ManageEngine

ROGUES ON THE RISE:

Is your network secure enough?

www.manageengine.com/products/oputils

Sharon A Ratna

Index

1.You cannot protect what you cannot see

"You cannot protect what you cannot see." This is a common IT parlance that roughly sums up the cause of several network attacks—an unmonitored IT component or application, or a connected user device running malware. Modern IT infrastructures are constantly under attack from several malicious entities trying to access, manipulate, and disrupt an organization's network. Even with vigilant security measures in place to protect the usability, availability, and integrity of networks, most networks are still vulnerable to attacks that seep in through the cracks.

With visibility being a crucial aspect to identify and tackle these attacks, managing shadow IT, IoT devices, and BYOD policies is becoming a nightmare for network security admins working in a challenging threat environment. These assets, which are often connected to the network with genuine motives, might be an infected rogue device.

What your cybersecurity efforts fail to address

In short, rogue devices are the devices connecting to your network under the pretext of being a trusted device while carrying out network attacks, enabling data theft or resource exploitation, and more.

As IT ecosystems scale beyond their manageable capacities into distributed networks and sub-networks, several gray areas emerge in their infrastructure. Most cybersecurity strategies focus on gaining visibility into these areas and protecting the cyber or data processing aspect of the network. While strategies such as deploying firewalls enable organizations to secure the software and transport layers of the OSI network model, they often do not enable visibility in the hardware layers.

These layers are where rogue devices operate. Hidden from software layer security scanners, rogue devices can go undetected by several cybersecurity measures.

Organizations failing to address the hardware layers while setting up their network security measures are exposing their IT infrastructures to the threat of rogue attacks.

2. Going rogue: How your employees become perpetrators of rogue attacks

With the democratization of IT, the procurement, installation, running, and management of several IT components and applications are no longer under the direct supervision of an organization's central IT team. Failing to obtain the perfect balance between being flexible enough for a good employee experience and being rigid enough to avoid network attacks can lead to serious network security issues. It's time to analyze if your flexible IT policies are making your employees perpetrators of rogue attacks!

The "unsuspecting" IT guy

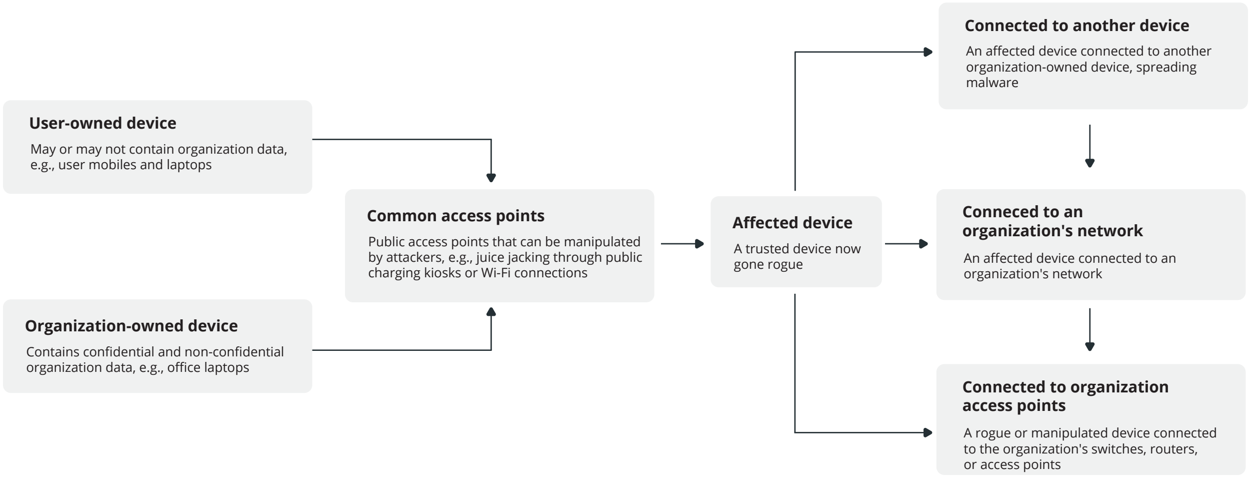
BYOD policies enable organizations to offer a more flexible networking experience for their employees. This means employees are going to connect their own devices to your network access points and consume the organization's networking resources, such as bandwidth and IP addresses. And it's not just that—employees are also going to be accessing and processing the organization's data with these devices.

