

Device Security

Challenges & Use Cases



Considerations

Who are you?	Who owns your device?	What type of device?	Where/how are you connecting?	What is the device hygiene?
<ul style="list-style-type: none"> • Employee • Partner • Contractor • Guest 	<ul style="list-style-type: none"> • Corporate • BYOD • Rogue 	<ul style="list-style-type: none"> • Windows, Mac • iOS, Android • VM • Non-user devices, IoT 	<ul style="list-style-type: none"> • Switch/ • Port/PoE • Wireless/Controller • VPN • IP, MAC • VLAN 	<ul style="list-style-type: none"> • Configuration • Software • Services • Patches • Security Agent

Challenges - You can't effectively control what you can't effectively see

Regulatory compliance and complying with business policies and industry/government mandates is an ongoing challenge. Security audits highlight areas of concern, and the clock starts ticking the moment shortcomings are identified.

Explosive growth of devices and platform diversity

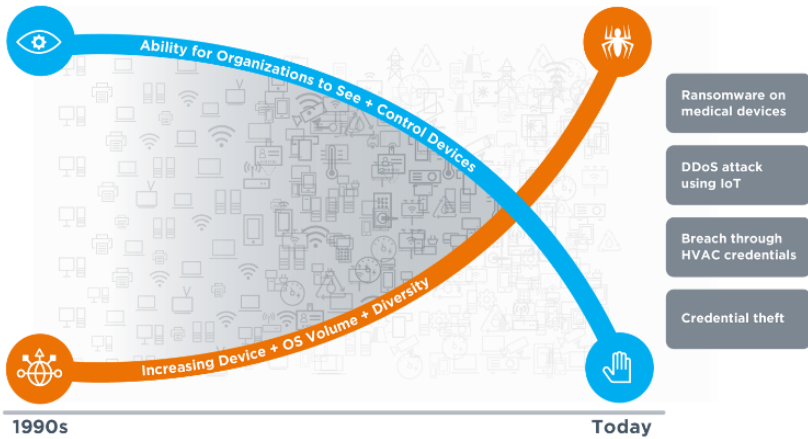
Increasing numbers of IoT and mobile computing devices has resulted in a much larger attack surface and created network blind spots rendering agent-based security methods ineffective.



- Innumerable device-specific operating systems (OS).
- Cannot get agents onto new devices.
- Cannot write agent-based software for every OS.

Siloed security creates gaps and delayed incident response. Large enterprises have dozens of security systems, yet, on average, fewer than three of them share security insights. This disjointed approach prevents a coordinated, enterprise-wide security response, allowing attackers more time to exploit vulnerabilities.

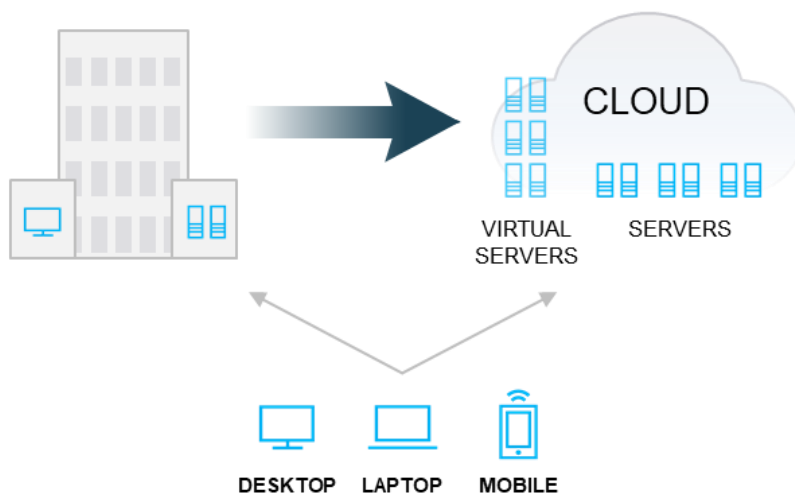
Widening IoT visibility gap with attackers taking advantage of the much larger attack surface.



- IoT & OT networks are no longer physically separated.
- Threats moving between cyber and physical dimensions.
- Assets are highly vulnerable and rarely can be patched.

