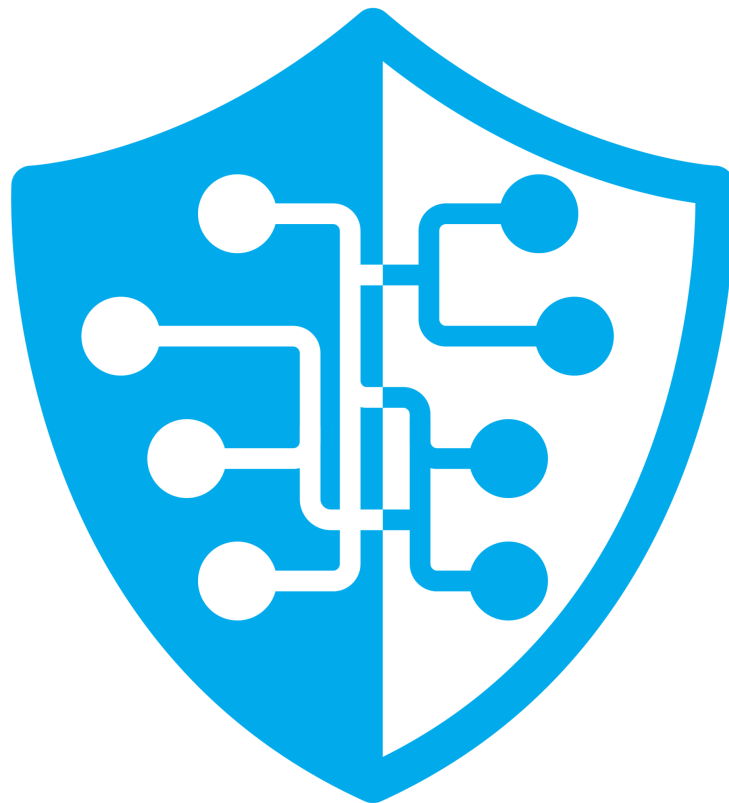


The Essential Guide to Network Threat Prevention

How to Protect Your Network Against Malware, Ransomware, DDoS, OT Attacks, and More



Presented by:



Contents

Contents	2
Introduction	3
OSI/ISO Network Security Model Layers 1-7	4
Malware & Ransomware	5
What Motivates Malware Attacks?	5
What Are the Common Vulnerabilities Exploited During a Malware Attack?	5
What Are the Most Effective Preventative Measures?	5
What Are the Best Tactics for Dealing With an Attack?	6
Distributed Denial-of-Service (DDoS) Attacks	7
What Motivates DDoS Attacks?	7
What Are the Common Vulnerabilities Exploited During a DDoS Attack?	7
What Are the Most Effective Preventative Measures?	7
What Are the Best Tactics for Dealing With an Attack?	8
Rogue Access Points	10
How Are Rogue Access Points Created?	10
What Can Rogue Access Points Look Like?	10
What Are the Most Effective Preventative Measures?	10
What Are the Best Tactics for Dealing With an Attack?	10
OT Attacks	12
What Are the Top Industries Targeted by OT Attacks?	12
What Are the Common Vulnerabilities Exploited During an OT Attack?	12
What Are the Most Effective Preventative Measures?	13
What Are the Best Tactics for Dealing with an Attack?	13
A Comprehensive Network Security Solution	14
About Byos	14

Introduction

It is no secret that cybercrime is on the rise.

Nearly every statistic, from the likelihood of a data breach — [which increased by 64% during 2020](#) — to the global costs of cybercrime — [projected to hit \\$10T by 2025](#) — is trending in the wrong direction.

And many technological trends, from the proliferation of OT devices — [forecast to reach nearly 30B by 2030](#) — to the rise of remote work — which [may account for over 36M US employees by 2025](#) — seem to play right into the hands of malicious actors.