However, these devices don't have stringent security configurations like they do in an organization-issued device. Attackers don't just exploit device vulnerabilities but also leverage the networking actions of unsuspecting employees to carry out rogue attacks. Your employees might become perpetrators of rogue attacks under some of the following common instances:

- **Public access points:** Connecting a user-owned device or office device to public Wi-Fi or hotspots allows malicious agents to manipulate the device. When connected to an organization device or the organization access points, this user-owned device can easily perpetrate rogue attacks on the organization.

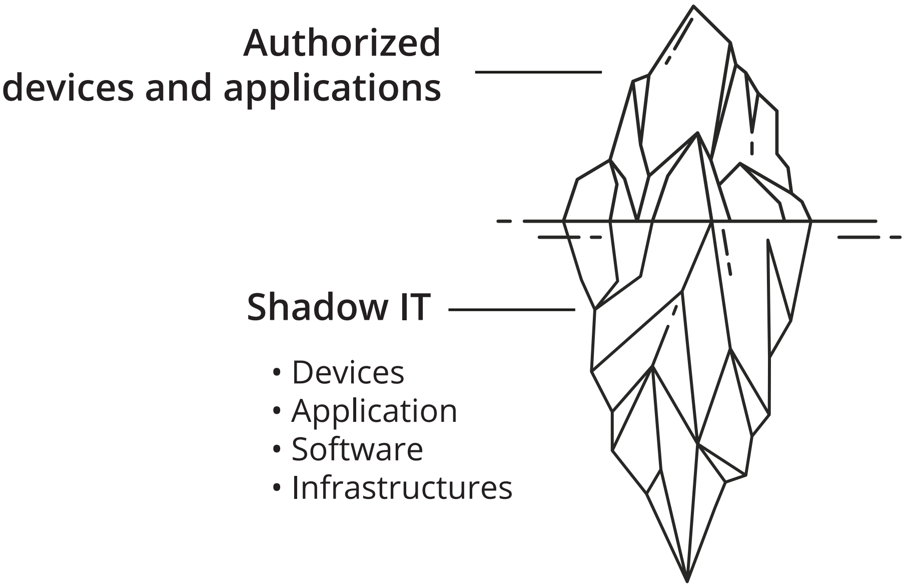
- **Charging kiosks:** Connecting a user-owned device or office device to public Wi-Fi or hotspots allows malicious agents to manipulate the device. When connected to an organization device or the organization access points, this user-owned device can easily perpetrate rogue attacks on the organization.

- **Unmonitored organization access points:** These access points offer a free pass for threat actors to carry out rogue attacks on the organization just by being in a close enough physical proximity.


User-owned device
May or may not contain organization data, e.g., user mobiles and laptops
Organization-owned device
Contains confidential and non-confidential organization data, e.g., office laptops
Common access points
Public access points that can be manipulated by attackers, e.g., juice jacking through public charging kiosks or Wi-Fi connections
Affected device
A trusted device now gone rogue
Connected to another device
An affected device connected to another organization-owned device, spreading malware
Conneced to an organization's network
An affected device connected to an organization's network
Connected to organization access points
A rogue or manipulated device connected to the organization's switches, routers, or access points

Lurking in the shadows

Shadow IT has somewhat become inevitable with the democratization of IT. Some common reasons for the use of shadow IT include increased efficiency, there being an immediate need, approval takes too long, or lack of knowledge about what should or shouldn't be installed. It's important for organizations' IT teams to be aware of all the assets and applications running in their networks, be it an employee's mobile hotspot or the finance team's new server for a quick fix.



