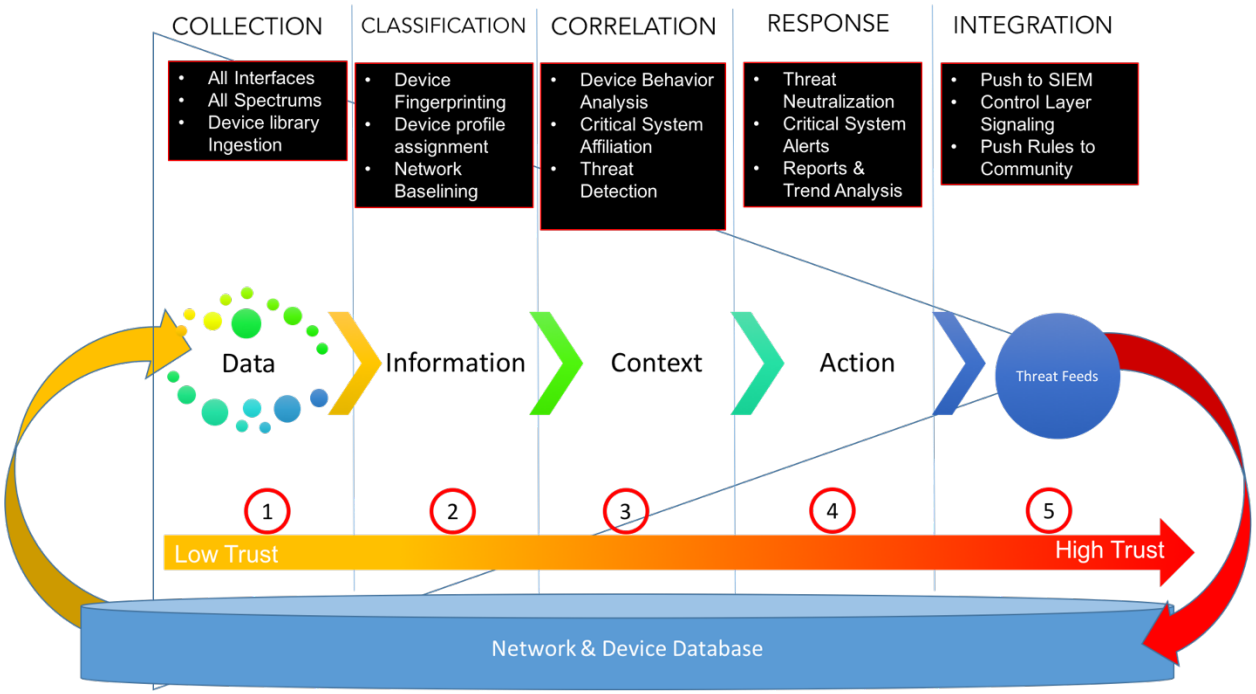


Figure 2: Pwnie Express Analytic Process

PHASE 1: GET THE DATA

Understanding systems requires first having a complete understanding of the ***whole*** device including its acceptable configuration and communications capabilities. There are multiple ways in which Pwnie Express collects device data, passive detection being foremost amongst them. The services running on the sensors passively listen for any and all indications of a device connection, whether that be new MAC address advertisements, new IP addresses appearing in a subnet or new wireless broadcasts appearing in the airspace. The process starts with device

collection. The collection process is driven by multiple proprietary services which, like a vacuum, pulls in all devices and networks seen by the local hardware sensor regardless of interface or spectrum. Another service running on the sensor passes all of this information securely back to the Pulse Management Console to go through deeper analysis, fingerprinting and classification.

*Figure 3: The **whole** device, beyond a description of interfaces*

PHASE 2: CLASSIFICATION

The next stage in the process is to classify the devices and networks. This is where all of the collected attributes described in the previous section are compiled into asset records and are sorted into specific categories by state, configuration, trust, location and more.

Classifications are reassigned continuously as the device and network changes. Pwnie Express uses a 'zero-trust' paradigm for all devices. The first time a device or network is seen, a new asset record is created and its trust level is automatically assigned to be 'unknown', meaning it should be considered untrusted until it can be determined trust-worthy or not. For every time the device or network's attributes change i.e. a new IP address is assigned or a new port opens up, this information is added to the timeline of changes on the individual asset record. Some states and configurations of assets will dictate automatic trust-level down-grades—for instance if a malicious wireless device is identified or if an asset has an excessive number of ports open. Additionally, some affiliations are automatically assigned such as whether or not the device or asset belongs to the corporation or not. Beyond these automatic classifications, users can further classify assets manually into specific definitions such as: crown-jewel or critical-network; business role; rogue, misconfigured or malicious.

