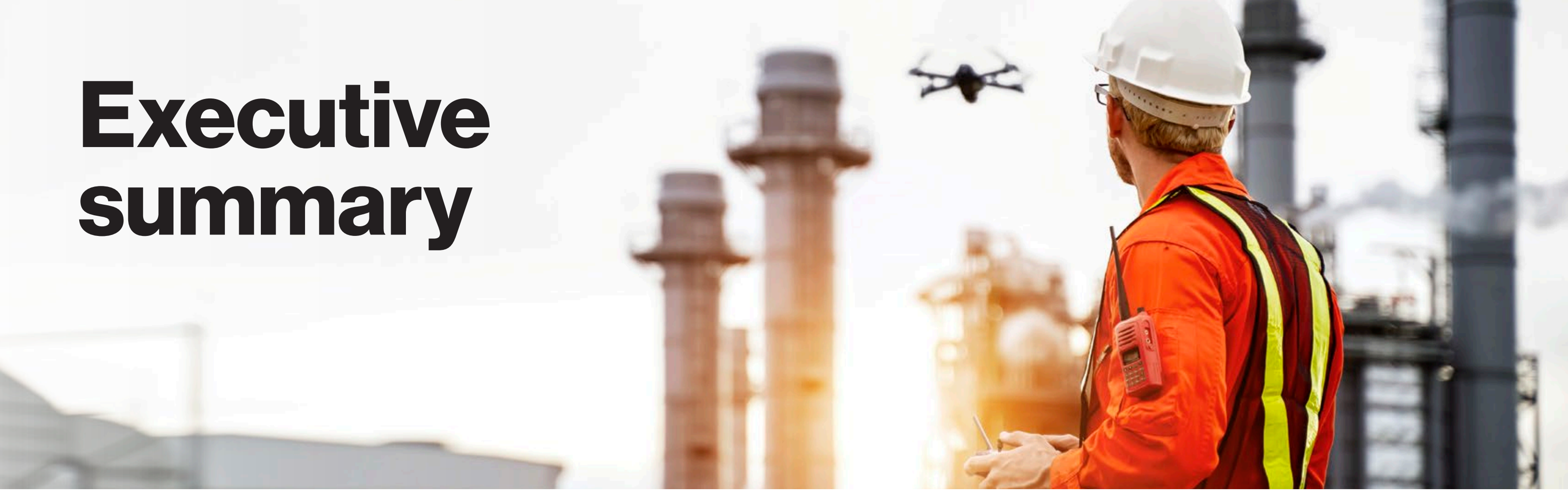
White paper

Establishing a zero trust model in IoT environments

A realistic and executable approach to helping your organization be better protected from IoT-focused cyber threats

verizon✓

Executive summary



In February of 2023, a United States healthcare provider disclosed that malicious actors breached their network, exfiltrated clinical images and protected health information (PHI) about cancer patients, then published it in the public domain. The attackers demanded ransom, but the provider refused to pay.[1] The attackers then published the data on the dark web in retaliation. An organization with a noble mission and vital role in our society suffered disruption, the loss of data and reputation and likely monetary damages.

However, this story is unique in at least one respect: the hackers exploited the convergence of Internet of Things (IoT) and information technology (IT) systems, a convergence that is also growing exponentially, not just in healthcare provision but across all industries and sectors. In this case, a medical device (IoT) captured patient images for radiation oncology treatment and transferred them to a networked computer system (IT).

Many organizations are deploying IoT devices throughout their facilities and networks—cameras, monitors, sensors, appliances and other gadgets—but are they protecting themselves from cybersecurity threats? Perhaps they do not know how best to approach this imperative. In this paper, we lay out a comprehensive approach to doing just this, based on the concept of zero trust. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207[2] provides the following definition of zero trust: Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

The guidance in the paper is straightforward and written for lay readers, while being tactically executable. It stands to benefit not only IT and cybersecurity professionals, but also other organizational stakeholders, from small businesses, large enterprises and government agencies. Some terminology is specific to the fields of IT and cybersecurity, but we attempt to define all terms so that all readers can easily understand them.

The paper discusses common IoT cyber threats to organizations, categorizing them based on a popular framework, then offers a four-step process to address them based on a zero trust capability model.

Four-step process to address common IoT cyber threats using the zero trust capability model

1. Establish baseline of current capabilities.
2. Prioritize the capability model to your IoT gaps.
3. Map potential supplier services to IoT priorities.
4. Map solutions to threat types and assign maturity levels.