You cannot protect what you didn't know you had! Inventory and asset management is crucial to ensuring no rogue device is operating in your network. However, shadow IT is making this an arduous task for several organizations.

Insider threats

While it's true that most of your employees do not willingly or knowingly disrupt your network, business processes, and core functionalities, **you can never be too careful!**

Even in highly secure networks, such as air-gapped networks, an insider can easily aid in rogue attacks. A new USB for data sharing or an additional switch port for extended connectivity are some of the common reasons used by malicious insiders to carry out or aid in rogue attacks.

3. Rogue attacks: Now you see them, now you don't

Rogue devices often do not pop up on your network security scanner. By manipulating the network's hardware layer, these devices can go undetected by software layer firewalls and other security software scanning your network. With shadow or stealth IT still prevalent in many organizations, rogue devices can go undetected even for months before they cause a severe network attack, resulting in huge financial and non-financial losses for organizations.

Common rogue attacks that cripple modern IT

Wireless

With a massive number of devices using Wi-Fi for network connection, rogue AP's threaten the wireless IT infrastructure.

Wired

Critical network communication and data flow happen via wired networks. Rogue switch ports are common enablers of rogue attacks here.

In the "middle"

Man-in-the-middle attacks threaten the confidentiality of network communications established between different network components.

Rogue access points

Wireless rogue access points are one of the biggest challenges for an organization to deal with when trying to minimize rogue attack vectors. Rogue access points can be a conundrum to deal with and identify as a threat, since:

- They can be access points set up by employees for better network connectivity. These access points are called **soft** access points in IT.
- They can be from teams or organizations next door that are accessing your network resources. Since access points do not require wired connectivity, averting these access points becomes challenging.

- Most dangerously, malicious access points set up by network attackers can compromise network security and integrity.

All of these access points should be treated as a threat to network security since they bypass the organization's security protocol.

Attack types: Data theft, traffic and network resource exploitation, and enablers of further attacks including DoS and hacking.

Rogue switches and routers

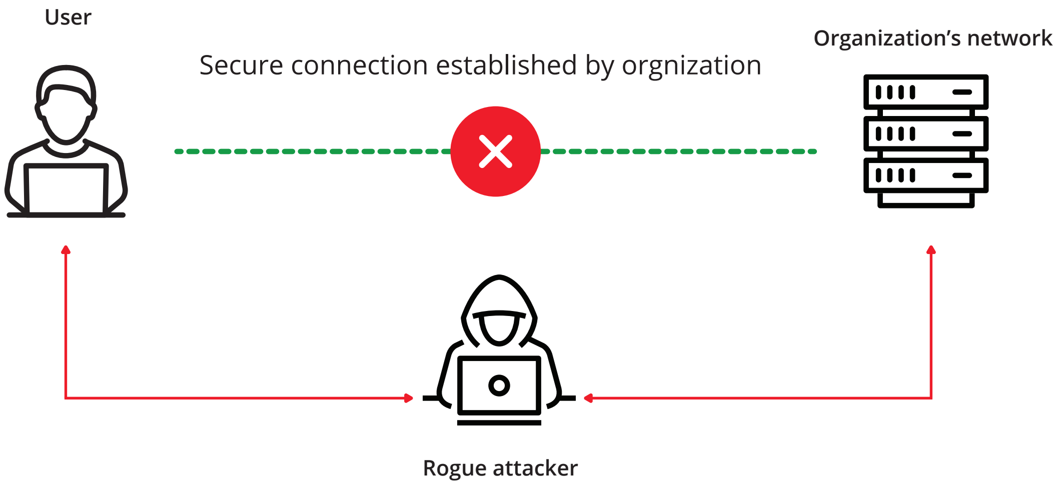
Rogue switches and routers are wired counterparts of rogue access points. While rogue access points can be set up by anyone who can get close enough to the organization's premises, rogue switches and routers require the attacker to be within the organization.