The 'corporate' classification is a privileged designation in the Pulse ecosystem. This designation is automatically assigned via the policy engine. Through this policy definition, Pulse will automatically look for networks which match the description and will queue them up to be approved as 'corporate networks'. Any asset which successfully authenticates to these corporate networks are also given corporate status.

Corporate devices are treated as more important than non-corporate or guest devices. This directly aids in the threat detection and analytic process, making it easy

For those that allow vendors or 3rd parties to connect to any part of their network, this is crucial intelligence to keep uncontrolled devices from associating with production systems.

to see if and when a privileged device is on an insecure network or, worse, when an unprivileged device is on a privileged network segment. For those that allow vendors or 3rd parties to connect to *any* part of their network, this is crucial intelligence to keep uncontrolled or untrusted devices from associating with production systems.

The added benefit of this definition is that it automatically builds an asset inventory list. Users can also validate their existing CSV-based asset inventory list by ingesting it via the Pulse API or by integrating with existing asset inventory tracking systems such as Active Directory. From this, it is easy to see if, when and where rogue devices, which may have by-passed existing NAC or 802.1x-based solutions, appear on the network.

PHASE 3: SYSTEM CORRELATION

Once the individual assets have been classified, the next stage in the process is to assess the relationships between them and determine whether or not they are appropriate based upon user-defined policies and previous behaviors observed. Characterizing these relationships allows us to make inferences, not just about appropriate asset behavior, but also how the assets are affiliated to larger systems. As a simple example, drones are often paired with a controller component—Pwnie Express identifies, not just the drone itself, but also the controller and correlates them both into a system definition. Should that relationship be broken or changed in an unusual way, Pwnie Express generates a threat event which appears as part of the asset record as well as in the threat dashboard for a holistic view of all active threat events.

PHASE 4 & 5: RESPONSE & INTEGRATION

In order to understand how to react to any threat, you need to know what it is, when the threat occurred, when and if the threat subsided, what it affects and where it is. Pulse provides all of this information throughout the product, from the asset records all the way through to reports. The asset records also include our (patent-pending) location service which allows you to determine precisely *where* the threat is coming from without having to walk SNMP or MIB-records.

Alerts are the means through which you are *notified* about the occurrence of a specific condition or event. Pulse comes out-of-the box with two-dozen alert definitions, and also allows users to create their own custom alerts. The alerts can be read in-product, sent to you over email or sent to the other portions of the security stack including your SIEM via our API.

Assuming there is a threat to the system, users then have the ability to take action on those findings both in the product—via deauthentication of malicious devices—or by pushing the threat data (asset information as well as threat definition) to other portions of the security stack or additional control mechanisms.

It is also important to understand if the threat is isolated, if it is systemic or if it is part of a coordinated attack. The Device Risk Scorecard can be used to provide this context and includes the remediation steps.

GROWING CONFIDENCE IN DEVICE CLASSIFICATION

Pwnie Express utilizes past behavior and configurations to predict the future. As new devices types appear, they receive a unique fingerprint which serves the purpose of not only rapid device classification through the funnel, but also improves the fidelity of classification, ensuring that inferences around expected behaviors, configurations and relationships are made with a high degree of confidence which improves over time. Though individual customer data is kept separate, the device fingerprints are referencable by all customers, ensuring that even if a device is new to an individual customer, there's already a high-confidence profile of device type and expected behavior as previously seen in other environments. This construct is also used to proactively inform customers about new vulnerabilities as they are discovered, malicious or suspicious networks (by SSID) as well as wireless attacks which may be affecting other organizations in close proximity.

CONCLUSION

Key business processes will become increasingly reliant on secure deployment and monitoring of connected systems. The speed and variety of device types, operating systems, and configurations creates an environment ripe for sabotage, compromise or availability issues and traditional approaches to solving the problem simply can't keep pace. Installing software on many of these devices is not an option - IT is often not managing these devices, in fact, they are often managed by the device

manufacturer themselves and these solutions are often installed without IT input or visibility.

Pwnie Express takes a holistic approach to dealing with this problem. By having a deep understanding of devices, networks and relationships between them Pwnie Express ensures the security, availability, and safety of these critical systems allowing the business to keep moving forward.