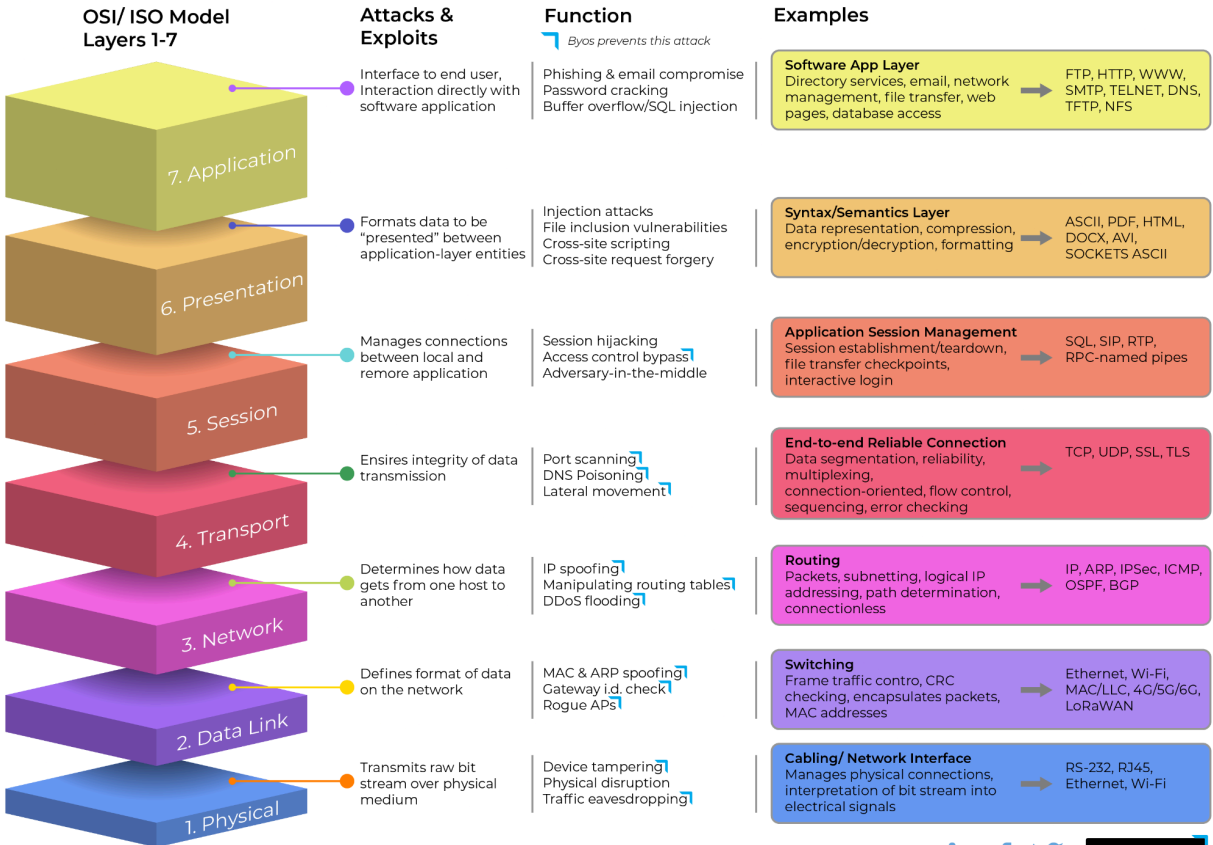
Although the current threat landscape is becoming increasingly hostile, the reality is that organizations have never been more capable of protecting themselves. Cybersecurity experts have developed hard-won, effective playbooks for dealing with every type of network security threat. Network security technology has matured, offering robust solutions for each stage in the cyber kill chain.

This guide provides a primer to these tactics and technologies. It is designed to help organizations looking to improve their security posture against the most common network threats. It explains the nature of these threats, articulates the latest actionable solutions, and provides direction on how to implement them.

The **first section** will tackle malware and ransomware, from the motivations that drive cyber criminals that use malware to the best tactics for dealing with an attack that's underway. The **second, third, and fourth sections** go into the same level of detail regarding distributed denial-of-service (DDoS), rogue access point, and operational technology (OT) attacks.

Finally, the **fifth section** outlines the benefits of the [Byos](#), a proactive solution security teams can use to protect their network against all of these threats by providing last hop security that stops ransomware from spreading.

OSI/ISO Network Security Model Layers 1-7



The OSI (Open Systems Interconnection) model is a conceptual framework used for understanding the different functions of a network system. The OSI was developed by the International Organization for Standardization (ISO) in hopes of increasing interoperability between different vendors and clearer standards for network communication. Although the OSI is not used for building networks (the [TCP/IP](#) is the most recognized and widely used protocol for network communication), it provides a helpful framework for classifying different types of cyber attacks.

Most cybercriminals will target a network on one of the seven layers of the OSI, and organizing threats along the different levels can make it easier to think about prevention, detection, and remediation strategies.

In this guide, we'll cover three of the most prominent vulnerabilities that bad actors use to exploit your network, if given an opening.

Malware & Ransomware

Malware is a general term for any software designed with malicious intent. While overall usage has continued to grow over the years, certain types of malware, like ransomware, have become particularly popular. In fact, the World Economic Forum ranked [ransomware as the world's leading cybersecurity threat](#).

Malware has been — and continues to be — a fundamental threat to modern businesses. Here's what you need to know to protect your organization.