The content within the paper offers realistic and achievable overarching guidance to help protect organizations in the incorporation of IoT throughout operational infrastructures using zero trust architectures.

[1] The HIPAA Journal

[2] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Zero Trust Architecture

Tactics, techniques and procedures (TTPs) for IoT attacks

The adversarial attack patterns used to exploit weaknesses in IoT ecosystems are diverse, rapidly evolving and the adversaries' tactics, techniques and procedures (TTPs) employed to exploit those weaknesses are effective. Several years ago, many of the publicized IoT security events were Distributed Denial of Service (DDoS) attacks using compromised IoT devices. DDoS attacks are still prevalent today; however, the attack patterns and results are becoming more diverse and complex.

The remaining part of this section provides examples of common TTPs adversaries use to exploit IoT systems and where applicable, describes how the TTPs for IoT converge with attacks on IT. The TTPs used in this section align to the MITRE ATT&CK[3] framework and have been validated in practice by Verizon's more than 20 years of experience responding to security breaches. Additionally, the TTPs used in the subsequent sections of this document to describe approaches to applying zero trust to IoT security initiatives.

Table 1 provides eight common adversary TTPs and the common IoT threat vectors related to those TTPs. The columns titled "Technique" and "Technique Description" were extracted from the MITRE ATT&CK framework. The column titled "Common IoT Threat Vectors" provides real-world observations based on Verizon's experience securing IoT devices.

Table 1: Tactics, techniques and common IoT threat vectors

Technique	Technique description	Common IoT threat vectors
Exploitation for client execution	Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecured coding practices that can lead to unanticipated behavior.	• Many IoT devices are unable to be patched by traditional, centrally managed IT tools. • Often IoT networks are excluded from vulnerability scans and remediation activities due to lack of resources and/or concerns about the potential impact to business operations.
External remote services	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as virtual private networks (VPNs), Citrix and other access mechanisms allow users to connect to internal enterprise network resources from external locations.	• IoT devices typically have remote management functionality enabled by default when shipped by the manufacturer. The default username and passwords are often enabled. • When a network is compromised and an attacker has valid user credentials, the attacker could use a VPN connection to move laterally into an IoT network.

[3] MITRE ATT&CK

Tactics, techniques and procedures for IoT attacks

Table 1 (cont.)

Technique	Technique description	Common IoT threat vectors
Lateral tool transfer	Adversaries may transfer tools or other files between systems in a compromised environment. Once brought into the victim environment (i.e. ingress tool transfer) files may then be copied from one system to another to stage adversary tools or other files over the course of an operation.	• Compromised IoT devices that are not physically or logically segmented on the network are used for lateral movements, data exfiltration and as a launching point for additional malicious software.
Hardware additions	Adversaries may introduce computer accessories, networking hardware or other computing devices into a system or network that can be used as a vector to gain access.	• Adversaries introduce unapproved hardware; however, it is more common for end-users to introduce unapproved, insecure IoT devices on the networks.
Exfiltration over alternative protocol	Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.	• IoT devices typically have file sharing protocols enabled by default when shipped by the manufacturer, making IoT devices an excellent threat vector to exfiltrate data (e.g., FTP).
Exfiltration over other network mediums	Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a Wi-Fi connection, modem, cellular data connection, Bluetooth or another radio frequency (RF) channel.	• IoT connectivity options are diverse (wired, wireless, e.g., 5G, 4G LTE, Wi-Fi, Bluetooth, etc.). Adversaries use these options to evade security monitoring tools and/or because the security controls are not implemented for certain connection types but not for others.
User execution	An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link.	• Victim-operated phishing attacks used to distribute malware that disables or destroys the IoT device (i.e., “bricking” is an effective way to disrupt operations before, during and after an attack). Many malware sandboxing technologies can’t be installed on the IoT devices’ operating system.
Network Denial of Service	Adversaries may perform network denial of service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on.	• As part of a large botnet, compromised IoT devices are used to launch DoS attacks due to the high-volume, distributed nature of the devices.

Zero Trust Capability Model

Now that we've covered examples of the tactics, techniques and procedures (TTPs) that are used to exploit common attack vectors across IoT and IT systems. We will now discuss applying the principles of zero trust. This section provides an illustrative example of a zero trust capability model, describes how to tailor to an IoT initiative using a four-step process and explains best practices.

Verizon developed the zero trust capability model (ZT Capability Model) described in this document based on multiple industry, government and/or technology partner guidelines. The ZT Capability Model is the foundation of this document and the subsequent sections of this document describe how to use this model to apply the principles of zero trust to IoT security initiatives.

