Why you need device-level endpoint protection for improving OT security

veridify.com/why-you-need-device-level-endpoint-protection-for-improving-ot-security

Challenges in transferring IT security methods to protect OT devices leave commercial and industrial facilities open to attacks. These attacks can disrupt building or process operations, create safety issues, and result in data theft or ransomware. OT devices in industry 4.0 applications in manufacturing facilities and chemical processing plants are vulnerable to attacks that break automated assembly lines, fracture process control systems, and close plants entirely and possibly indefinitely. These attacks affect productivity, damage capital equipment, and cost building managers and industrial complexes losses in finances. Device-level endpoint protection enables each OT device with self-protection through mutual authentication using a zero trust framework. This secures OT devices in a way that no firewall or microsegmentation solution can.

Risks of Network-Level Security

Network-level security solutions permit cyberattack traffic to flow unabated through building networks and industrial OT applications for manufacturing and process control. Firewalls and microsegmentation are network-level security approaches. Firewalls and microsegments rely on rules-based traffic blocking, network monitoring, and security incident reporting for attacks that have already happened. While these capabilities can be beneficial, network-level protection does not prevent cyberattacks.

Firewalls suffer breaches by nation-states, APTs, and criminal hackers. Firewalls are frequent targets of successful malware attacks. These networked devices block or allow traffic using limited rules-based security.

Even intelligent firewalls only alert when suspected attack behavior reaches a threshold. By then, cybercriminals have come and gone with critical data, compromised building or process controls, or planted malware. Firewalls can’t stop the propagation of malware across files and software. Security gaps in firewalls permit malicious commands to reach devices.

Devices in microsegments are at risk of attack. Microsegmentation focuses on network monitoring for communications between two devices. But attacks across a network reach these microsegments. Network monitoring, whether for the network at large or two OT devices, assumes that the organization learns of attacks after the fact. Microsegmentation can only instantiate optimized network security practices. Breaches of microsegments are inevitable since microsegmentation only detects threats and alerts organizations so they can respond to attacks. Microsegments count on security policies, and attackers break security policies and access unprotected devices.

Firewalls and microsegments require increasing block rules and fine-grained security policies. Because firewalls and microsegments are network-level, they assume the need for traffic monitoring, which must use deep packet inspection and other network-level approaches. Firewalls and microsegments only identify and respond to attacks and don't prevent them. Visibility and monitoring of network assets don't stop attacks; they only enable you to see attacks in progress and report on them.

Benefits of Device-Level Endpoint Protection

Device-level protection is simple, unlike complex firewalls and microsegmentation. Device-level protection enables each building, manufacturing, and process control OT device to protect itself. Device-level identification, authentication, and mutual authentication between devices ensure zero trust security.

Device-level endpoint protection benefits include the following:

- Prevents attackers and attack traffic from connecting or communicating with protected building, manufacturing, and process control OT devices
- Prevents attack propagation through protected endpoints
- Surrounds device communications with advanced encryption tunnels that protect devices today and beyond—when quantum-level attacks appear

Attackers can't establish a device-level presence when device-level endpoint protection secures OT devices. Only identified, authenticated OT endpoints can connect to and communicate with each other, preventing communication from unauthorized devices.

Device-level protection safeguards devices regardless of the network-level protection benefits or weaknesses in microsegments. This prevents cyberattacks, reducing the attack surface by eliminating vulnerabilities. It contains threats and secures devices at the device level rather than via network-level security policies.

Device-level endpoint protection doesn't permit any connections from the internet or direct connections from the cloud and automatically rejects unidentified and unauthorized connections from devices. This enables devices to protect themselves at the edge with real-

time security. Device-level protection keeps OT devices free of remote exploitation as there is no exposure to the internet and only limited indirect access to the cloud.

Operating engineers and network technicians can install device-level endpoint protection for OT security without IT staff or cybersecurity experience.

Veridify's DOME platform provides device-level endpoint protection for OT devices and networks. Schedule a demo.