They have a severe impact on the organization's security and integrity. Critical networking information such as MAC IP details in the Address Resolution Protocol (ARP) tables of the switches and routing tables of routers can expose inner networking configurations to the attacker. As the major controllers of Layer 2 and Layer 3 traffic, it's important to ensure that the routers and switches deployed are trusted, organization-authorized network devices.

Attack types: Switch spoofing, ARP spoofing, and enablers of further attacks including IP spoofing and DNS cache poisoning.

Man-in-the-middle (MITM) attacks

While being virtually undetectable by security scanners, rogue devices are the major enablers of MITM attacks. Acting in almost all layers of the network's OSI model by manipulating access points, switches, routers, and endpoint devices, rogue attackers can infiltrate organizations to run MITM attacks.



Man in the middle attack

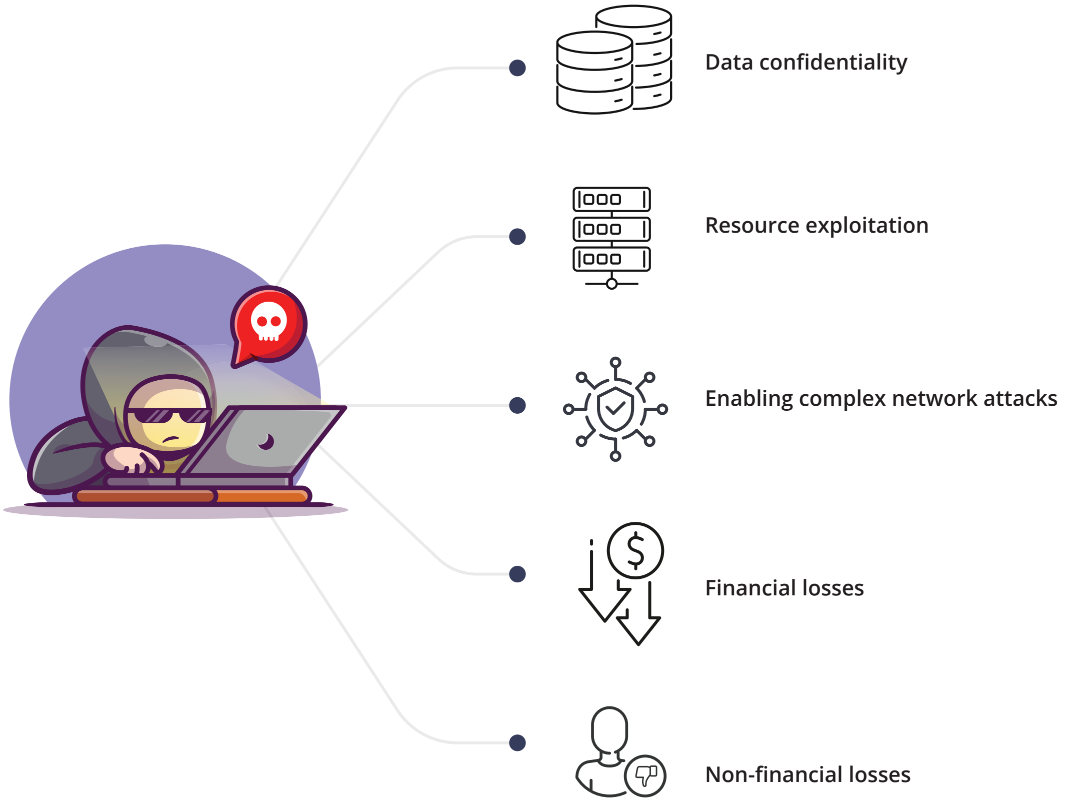
Some of the common attack types include:

- **Packet sniffing:** Unencrypted network data processors, data streams, and traffic flows are exploited by rogue attackers using MITM techniques.
- **Session ID stealing:** When critical transactions, such as payment gateway actions or password logging, are performed through rogue access points, attackers can steal the session IDs to carry out MITM attacks that can result in heavy financial losses.
- **Data theft:** A major concern to organizations, data theft becomes unavoidable with undetected rogue devices perpetuating MITM attacks. These kinds of attacks can go undetected even for years without effective security strategies.