Table 2 depicts the ZT Capability Model with 8 ZT pillars and 48 ZT Capabilities. The ZT pillars are the black boxes organized horizontally. The ZT capabilities are organized vertically to each ZT pillar.

> Note: Your organization may be required to use a different model for zero trust that would take precedence over the model outlined in this paper.

Table 2: Zero trust capability model

Core pillars

	User	Device	Network	Infrastructure	Application	Data	Visibility and analytics	Orchestration & automation
Core capabilities	Access management	Vulnerability management	Zero trust architecture	Cloud workload protection	Web application firewall	Encryption	Device visibility	Policy engine
	Authentication	Device security	Software-defined networking	Cloud-access security broker	Application security	Data security	Threat intelligence	Policy administrator
	User & entity behavior analytics	Device identity	Segmentation	SaaS management platform	Container security	Data spillage	Security information event mgmt	Policy enforcement point
	Identity management	Device compliance	Network security	Secure access service edge	Secure access cloud	Information rights management	CDM system	Security policy management
	Conditional access	Device authentication	Zero trust network access		Isolation	Data loss prevention		
	Dynamic risk scoring	Device management	Network access control		Any device access	Industry compliance		
		Device inventory	Transport encryption			Integrity		
		Enterprise mobility management	Session protection			Classification		

Executing a 4-step process using zero trust architecture

Step 1:

Establish baseline of current capabilities.

The first step of the zero trust IoT initiative is to establish a baseline of your organization's current capabilities using a simple color-coded schema to represent the capabilities that you currently meet, partially meet and do not meet (i.e., your current mode of operation (CMO).

Table 3 illustrates a notionally populated version of the ZT Capability using a color-coded schema where green means "Met," yellow means "Partially met," and red means "Not met."

Table 3: Zero trust capability model—capability coverage (notional)

🟩 Met 🟨 Partially met 🟥 Not met

Core pillars

Core capabilities

User	Device	Network	Infrastructure	Application	Data	Visibility and analytics	Orchestration & automation
🟨 Access management	🟥 Vulnerability management	🟨 Zero trust architecture	🟨 Cloud workload protection	🟨 Web application firewall	🟨 Encryption	🟥 Device visibility	🟨 Policy engine
🟨 Authentication	🟨 Device security	🟨 Software-defined networking	🟥 Cloud-access security broker	🟨 Application security	🟨 Data security	🟨 Threat intelligence	🟨 Policy administrator
🟨 User & entity behavior analytics	🟨 Device identity	🟥 Segmentation	🟨 SaaS management platform	🟨 Container security	🟨 Data spillage	🟥 Security information event mgmt	🟥 Policy enforcement point
🟨 Identity management	🟨 Device compliance	🟨 Network security	🟥 Secure access service edge	🟨 Secure access cloud	🟨 Information rights management	🟨 CDM system	🟥 Security policy management
🟥 Conditional access	🟨 Device authentication	🟥 Zero trust network access		🟥 Isolation	🟥 Data loss prevention		
🟥 Dynamic risk scoring	🟥 Device management	🟨 Network access control		🟥 Any device access	🟨 Industry compliance		
	🟨 Device inventory	🟨 Transport encryption			🟨 Integrity		
	🟨 Enterprise mobility management	🟨 Session protection			🟥 Classification		

Step 1:

Establish baseline of current capabilities.

Recommendations:

Every project or initiative has a starting point. Look to gather the right people, set the right timelines and be realistic with goal setting. The below points break out recommendations on how to frame the beginning of the zero trust project.

1. Stakeholders—Assemble a team of cross-functional expertise in order to establish zero trust as an enterprise-wide initiative (e.g., Security, IT Operations, Finance, etc.). If security protocols touch a group or department's work product, then it can be assumed they should be represented as a stakeholder.
2. Timeline—Ask the team to participate in two time-boxed meetings. The first meeting should consist of gathering team input resulting in a partially populated capability model. Consider a bulletin board or computer program allowing sticky notes with pillars and applications that you can move around and prioritize as a group. The second meeting should result in a completed and agreed upon capability model and timeline to revisit the model to track progress (e.g., quarterly, bi-annual, annual).
3. Deliverables—Produce 10 slides. The slide deck should comprise of a one slide executive summary, one slide with the color-coded model and eight slides that provide the definition of each pillar and each capability that maps to that pillar.
4. Priorities—Do not worry about prioritizing the pillars and capabilities at this step. Just capture the components specific to your organization under pillars.