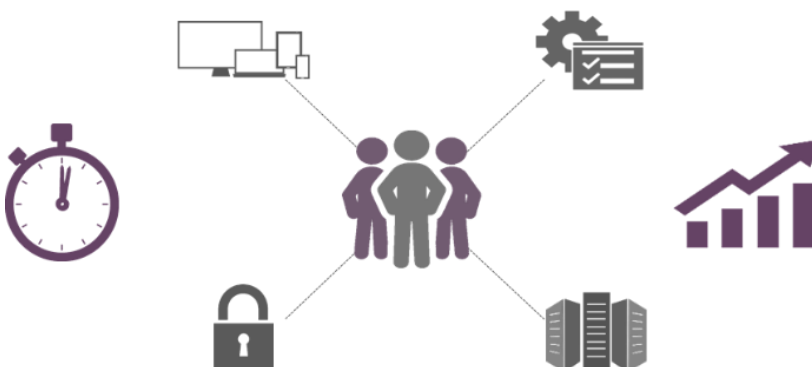
Cloud adoption creates new challenges and further reduces visibility. The disappearing enterprise perimeter, increase in virtualization technology and movement of workloads to the public cloud have resulted in decentralized management of IT assets as more people have direct access to virtual and cloud-based resources.

DATA CENTER



- Multiple device locations and access points.
- Heterogeneous environment with multiple vendors.
- De-centralised management.

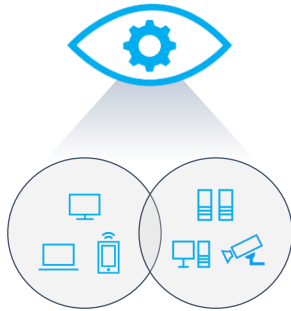
Competing demands on IT time & resource often results in tasks and projects being continually reprioritised and due to technology investments needing to be sweated for longer aligned with budget constraints, compromises are common.



- Skills shortage.
- Reactive IT work outweighs development.
- Projects undertaken autonomously versus cohesively, result in lost return on investment (ROI).

Use cases

Network Asset Management



Key Challenges

- Incomplete and accurate asset data.
- Inability to discover transient, IoT and BYOD devices.
- Incident turnaround and mean time to repair.

Key Benefits

- Drive audit and compliance success.
- Reduce labour required for asset discovery.
- Reduce unused software license costs.

Endpoint Compliance



Key Challenges

- Constantly changing configurations diverge from company standards.
- End users accepting poor performance as normal.
- Unable to locate known vulnerabilities.

Key Benefits

- Poor performance issues quickly identified.
- Rich reporting, helps identify shadow IT.
- Proactive, delivering better quality of service to users.

Continuous Monitoring



Key Challenges


- Difficult to do real time discovery.
- Lack of automated response.

Key Benefits

- Improve incident response times.
- Minimize threat exposure to the corporate network.

Use cases continued

Incident Response



The diagram for Incident Response features a large blue hand icon at the top. Below it, a laptop icon with a warning triangle is connected by lines to three smaller icons: a person (representing user), a device type (representing device type), and a location pin (representing location).

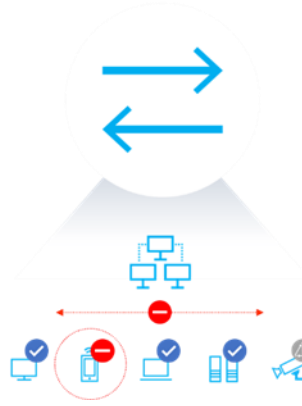
Key Challenges

- Inability to locate system vulnerabilities (i.e. WannaCry)
- Inability to detect and respond quickly to attacks

Key Benefits

- Obtain contextual information (location, user, type of device etc) for vulnerability assessments
- Discover vulnerable systems and respond in an automated way

Network Segmentation



The diagram for Network Segmentation shows a large blue double-headed arrow at the top. Below it, a network diagram with a red circle and a minus sign is connected by lines to several device icons (laptop, smartphone, tablet, server) with checkmarks, and a server icon with a warning triangle.


Key Challenges

- Segmentation isn't dynamic to changing system hygiene
- Segmentation is difficult to manage across heterogeneous infrastructure and environments

Key Benefits

- Stop East West malware propagation
- Ensure device compliance to network policies
- Manage segmentation centrally across different network segmentation technologies

Summary of Benefits



The diagram for Summary of Benefits is divided into four quadrants, each with an icon and a list of benefits:

- 1. Visibility** (Eye icon):
 - ✓ Continuous monitoring
 - ✓ Agentless deployment
- 2. Time-to-Value** (Stopwatch icon):
 - ✓ Rapid installation
 - ✓ Existing IT systems
- 3. Orchestration** (Double-headed arrow icon):
 - ✓ Fragmentation reduction
 - ✓ Automated response
- 4. Professional Services** (Gears icon):
 - ✓ Complementary expertise
 - ✓ Reduced demand on time & resource