Enterprise Strategy Group | **Getting to the bigger truth.™**

Solution Showcase

Forescout: Ensuring Business-centric Device Visibility Across the Extended Enterprise

Date: April 2019 **Author:** Jon Oltsik, Senior Principal Analyst and ESG Fellow

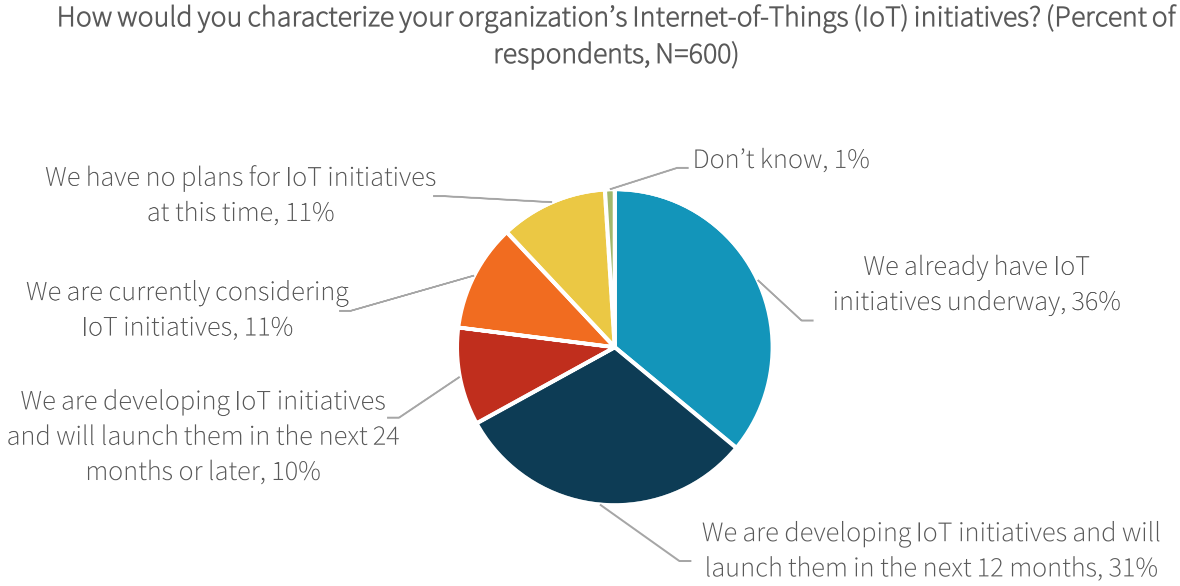
Abstract: CISOs are responsible for enabling digital transformation (DX) priorities in support of a variety of business initiatives, allowing managers to view key operations data across an array of IT and OT networks (e.g., the extended enterprise) that can be used to drive business decisions and innovation. Yet, they face a major challenge: Many firms struggle to discover, assess, and control network-enabled devices that anchor these DX projects. Knowing which policies and cybersecurity controls to apply to a device requires continuous and in-depth device visibility from both a technical and business context. Organizations typically employ a variety of tools to achieve this goal. However, the visibility provided is often limited, inconsistent, and only relevant to a single point in time. What's needed? New device visibility solutions that capture detailed technical and business context that can enable business-centric visibility.

Enterprises Lack the Right Level of Device Visibility

With the proliferation of digital transformation initiatives, various technologies now serve as anchors for business processes. This transition is often supported by a variety of new device types—including devices connected to the Internet of Things (IoT)—in industries such as health care, retail sales, and manufacturing. According to ESG research, 36% of IT decision makers report their organizations have IoT initiatives underway, 31% are developing them for the next 12 months, and 10% are planning IoT initiatives for the next 24 months or later (see Figure 1).[1]

[1] Source: ESG Research Report, *2019 Technology Spending Intentions Survey*, February 2019.

Figure 1. IoT Initiative Plans



Source: Enterprise Strategy Group

As part of these DX and IoT initiatives, CISOs are expected to oversee the protection of a diverse set of network-enabled devices (physical and virtual) deployed across extended enterprises including corporate campuses, on-premises and remote data centers, public and private clouds, and OT networks. These network-enabled devices connect/disconnect with increasing frequency. In addition, changes in device posture and user roles are ongoing. To accurately understand the proper business context, mitigate risk, and apply the right security controls, cybersecurity teams need current and detailed information about all devices, including unmanaged IoT devices, all the time. As such, there is a need for continuous monitoring to capture the detailed device functionality necessary to satisfy emerging business and technical requirements.