Note: Priorities will surface during Step 1 but be codified in Step 2.

Step 2:

Prioritize the ZT Capability Model to your zero trust IoT gaps.

The second step is to align the pillar and capabilities specifically to your IoT initiative based on the findings from the previous step. The purpose of this step is to align and organize the ZT Capability Model with your IoT priorities. Table 4 provides a notional illustration of the output of this step.

- The eight pillars have now been reorganized from left to right, with the device pillar listed first in order to depict the importance of the IoT devices.
- The capabilities have been reorganized into the 3 color-coded "buckets" to illustrate the top priorities by capability. The primary priorities are in red and the secondary priorities are in yellow.

Table 4: Top priorities by pillar (notional)

Core pillars

🟩 Met 🟨 Partially met 🟥 Not met

Core capabilities

Device	Network	Infrastructure	Visibility and analytics	Application	User	Data	Orchestration & automation
🟥 Vulnerability management	🟥 Zero trust network access	🟥 Secure access service edge	🟥 Device visibility	🟥 Isolation	🟥 Dynamic risk scoring	🟥 Data loss prevention	🟥 Security policy management
🟥 Device management	🟥 Segmentation	🟥 Security information event mgmt	🟥 Threat intelligence	🟥 Any device access	🟥 Conditional access	🟥 Industry compliance	🟥 Policy enforcement point
🟨 Device inventory	🟨 Software-defined networking	🟨 Threat intelligence	🟨 Security information event mgmt	🟨 Secure access cloud	🟨 User & entity behavior analytics	🟨 Classification	🟨 Policy administrator
🟨 Device compliance	🟨 Transport encryption	🟨 Secure access service edge	🟨 CDM system	🟨 Application security	🟨 Identity management	🟨 Data spillage	🟨 Policy engine
🟨 Device security	🟨 Session protection			🟨 Web application firewall	🟨 Access management	🟨 Data security	
🟨 Device identity	🟨 Network security			🟨 Container security	🟨 Authentication	🟨 Encryption	
🟨 Device authentication	🟨 Network access control					🟨 Information rights management	
🟨 Enterprise mobility management	🟨 Zero trust architecture					🟨 Integrity	

Recommendations:

1. High priorities – Limit the highest priorities (i.e., in red) to the top two capabilities by pillar. These are priorities you want to accomplish first because of constraints (e.g., budget).
2. Solution convergence – Modern solutions converge many of the capabilities into a single platform resulting in a "domino effect" that turns many of the capabilities "green" (e.g., secure access service edge (SASE).

Note: Your organization may have more than two red priority capabilities based on the nature of your business model. Keep in mind everything can't be red and a priority. And on the contrary, there could be just one priority capability.

Step 3:

Map potential supplier services to zero trust IoT priorities.

Your organization may have a good feel for the inner workings of your business processes, but how does that model take into account multitudes of suppliers who may plug into your model? After completing the prioritization activity, the next step is to evaluate how your organization and suppliers can address the top gaps identified in the previous steps. More simply stated, this is a way to determine if a supplier can help you move from "red" to "green."

Table 5 is a notionally populated illustration that can be used to evaluate a supplier's capabilities to determine if they can meet your gaps. You can send this template to your suppliers without the service offerings and consumption model populated, and then have your supplier populate the answers.

- The top two capability gaps by pillar are color-coded in dark gray.
- The gray box below the capability gaps contains two sections titled: "Service offerings" and "Delivery model."
- Service offerings are the names of the supplier's services that map to one or more of the capability gaps.
- The consumption model is used to note the delivery model of the supplier's offering. "Managed" means the offering is a managed service. "Consulting" means there are consulting and/or professional services involved in the supplier's service. "Resell" means the supplier resells an original equipment manufacturer (OEM) product without managed or consulting services attached. "Caveats" means there are additional considerations for discussion.

Note: For the purposes of this model, a supplier is defined as a provider of services, solutions and equipment in support of the network infrastructure.