What Motivates Malware Attacks?

Financial Gain	Political Aims	Espionage	Notoriety
To steal valuable information or extort money from a target organization.	To use malware to disrupt rival groups or cause serious harm to other countries.	To use malware to spy on individuals, companies, and government organizations.	To execute malware attacks to gain prestige within their community or pull a prank.

What Are the Common Vulnerabilities Exploited During a Malware Attack?

Human Error	Poor Password Hygiene	Shadow IT	Outdated Software
Employees can easily fall prey to malware, phishing or other forms of fraud.	Weak or stolen passwords are used to break into a system to deliver malware or gain access.	Technology that is unknown to IT or is unmanaged, is a top security concern for 69% of tech executives .	Failure to keep the tech stack up to date leaves the door open for compromise.

What Are the Most Effective Preventative Measures?

Malware Security
Companies can help reduce malware through cybersecurity training. Training creates a “security culture” and should be a first line of defense. However, relying on people to catch every malicious email or website has proven to be problematic. As a result, we have to start assuming that people aren't perfect, and that it is our responsibility to prevent malware from taking root, and prevent its spread when it does get past our first lines of defense.

Identity Management

Modern identity and access management (IAM) technology adds another layer of security between your employee and your network. IAM solutions help ensure that only authorized users are granted access to your company's IT resources by vetting requests via established identity verification protocols. They also provide organizations with comprehensive user credentials and permissions controls so administrators can maintain rigorous access principles, like least privilege access and separation of duties. Passwordless technologies are growing by leaps and bounds because they provide protections in ways that even MFA has failed to resolve. These next generation preventative technologies make privilege escalation challenging even when malicious actors have obtained users' credentials.

Updating, Hardening, and Streamlining

Updates to existing software ensures that the latest security features and bug fixes are engaged, **harden** the IT infrastructure to cut non-essential services and patch vulnerabilities, and **streamline** the tech stack by retiring unused applications and shadow IT.

What Are the Best Tactics for Dealing With an Attack?

Accelerate Time-to-Detection

Although advanced security information and event management systems (SIEMs) can help organizations identify a compromise, time-to-detection can be sub-optimal — allowing malicious actors to dig their heels into the network. Companies can improve response through the use of [endpoint detection and response \(EDR\)](#), [managed detection and response \(MDR\)](#), [or extended detection and response \(XDR\)](#), [security information & event management \(SIEM\)](#), and [user & entity behavior analytics \(UEBA\)](#).

Contain and Remediate

Preventing malware from gaining an initial foothold and then stopping the spread is critical. Creating a network with “absolute-least-privilege-access” through the use of zero trust principles implemented with the right technology prevents hackers from gaining access to a device, and implementing proper access controls, combined with [anti-lateral-movement technology](#) enables organizations to quickly lock down infected devices before the malware can gain broad access. When a threat is contained to one endpoint, remediation is orders-of-magnitude faster and more manageable for the entire organization.

[Click here to learn how to prevent and neutralize malware, ransomware, and other forms of malicious cyber attacks.](#)

Distributed Denial-of-Service (DDoS) Attacks

Denial-of-service (DoS) attacks seek to prevent legitimate users of a service from getting access to or using that service by flooding the system with traffic or exploiting an existing vulnerability in the target software.

The most prevalent form of DoS attack is the distributed denial-of-service (DDoS), which uses coordination among multiple malicious actors to create confusion and frustrate attempts to combat the threat. DDoS attacks are growing fast: In late 2022, the [NetScout 2022 DDoS Threat Intelligence Report](#) put the number of DDoS attacks at just over 6 million attacks globally, with the bandwidth increasing 57% over a six-month period.

To build a comprehensive security plan, organizations must be familiar with DDoS attacks and how to fight them. Here is a complete rundown on this threat.

What Motivates DDoS Attacks?

Financial Gain	Political Aims	Notoriety
To extort money from a company or government institution.	To further specific terrorist or political activists' goals.	To demonstrate their technical prowess, or simply amusement or challenge.

What Are the Common Vulnerabilities Exploited During a DDoS Attack?

System Limitations	System Bugs
IT applications and services often have usage thresholds that, once exceeded, can grind an entire system to a halt.	IT systems can contain bugs and other vulnerabilities that cause a system to crash or malfunction if exploited.

What Are the Most Effective Preventative Measures?

Vulnerability Audits
Vulnerability audits help your organization drive security improvements that protect against DDoS attacks. This process involves discovering all the devices on your network, identifying their function, documenting their system information, and mitigating their current vulnerabilities. After this analysis, the security team should prioritize and patch issues according to severity.