4. Rogue attack impact: Are you willing to risk IT?

Network security is at the core of ensuring an uninterrupted, reliable, and trusted networking experience for your orgnization's employees. Tackling and preventing rogue devices requires stringent security polices both in the hardware and software layers of the IT ecosystem. While this does call for lesser flexibility and more stringent IT security practices, the trade off is negligible when compared to the alternative—more flexibility, less security.

The impact of rogue devices can be devastating for organizations of all scales and complexities.



- **Data confidentiality:** Compliance violations; data theft, loss, and manipulation; and eavesdropping by rogue devices can critically compromise an organization's confidentiality.

- **Enablers of complex attacks:** Several advanced and modern network attacks are often carried out based on a primary rogue intrusion or attack, such as a MITM attack. This makes the cause or root of these attacks go undetectable until a major network incident occurs.

- **Financial losses:** Resource exploitation, network downtime, and other consequences of rogue attacks result in costly financial losses to organizations. Statutory and compliance regulation fines can also strain an orgnization's IT operations budget.

- **Non-financial losses:** Like many cybersecurity attacks, rogue attacks result in non-financial losses as well. From serious loss of reputation and brand equity to loss of employee efforts, rogue attacks pose several untoward consequences.

5.Tackling rogues: Changes to "rogue-proof" IT

So, how do organizations tackle rogue devices? For most organizations, it's still a challenging task. Like every other IT threat mitigation strategy, tackling the threat of rogue devices requires organizations to be up to date on the latest security best practices and recommendations. However, it doesnt stop with just how well your IT security team is doing. It also requires changes at the technological, business, and organization culture levels.

Technology

Does your IT team have complete visibility into vour entire IT ecosystem?

Policies

Is IT "flexibility" weakening your organization's defense against rogue devices?

Culture

Rogue prevention is not the task of just your IT team. Is your entire organization involved?

- **Technology-level changes:** A crucial step to averting rogue attacks is making rogue device detection and prevention an integral part of your network security strategies. Network admins should continually monitor their network endpoints for new devices connecting to their network. Going a step further, the rogue device detection practices implemented should be in tandem with the firewall's intrusion detection and prevention strategies to ensure effective rogue attack prevention.

- **Policy changes:** While it's important to provide a seamless networking experience for employees, unmonitored and flexible IT paves the way for shadow IT. To avoid gray areas in the IT infrastructure, organizations need to fine-tune their IT procurement, deployment, and request policies along with BYOD policies.

- **Organization culture:** It's important to educate employees on possible entry points, threats, and the impact of rogue devices to avoid the instance of "the unsuspecting IT guy." Employees and teams should hold appropriate levels of responsibility for the IT deployment actions they oversee or undertake. New employees should be made well aware of BYOD policies and other IT security protocols. A clear distinction between the usage and network accessibility of organization-issued, trusted devices and users' guest devices should be established.