Table 5: Supplier service offering mapped to zero trust IoT priorities (notional)

Core pillars

	Device	Network	Infrastructure	Visibility and analytics	Application	User	Data	Orchestration & automation
Core capabilities	Vulnerability management	Zero trust network access	Secure access service edge	Device visibility	Isolation	Dynamic risk scoring	Data loss prevention	Security policy management
	Device management	Segmentation	Security information event mgmt	Threat intelligence	Any device access	Conditional access	Industry compliance	Policy enforcement point
Service offerings	• Vulnerability management service (VMS) for vulnerability management • IoT device management service for device management • Security service edge (SSE) for device management	• Security service edge (SSE) for zero trust network access • Security service edge (SSE) for segmentation • Software-Defined Wide Area Network (SD-WAN) for segmentation	• SSE for secure access service edge (SASE) • SD-WAN for SASE • SSE for cloud access security broker	• IoT device management service for device visibility • SSE for device visibility • Security information and event management (SIEM) for device visibility	• SSE for isolation • SSE for any device access	• SSE for dynamic risk scoring • SSE for conditional access • VMS for dynamic risk scoring	• SSE for data loss prevention • IT risk assessment for industry compliance • Penetration testing for industry compliance	• SSE for security policy management • IoT device management service for device management • SSE for policy enforcement point
Delivery model	**Managed:** Yes **Consulting:** Yes **Resell:** No **Caveats:** Yes	**Managed:** Yes **Consulting:** Yes **Resell:** No **Caveats:** Yes	**Managed:** Yes **Consulting:** Yes **Resell:** No **Caveats:** Yes	**Managed:** Yes **Consulting:** Yes **Resell:** No **Caveats:** Yes	**Managed:** Yes **Consulting:** Yes **Resell:** No **Caveats:** Yes	**Managed:** Yes **Consulting:** Yes **Resell:** No **Caveats:** Yes	**Managed:** Yes **Consulting:** Yes **Resell:** No **Caveats:** Yes	**Managed:** Yes **Consulting:** Yes **Resell:** No **Caveats:** Yes

Step 3:

Map potential supplier services to zero trust IoT priorities.

Recommendations:

1. Caveats—When evaluating supplier solutions (existing and new), discuss caveats to their service offerings to determine the impact to your requirements. For example, if you require a FedRAMP Authorized solution, identify if the supplier's service offering meets that requirement.

2. Mapping—Limit the supplier's mapping of their service offerings in your first discussion to their top 3 service offerings per core pillar. This approach will help keep the conversation narrowly focused on your priorities instead of their capabilities, which they may broaden to gain a further foothold in an organization. If the supplier cannot meet your top priorities now or in the very near future (i.e., color-coded red), they may not be able to meet your secondary or tertiary priorities (i.e., color-coded amber).

3. One-to-many ZT capability mapping— If a supplier's services meet your top priorities (i.e., color-coded red, "Not met"), then have the supplier complete the same mapping to your secondary and tertiary priorities (i.e., color-coded amber, "Not met"). This activity will result in identifying the supplier's solutions that map to the rest of the ZT Capability Model.

Note: Your organization may need to be ready from a budget standpoint to fund gaps within the model that were not accounted for originally, including the enablement of new functionality that exists in preexisting platforms. Additionally, you may identify capabilities in preexisting platforms that can be enabled without additional budget.

Step 4:

Map solutions to threat types and assign zero trust maturity levels.

After completing the mapping solutions and technology platforms to your priorities, it is vital to begin mapping out the different types of attacks your organization may receive to the identified pillars and capabilities. The next steps are listed below.

Table 6 illustrates a notionally populated example of the output.

- Maps TTPs from the MITRE ATT&CK framework to your solutions.
- Provide a brief description of the key components of the solution.
- Map the solutions to the primary ZT pillar and ZT capability addressed.
- Determine how the solutions improve your zero trust maturity level—the current mode of operation (CMO) is your current maturity level without the solution. The future mode of operation (FMO) is the maturity level you will achieve after implementing the solution(s).

Table 6: Mapping of solutions to attack types with zero trust maturity level assignment

MITRE ATT&CK	Solution	Pillar	Capability	CMO	FMO
Exploitation for client execution	• Perform vulnerability scans on 100% of IoT devices • Perform vulnerability scans on a scheduled basis • Remediate vulnerabilities on a continuous basis	Device	Vulnerability management	**Not met**	**Met**
External remote services	• Deploy security service edge (SSE) solution • Remove virtual private network (VPN) hardware • Enable conditional access in SSE solution with MFA	Network	Zero trust network access	**Not met**	**Met**
Lateral tool transfer	• Implement microsegmentation using SSE solution • Restrict traffic flows with SSE-based FW, IDS/IPS • Implement 5G network slicing for IoT networks	Network	Segmentation	**Not met**	**Met**
Hardware additions	• Continuously track and reconcile IoT assets in CMBD • Perform asset discovery with vulnerability scanners • Deploy NAC to block unapproved hardware additions	Visibility & analytics	Device visibility	**Not met**	**Partially met**

Step 4:

Map solutions to threat types and assign zero trust maturity levels.