Multi-level Protection Solutions

Another critical component of your prevention strategy should be implementing multi-level protection strategies. Leveraging threat management and intrusion prevention technology, these solutions can keep a DDoS attack from overwhelming your system by identifying the initial signs of an attack and immediately blocking it. Organizations can pair this software with [hardware solutions](#) to significantly raise their system's resilience to DDoS attacks. Internet providers also provide solutions and additional protections, generally at additional expense, for advanced protections.

Device and Network Cloaking

The most effective means of putting an end to DDoS is to make the devices discoverable and accessible only to known and trusted devices. Since these devices are invisible to any device on the Internet that is not trusted, they do not respond to unknown or untrusted devices.

What Are the Best Tactics for Dealing With an Attack?

Follow Your Response Plan

Every organization should develop a plan that helps them mount a fast and effective response in the event of a DDoS attack. This plan should outline each team member's role during the attack, explain how escalation will be handled, and clearly describe the resolution process. It should also include a systems checklist and other vital details. Response plans are critical to minimizing ad hoc decision-making and focusing your efforts during the chaos and pressure of an attack, so make sure your team has one on hand.

Maximize Network Defensibility

DDoS attacks are difficult to fend off with a large attack surface. Approaches like cloaking, zero trust, and microsegmentation can significantly increase your network's defensibility by drastically shrinking the attack surface. There are a limited number of security technologies that can provide a single, integrated solution that fully addresses all three capabilities. You should also use caution that there are differences in the methods that vendors use to provide these functions. For instance, network cloaking vs. device cloaking can produce two different outcomes depending on your situation.

[Click here](#) to learn how Byos can help you minimize your organization's attack surface with this approach.

Rogue Access Points

Rogue access points are unmanaged wireless access points that connect to an organization's network. Cybercriminals can use this attack vector to spy on individuals, steal data from an organization, or install malicious software.





Rogue access points are notoriously effective, even against security-conscious individuals. One experiment run at the world-famous RSA security conference [lured nearly 2500 experts to connect to a dummy rogue access point](#).

While rogue access points are a significant cybersecurity challenge, there is a proven game plan for managing this risk — the following section outlines its key components.

How Are Rogue Access Points Created?

Employee Error	Coordinated Effort
Accident is the most common source of rogue access points. Employees can unintentionally create them using their home router — or even their mobile phone.	If a malicious actor can slip through an organization's physical security and get on premises, they can install a rogue access point to gain network access and carry out an attack.

What Can Rogue Access Points Look Like?

			
Wireless Access Point	Personal Routers	Wireless Cards	Mobile Devices

What Are the Most Effective Preventative Measures?

Education & Usage Policies

Well-meaning employees create substantial rogue access point risk inside an organization. Your employees should know the protocols for safe technology use and how to properly work with IT when setting up a network connection, but your procurement organization can also contribute to the process. Unauthorized access points can be discovered with network and RF scans through the existing APs and infrastructure..

Physical Protection Tactics

There are several physical security measures companies can take to reduce rogue access point risk. Such tactics include doing scheduled sweeps of the premises for suspicious devices, attaching labels to network assets and infrastructure, and maximizing the amount of equipment that is physically locked away. These tactics minimize the time it takes to find an unauthorized device and make it much harder for malicious actors to place one into your network.

Rogue Access Points Outside your Organization

Home networks, public networks (airports, coffee shops, hotels, etc.) and third-party networks cannot be controlled by your cybersecurity organization. When devices or users access your network or cloud, you are essentially inviting in the vulnerabilities and exploits that are in those devices. You can't patch, scan, or enforce configuration on personal devices, BYOD, or your suppliers, contractors, or customers. Therefore, you need to implement protections and access control policies so that malicious threats on those devices are prevented from accessing or spreading across your network and devices.

What Are the Best Tactics for Dealing With an Attack?

Create Intra-Network Barriers

Flat networks allow malicious actors easy access to your IT resources once they have made it inside your network. Edge microsegmentation creates a more complex environment for intruders, who still need to overcome numerous cyber defenses post-compromise. This approach significantly slows — if not entirely stops — their progress through the network.

[Click here](#) to explore how Byos' solution can help you defend itself against rogue access point attacks.

Pin and Destroy

Some Wireless Intrusion Prevention Systems (WIPS) have containment functionality that allows them to mitigate the damage of an attack via a rogue access point. A wired containment strategy uses network scanning or traceroute to find the rogue access point's switch port and disable it. Wireless containment, meanwhile, uses targeted deauthentication, distraction, etc. to interfere with the attack. Once the rogue access point has been contained, you can send a team to assess the situation in person and remediate the threat.