6.A look into OpUtils, the rogue mitigation solution trusted by admins worldwide

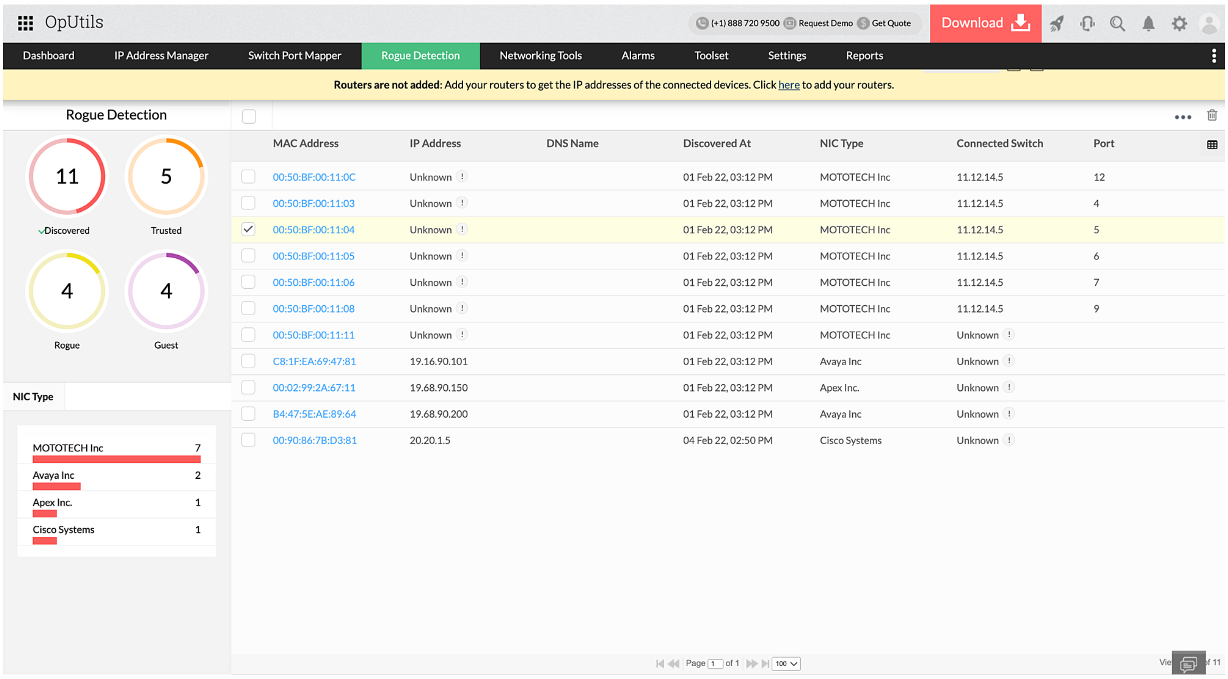
ManageEngine OpUtils is comprehensive **rogue device detection and prevention software** that offers a holistic approach to safeguard your network from rogue attacks. Its Rogue Detection module is tightly integrated with OpUtils' **IP address management** and **switch port mapping** modules that enable network admins to gain complete visibility into their address space and network connectivity.

OpUtils' rogue mitigation tool highlighted features

The first line of defense against rogue attacks has never been more easy to set up!

Rogue device detection

OpUtils' rogue device detection module can be set up in under minutes in networks of all scales and complexities. OpUtils continually scans critical network endpoints, such as routers, switch ports, and ARP tables, and records them to identify new devices connecting to the network. Its continual holistic network scanning uses various network protocols to ensure no new device connecting to your network goes undetected.



Routers are not added: Add your routers to get the IP addresses of the connected devices. Click here to add your routers.

