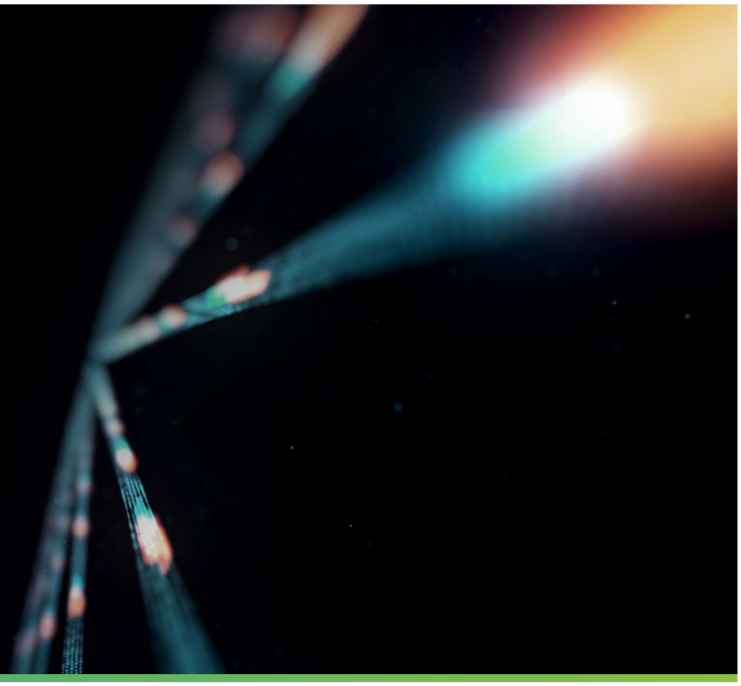

Benchmarking Cyber Risk and Readiness

Understanding the Prevalence and Risk of Internet-Exposed Protocols on Organizations' Networks

Executive Summary

The *Shields Up* notice issued by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) in the wake of Russia's invasion of Ukraine put organizations around the world on notice about the heightened risk of cyberattack activity from one of the most sophisticated nation states and its allies. While some of the *Shields Up* recommendations focused on new approaches to cyberdefense, many of them focused on the foundational basics of cybersecurity: secure passwords, rapid patching and updating, and properly configuring services to avoid exposing critical assets and data. In this report, we focus on this question of configuration, looking at when and why organizations leave ports and protocols exposed to the internet, the prevalence of these exposures, and how organizations can minimize both disruption and risk.

A Changing Risk Calculus

On February 25, 2022, just two days after Russia began its military invasion of Ukraine, the Cybersecurity and Infrastructure Security Agency (CISA) issued its first-ever *Shields Up* notice warning that the Russian government and its allies (both nation-state and independent) were likely to increase cyberattacks against Western governments and organizations in retaliation for their support of Ukraine.

The *Shields Up* notice includes guidance for organizations to strengthen their overall security posture, starting with reducing the likelihood of a damaging cyber intrusion. It outlines essential steps security teams should take, including:

- Update software, priority those that address known exploited vulnerabilities
- Disable all ports and protocols that are not essential
- Implement strong cloud controls
- Quickly identify and assess unusual network behavior

> “
> Evolving intelligence indicates that the Russian Government is exploring options for potential cyberattacks. Every organization—large and small—must be prepared to respond to disruptive cyber incidents.
>
> **CISA Shields Up Notice, February 25, 2022**

A key recommendation involves disabling all unnecessary or insecure ports and protocols. While this might seem straightforward, a surprising number of organizations still expose, either as a calculated risk or as a result of misconfiguration, notoriously insecure protocols like Server Message Block version 1 (SMBv1) to the internet. The ExtraHop Threat Research team previously looked at the prevalence of insecure protocols across enterprise environments. In this report, we focus on network protocols that generally shouldn't be exposed to the public internet, and the frequency with which they are being run on open ports across enterprise organizations.

By reading this report, security and IT leaders can gain a better understanding of the risks associated with exposing ports and protocols, and assess their risk posture relative to other enterprise organizations.

First, we'll take a closer look at protocols themselves and examine why organizations expose protocols to the internet where they can be accessed by malicious outsiders. Then we'll take a look at the prevalence of specific protocols—including old, officially unsupported versions of protocols—that were found active on networks in a survey ExtraHop conducted of thousands of organizations across multiple industries.