Basic Device Visibility Is Not Enough

Historically, a variety of tools were used to discover network-enabled devices across an extended enterprise. This might lead one to assume that organizations get an appropriate level of business and technical visibility. In truth, the state of device visibility is totally inadequate, as an explosion in device diversity has spawned new categories of tools to manage mobile, virtual, cloud, and IoT systems – many of which remain invisible to administrators.

Traditional tools tend to discover, classify, and inspect devices in isolation—if they can even find them. They often use network packets or device-based agents to get a cursory understanding of each discovered device but rarely furnish the level of detail required to determine true situational awareness. This "bottom-up" approach can capture limited data about devices and the networks to which those devices are attached but provides no notion of application flows or the business processes that depend upon communications between multiple devices—data required to achieve business-centric visibility.

Additionally, CISOs often base their cybersecurity efforts on point-in-time assessments that do not reflect their current state of security. They don't know what devices are or are not connected to their network, the function of those devices, the role they play within interconnected systems, or how changes to those devices may impact the organization's overall security profile. These conclusions are validated by ESG risk management research that looked at both the timeliness of the device data and the completeness of the asset inventory from which the data is captured.

- **Cyber risk management is based upon periodic reviews rather than continuous monitoring.** Nearly two-thirds of organizations do baseline assessments, but this data is only valid at a particular point in time.[2] Thus, risk management decisions are often based upon historical (and potentially inaccurate) information rather than current data. This is at odds with the previously stated need for organizations to monitor devices on a continuous basis.
- **Organizations don't have a complete inventory of the assets on their networks.** Alarmingly, this lack of asset accounting applies to 63% of organizations.[3] And without a full and accurate picture of the assets on their networks, including every asset's current security state, CISOs can't communicate precise risk metrics to business executives and they can't implement the set of security controls necessary for effective risk mitigation.

At best, this bottom-up approach and the data it captures yield limited results, especially with the onslaught of new devices used to support DX initiatives. Given these limitations, cybersecurity teams are forced to rely on multiple siloed tools to assess what is on their networks, gather data about each device, translate this data into business risk, and then guess at what types of cybersecurity controls are needed. This piecemeal approach is inadequate when dynamic business processes depend upon device communications across an extended enterprise. CISOs should take note: Gluing together tools and guessing about the state and role of devices leaves organizations susceptible to significant levels of cyber risk.

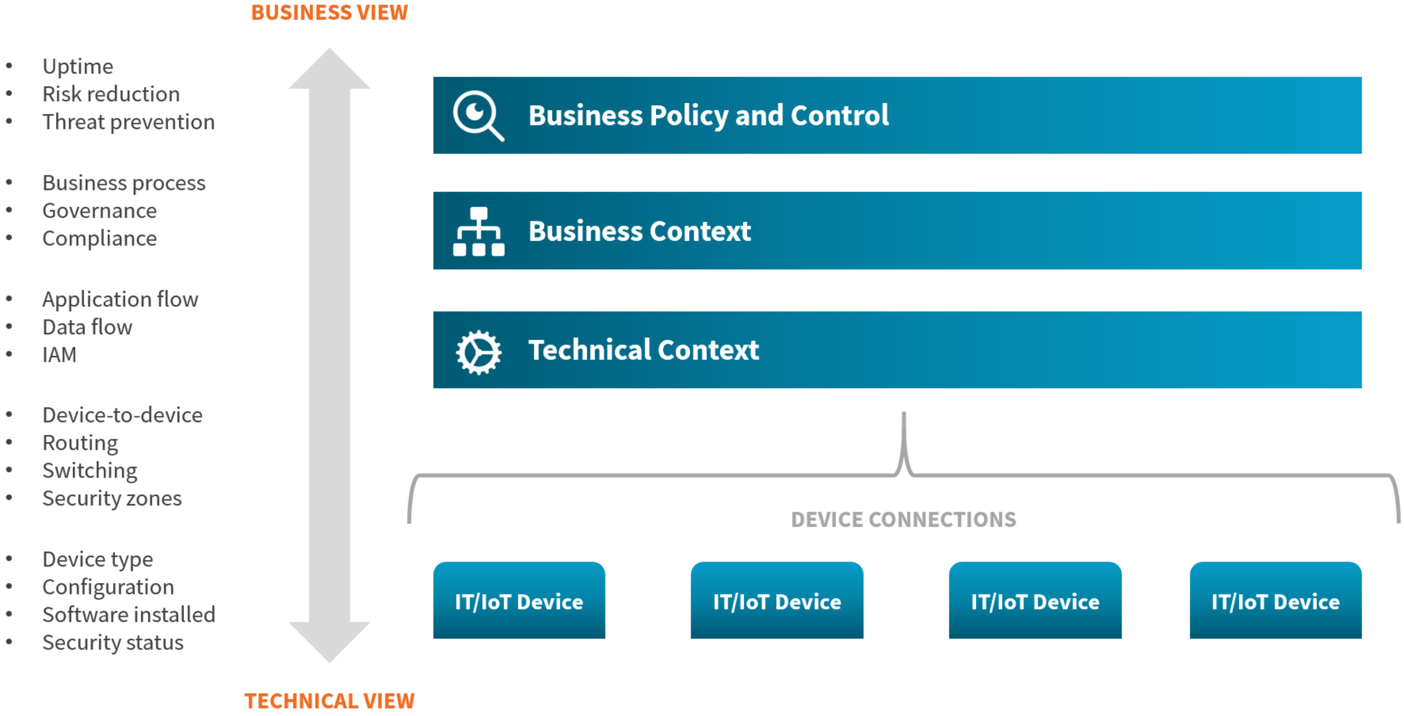
Organizations Need Business-centric Visibility