Table 6 (cont.)

MITRE ATT&CK	Solution	Pillar	Capability	CMO	FMO
Exfiltration over alternative protocol	• Disable protocols on IoT devices pre-deployment • Implement DLP controls on all IoT networks • Perform continuous vulnerability scans	Data	Data loss prevention	**Not met**	**Met**
Exfiltration over other network medium	• Perform event logging on IoT networks into SIEM • Monitor and analyze IoT network traffic • Implement user and entity behavior analytics (UEBA)	Visibility	Security information and event management	**Not met**	**Met**
User execution	• Perform malware sandboxing with SSE solution • Configure cloud access security broker (CASB) prevent unsanctioned cloud use • Deploy application control to block executables	Application	Isolation	**Not met**	**Partially met**
Network Denial of Service (DoS)	• Implement microsegmentation using SSE solution • Enable DDoS protection in SSE for outbound traffic • Deploy DDoS protection for inbound traffic	Network	Segmentation	**Not met**	**Met**

Recommendations:

1. Solution convergence—Step #4 is where your organization will identify and document the one-to-many mapping from a single solution to multiple ZT pillars and ZT capabilities. For example, a security service edge (SSE) solution addresses multiple ZT capabilities across Multiple ZT Pillars.
2. Cross-pillar capabilities— Although there is typically a one-to-many mapping of solutions to the ZT Capability Model (i.e., cross-pillar capabilities), assign one solution to one ZT pillar and one ZT capability; this will likely mean listing a solution more than once. This approach helps streamline your organization's efforts, prioritizes your approach and makes the output of the exercise more easily consumable for audiences that may not have extensive knowledge about zero trust and/or IoT security.
3. Frameworks—The framework chosen for this white paper was the MITRE ATT&CK framework because of the wide industry adoption, the applicability of the TTPs to IoT and the compatibility with the concepts of zero trust.
4. Acronyms—The acronyms used but not defined in the document are: firewall (FW), intrusion detection system/intrusion prevention system (IDS/IPS), configuration management database (CMDB), data loss prevention (DLP), network access control (NAC), security information and event management (SIEM), cloud access security broker (CASB).

Helping your organization be better protected.

Closing

In the opening paragraph of this paper, we noted the recent story of an unfortunate US healthcare provider who was hacked at the convergence of IoT and IT, a convergence that is growing exponentially across all industries and sectors.

Many organizations are deploying IoT devices throughout their facilities and networks and they must protect themselves from disruption as well as loss of data, reputation and money. In this paper, we discussed a comprehensive approach based on a Zero Trust Capability Model:

1. Establish baseline of current capabilities
2. Prioritize the capability model to your IoT gaps
3. Map potential supplier services to IoT priorities
4. Map solutions to threat types and assign maturity levels

The model outlined in the paper is a solid, realistic and executable approach to helping your organization be better protected from IoT-focused cyber threats. Additionally, the steps described in this model sets the stage for your organization to iterate and track progress at a frequency that fits your needs (e.g., quarterly).

Verizon believes the model can be understood by all stakeholders and implemented effectively.

Why Verizon?

Verizon Cyber Security Consulting is a global leader with a security team of over 600 consultants in 30 countries.

Verizon's security consulting provides clients with solutions to identify, protect, detect, respond, and recover from cyber threats. Verizon's approach to cybersecurity is comprehensive, helping organizations reduce risks and defend against cyber threats. The consulting services team is dedicated to delivering excellence and staying ahead of the ever-changing landscape of cyber security, helping customers with their transformation. By utilizing advanced technologies and industry-leading practices, Verizon's security consulting services help organizations Implement and deliver complex solutions to achieve the desired level of risk.

Services range from advisory to ongoing management services, covering next gen cyber defense, enterprise security for zero trust networking and SASE, IT and application security services, and security operations incident response and security tools lifecycle management.

Verizon contributors

Wes Withrow, Public Sector Solutions Executive

Ashish Khanna, Director, Security Consulting Services

Brett Barganz, Solutions Executive, Connected Healthcare

Grant O'Brien, Manager, Federal/Defense Marketing

Many organizations turn to a capable partner like Verizon on their journey to zero trust for IoT.

If you would like assistance, visit our Zero Trust Dynamic Access web page.

verizon✓