Rogue Detection

11	5	4	4
✓Discovered	Trusted	Rogue	Guest

NIC Type

NIC Type	
MOTOTECH Inc	7
Avaya Inc	2
Apex Inc.	1
Cisco Systems	1

	MAC Address	IP Address	DNS Name	Discovered At	NIC Type	Connected Switch	Port
□	00:50:BF:00:11:0C	Unknown !		01 Feb 22, 03:12 PM	MOTOTECH Inc	11.12.14.5	12
□	00:50:BF:00:11:03	Unknown !		01 Feb 22, 03:12 PM	MOTOTECH Inc	11.12.14.5	4
☑	00:50:BF:00:11:04	Unknown !		01 Feb 22, 03:12 PM	MOTOTECH Inc	11.12.14.5	5
□	00:50:BF:00:11:05	Unknown !		01 Feb 22, 03:12 PM	MOTOTECH Inc	11.12.14.5	6
□	00:50:BF:00:11:06	Unknown !		01 Feb 22, 03:12 PM	MOTOTECH Inc	11.12.14.5	7
□	00:50:BF:00:11:08	Unknown !		01 Feb 22, 03:12 PM	MOTOTECH Inc	11.12.14.5	9
□	00:50:BF:00:11:11	Unknown !		01 Feb 22, 03:12 PM	MOTOTECH Inc	Unknown !	
□	C8:1F:EA:69:47:81	19.16.90.101		01 Feb 22, 03:12 PM	Avaya Inc	Unknown !	
□	00:02:99:2A:67:11	19.68.90.150		01 Feb 22, 03:12 PM	Apex Inc.	Unknown !	
□	B4:47:5E:AE:89:64	19.68.90.200		01 Feb 22, 03:12 PM	Avaya Inc	Unknown !	
□	00:90:86:7B:D3:81	20.20.1.5		04 Feb 22, 02:50 PM	Cisco Systems	Unknown !	

Rogue device inspection

Once detected, OpUtils lists the newly identified network devices under its Rogue Detection module. Using this module, network admins can examine various networking aspects of the device, including its address space details and switches through which the device has communicated.

Network admins can inspect and whitelist or mark authorized devices as "Trusted" and other non-malicious user devices as "Guest" by configuring a validity period. Suspicious devices can be blacklisted or marked as "Rogue," and after inspection, network admins can carry out the necessary steps to mitigate rogue access.

Rogue device mitigation

The first step to tackling identified rogue access and mitigating the impact of rogue attacks is to block the rogue device from accessing your network. OpUtils helps you do this by scanning and displaying the switch port that is enabling rogue devices' communication with your network. You can instantly block these switch ports remotely from the OpUtils console, and thwart rogue devices from wrecking havoc in your network.

There is no better time than now to avert the threats, impact, and aftermath of rogue attacks. Have you deployed the leading rogue device management software yet?

⬇ Download

$ Get quote

For more information about OpUtils, visit: www.manageengine.com/products/oputils/features.html

About the author

Sharon A Ratna

Product Marketer

Sharon A Ratna is a product marketing analyst for ManageEngine's ITOM suite that has helped IT teams in Fortune 100 worldwide for over 20 years. She researches and writes on technologies that develop, enhance, and simplify the current solution capabilities and new opportunities in the ITOM domain. With an exceptional understanding of marketing trends and consumer pain points, she works with the product management, development, and support teams to fine-tune and execute engaging marketing strategies. A passionate storyteller, in her free time enjoys reading books and traveling.

Glossary

Term	Definition
IoT	Internet of Things
BYOD	A bring your own device (BYOD) policy allows users to bring and connect their own devices to the organization's network.
Shadow IT	When IT components, such as devices and applications, are run without authorization from the orgnization's IT team.
Stealth IT	A term used interchangeably with shadow IT.
OSI model	The Open Systems Intercommunication (OSI) model explains the seven layers that enable network communication.
Air gap network	A network disconnected from other parts of the orgnization's network and following stringent security measures. These highly protected networks avoid both wired and wireless communication outside the network.
DoS	A denial-of-service (DoS) attack targets a particular critical network resource, such as a server, and overloads its capacity, notably the server traffic, making it unreachable to other genuine devices trying to access the critical device.
DDoS	A variation of DoS, distributed denial of service (DDoS) attacks focus on multiple critical resources at a time, causing widespread network outages and unreachability.
Man-in-the-middle attack	A type of network attack where the attacker positions themselves in the line of communication or in the middle of a transaction between two networking entities, such as a user and another user, or a user and an application.