Most device detection solutions take either a bottom-up or top-down approach to device visibility. As previously described, the bottom-up visibility model starts with devices. Depending on the solution, it may provide lots of technical detail but limited (if any) business context. In contrast, a top-down approach starts at the business process to which a device is connected but has limited (if any) technical context.

CISOs need a new solution that combines the technical context provided by a bottom-up approach with the business context enabled by a top-down approach. This combination can provide business-centric visibility that aligns individual devices to the business applications and processes used in support of DX initiatives.

[2] Source: ESG Master Survey Results, *The Pressing Need for Comprehensive Cyber Risk Management*, March 2019.
[3] ibid.

Figure 2. Business-centric Visibility



Source: Enterprise Strategy Group

As seen in Figure 2, business-centric visibility requires detailed data regarding the devices discovered, their connections, and both technical and business context—a level of visibility that can be used to assign business policies and cybersecurity controls to reduce cyber risk as well as improve threat prevention and uptime. This device information should be available via a central management console that also supports a variety of management and technical reports. Specific information that needs to be captured may include:

- Devices: Need to identify the type (PC, tablet, IoT, OT, virtual devices, cloud instances, etc.) and device hygiene (software installed, patches available, passwords, configuration, power, etc.) as well as software and OS update status. In other words, organizations need a deep and continuous understanding of all devices on the network.

- Device connections: Need to understand to what and where the device is connecting: device-to-device, wired and wireless routing/switching, VLANs, security zones, etc. This view starts to divide devices into logical groups of devices that need to communicate.

- Technical context: Need to understand how the device is engaged from a technical perspective: application flows, data flows, protocols, identities, etc. This view can help organizations understand how devices communicate and can help them think about cybersecurity controls like network segmentation and application whitelisting.

- Business context: Need to understand how the device is engaged from a business perspective: business processes enabled, user/unit owner, compliance/governance, applications to which they are connected, etc. This layer can help map device communications into business processes. Visibility at this level can help organizations understand what should happen, giving them the knowledge to block what shouldn't happen.

- **Central control and reporting:** Need to ensure that all devices can be centrally managed and controlled (ability to apply policies and patches to devices, segment networks, etc.), and provide both technical- and management-level reporting required to support risk management, compliance, etc.

Business-centric visibility can be used by CISOs and their staffs to provide business managers with real-time data to help prioritize risk mitigation decisions and ensure that the cybersecurity budget is spent wisely. This information can also help the compliance/governance functions become part of a well-run cyber risk management practice rather than check-box exercises that stand on their own. Finally, business-centric visibility can help increase the productivity of security operations, where real-time data is used as a guide to prioritize actions and govern best practices.

The Path to Business-centric Visibility: CISO Considerations

While all vendors claim to provide visibility, their definitions vary, with most offering solutions that can only capture and deliver a limited set of bottom-up (technical) or top-down (business) data.