OT Attacks

Operational Technology (OT) attacks are cyber attacks that target connected devices, such as smart cameras, thermostats, or locks.

The rapid adoption of WiFi-enabled devices has created operational efficiencies for organizations — and opportunities for cybercriminals. Consequently, organizations are increasingly looking to understand the risks posed by these devices and the steps they can take to mitigate them.

From the most targeted industries to the latest prevention tactics, here’s an overview of OT attacks.

What Are the Top Industries Targeted by OT Attacks?

Healthcare	Manufacturing	Utilities
<p>Medical devices deliver life-saving services, and malicious actors have used this fact as leverage. Over half of hospitals have experienced an attack in the past two years, and just under half of those who experienced a ransomware attack paid up to resolve the situation.</p>	<p>A key component of the Industry 4.0 shift is the bringing the OT devices into the digitized production process. Critical infrastructure & OT security is the fastest growing concern today.</p>	<p>OT devices have been deployed for years, (almost 1.2B endpoints in 2019 alone). This critical infrastructure was developed without security in mind. Government and utility providers are struggling with this as a top priority.</p>

What Are the Common Vulnerabilities Exploited During an OT Attack?

Convergence	Network Sprawl	Unencrypted Data
<p>The convergence of IT and OT in industries like manufacturing has created a much larger — and harder-to-secure — attack surface.</p>	<p>Organizations focused on driving OT innovation can expand their network faster than IT can account for all its components, creating blindspots across the fleet.</p>	<p>While OT devices do not always store data, they’re often used to transmit important information. Much of it lacks the encryption required to protect the data when it is being transmitted or stored.</p>

What Are the Most Effective Preventative Measures?

<p>Asset Tracking</p>
<p>To rein in the risks caused by network sprawl, companies can develop protocols for installing or updating devices that require the parties involved to manually enter device details into an authoritative database. Smaller companies can implement quarterly audits of all network-connected devices. In addition to these processes, organizations can use helpdesk systems, SIEMs, System Center Configuration Managers (SCCM), and automated scanners to enhance their inventory tracking capabilities.</p>
<p>Data Encryption</p>
<p>During equipment audits, security teams should note OT devices are involved in data storage or transmission and whether or not they have encryption functionality. Teams should implement AES 256-bit encryption for data at rest. For data in transit, TLS 1.2 encryption is the absolute minimum, but v1.3 is highly recommended.</p>

What Are the Best Tactics for Dealing with an Attack?

<p>Deploy Mitigation Protocols</p>
<p>Although you always want to build as many preventative measures as possible into your cybersecurity, your security team must operate understanding that compromise is a matter of when — not if. This assumption is especially relevant to organizations that rely heavily on OT, as their fleet of devices is often far more extensive and more challenging to manage than companies with fairly traditional IT infrastructure. So develop mitigation protocols detailing the identification, containment, and remediation process your security team should follow when the inevitable does occur.</p>
<p>Leverage Innovative Tactics</p>
<p>When it comes to mitigation strategies, microsegmentation has proven to be a potent threat containment and elimination strategy for industries like manufacturing, where OT devices play a critical role.</p> <p><i>Read this page for an in-depth discussion on how industrial players and other OT sectors are Byos to protect their most important assets.</i></p>

A Comprehensive Network Security Solution

While each of the threats we've covered in this ebook warrants individualized tactics, there are approaches that improve an organization's ability to handle these risks.

Creating a network with "absolute-least-privilege-access" through the use of zero trust principles implemented with the right technology prevents hackers from gaining access to a device, and By dividing your network into endpoint-specific sub-networks, implementing proper access controls, combined with [anti-lateral-movement technology](#) using device cloaking and microsegmentation enables organizations prevent initial access and to to quickly lock down infected devices before the malware can spread to any other devices.

[Contact our experts today](#) to see how Byos can help you overcome your most pressing network security challenges.

About Byos

OT, mobile devices, "the cloud," working-from-home, and video streaming have all radically changed how the internet works. That growth and complexity is accelerating. Yet there is little difference in how internet security operates from the time when it was originally built almost 50 years ago.

Byos is stepping up the challenge to create a new way of securing "the net," and in doing so, is proving that network security can be simpler and, at the same time, fundamentally more secure. Byos makes all devices, and the network itself, invisible. Byos communicates ON the network without being connected TO the network by isolating each device on its own network of one. Even if a device is compromised by some other means, like malware from an email, Byos limits the spread.

Byos is backed by Silicon Valley investors and advisors and based in Nova Scotia. We serve customers across all industries and governmental institutions. For more information, visit www.byos.io.