To avoid confusion or missteps, CISOs (and others) should consider the following questions when evaluating solutions for discovering, assessing, and controlling devices. The goal here is to provide a consistent and complete inventory and accounting of devices deployed as well as the risk information required by business management. As they consider technical solutions, CISOs should ask:

- **Do I have sufficient detail for *all* connected devices?** Demand the ability to quickly capture the appropriate level of detail across devices to enable consistent application of policies and security controls.

- **Are device details, including changes in device state, continuously up to date?** The ability to accurately assess and mange business risk requires a real-time understanding of device context rather than point-in-time snapshots that may no longer be relevant.

- **Can I aggregate all visibility tools into a common view?** True device visibility can only be accomplished when all devices can be viewed with the same level of detail and context.

- **Can I view network connections from end to end in a business-process context?** It's essential to have contextual insight into asset ownership, system ownership and access rights/responsibilities. This view is necessary to understand network connections across security zones as well as the business processes combining multiple devices.

- **Do I have a central view of visibility that can be used to establish controls for risk reduction, real-time governance/compliance, and improved security operations?** A view of all devices that provides both technical and business context will enable business-centric visibility and well-informed risk mitigation decisions.

- **Can I see virtual machines (VMs) and cloud instances being spun up?** VMs (and other types of workloads) are being used on an increasing basis. It is important that they be included as part of an overall view into devices deployed across an extended enterprise.

Business-centric visibility represents an architecture where data is collected, processed, and shared through technical integration. It can dissolve technology silos and multiply the benefits of visibility across an organization's IT management and security investments. To facilitate this, business-centric visibility tools must be built using open APIs, while leading vendors will form technology ecosystems for partner integration.

Enter Forescout

While device detection vendors claim to provide comprehensive visibility for network-enabled devices, many offer little more than an incomplete bottom-up or top-down view for a limited set of devices. One exception to this rule is Forescout and its unified device visibility and control platform for IT and OT networks. Forescout can help organizations continuously discover, classify, and assess devices to gain situational awareness and reduce risk.

Forescout brings an agentless approach to device discovery that can help address the challenges of endpoint visibility and control in large, dynamic, and diverse environments. Using a combination of active and passive discovery techniques, the Forescout platform can identify IP-enabled (wired or wireless) devices the instant they connect to a campus, data center, cloud, or OT network—without an agent installed on the device. These devices can be either managed or unmanaged, corporate or personal. Device types include traditional computing systems, mobile devices, IoT devices, network peripherals, network infrastructure components, OT devices and infrastructure components, rogue or hacker-impersonated hardware, and other network-enabled physical or virtual devices. In addition, Forescout now extends its agentless visibility and network-based situational awareness deeper into OT and industrial control system (ICS) environments through deep packet capture/inspection of 100+ IT/OT protocols and various risk-assessment capabilities.

After discovering a connected device, Forescout attempts to classify the device (using its large and growing device fingerprinting database), and then gathers detailed information about device type, function, operating system, vendor, and model. It then assesses users as well as applications, other types of software (including patch levels), etc., that provide both technical and business context. Forescout has engineered an approach to agentless discovery that does not limit its ability to collect detailed information about either the device or the ecosystem in which it is attempting to operate. Forescout then assesses the security and compliance posture of each device against policy, including native IT and OT vulnerability checks. It can allow, deny, or restrict access to internal network resources through multiple control options, issue notifications, and initiate remediation—directly or through tight integrations with security and IT management technologies—based on established policies and discovered security state. In this way, Forescout can provide comprehensive business and technical insight without disrupting critical business processes.

The Bigger Truth

Cyber risk continues to escalate with the introduction of large numbers of network-enabled devices supporting DX initiatives. These devices often remain unknown, unmanaged, or insecure because current visibility solutions are incapable of identifying various device types and only provide a limited amount of point-in-time visibility regarding the devices that are detected. This situation is a mismatch for measuring and mitigating cyber risk in a timely fashion.

To address these challenges, CISOs need to employ business-centric visibility solutions that can continuously discover, classify, and assess the health and hygiene of a heterogenous mix of IT and OT devices across environments, data centers, hybrid clouds, and OT networks. Solutions should support the discovery of all devices, collect the data required to provide the technical and business context ,and provide business and technical staff with central command and control for policy management, configuration management, policy enforcement, and reporting. In this way, business-centric visibility can help improve security efficacy, operational efficiency, and business enablement. Forescout is one of few vendors whose solution can align with these new requirements.