For additional information about specific protocols, be sure to explore the ExtraHop Protocol Glossary.

Learn More about Shields Up

ExtraHop published two reports offering guidance to organizations interested in putting CISA's *Shields Up* suggestions into practice.

- *A Practical Guide to Shields Up: Advice for Corporate Leaders and CEOs in Implementing CISA's Cybersecurity Doctrine to Defend your Enterprise* offers high-level guidance to business leaders responsible for understanding operational risks and prioritizing investments accordingly.

- *A Practical Guide to Shields Up: Advice for Organizations in Implementing CISA's Cybersecurity Doctrine to Defend Your Enterprise* offers more technical guidance for IT organizations interested in putting Shields Up advice into practice.

Network Protocols: A Barometer for Cyber Readiness

Protocols are the communication mechanism of the internet, allowing different devices and services to talk to each other across networks. Protocols are also a critical part of network security. Used properly, they can protect data and commands as they traverse a network. Used improperly, they can unintentionally expose data and systems to attackers, in some cases offering an opening for cybercriminals to insert their own malicious data and commands.

Many commonly used protocols were developed decades ago, long before programmers had to worry about ransomware or other modern forms of cyberattack. As a result, these protocols fail to provide the security controls baked into more modern protocols. Yet many of these old protocols remain in use, in some cases providing services that IT teams and end users consider essential or supporting legacy systems that the organization has yet to phase out.

The use of these protocols isn't inherently a problem. If the devices using them to communicate are configured correctly—meaning that their ports are secured appropriately and devices are properly patched—the protocol isn't exposed and there's little risk to the organization. But for a variety of reasons, many ports are left open, able to receive communications from the open internet.

Exposed Protocols: The Attack Path Inside the Enterprise

Attackers are searching for any way into a network—any unguarded network port or any network protocol with lax security controls. They run scanning software that probes network interfaces by sending test messages to addresses and port numbers. Then they analyze the replies they receive to determine how an organization's internet-facing network is configured and what opportunities that configuration offers for attack.

Once attackers have breached the network and installed software on a single device, they will take advantage of the implicit trust most devices place on other devices behind an organization's firewall to traverse the internal network, spreading malware, searching for valuable data to copy and steal, or shutting down devices to cause economic destruction. Ports and protocols are essentially the doors and hallways that attackers use for exploring networks and causing damage. That's why knowing which protocols are running on your network and what vulnerabilities are associated with them is so important.

The Exposure Risk Calculation

Protocols including HTTP and HTTPs, FTP and sFTP, and SMTP and POP3 enable major communications across the internet, from website traffic to file transfers to email. These protocols are exposed by design. They allow the outside world to communicate with your network, and most of them, like HTTPS, are encrypted to protect sensitive data as it flows north-south across the firewall.

But even protocols designed to be exposed provide points of ingress for cyberattack. Take, for example, the exploitation of the Log4j vulnerability known as Log4Shell. In the hours following the disclosure of the vulnerability, many organizations saw a flood of intrusion attempts on port 80, commonly associated with HTTP. Within 48 hours, attackers began encrypting that traffic, attempting to exploit the vulnerability over port 443 (HTTPS) to better obscure their activity from security analysts.

Another example is the domain name system (DNS) protocol. DNS makes navigating the internet easier for users by mapping IP addresses to human readable domain names, but is frequently misused by attackers for malicious purposes such as command and control (C2) and data exfiltration. There's a reason everyone blames DNS.

But there are other protocols, including those primarily used for communications inside an organization, that may also be exposed to the internet. It is the exposure of these protocols that introduces the greatest risks for organizations, and the ones to which the *Shields Up* guidance is most attuned.

Remote Desktop Protocol (RDP) allows remote access (screen, keyboard, mouse) to Microsoft servers. SSH provides command-line access to Linux servers. Both are heavily targeted protocols because they can give an attacker direct access to critical systems. SMB/CIFS allows for access to files and folders giving attackers direct access to your data. However SMB is also heavily targeted by exploit developers and has in the past allowed command-line access to servers in a similar manner to RDP or SSH when successfully exploited. Eternal Blue is a classic example of an SMB exploit that gives you a shell on an exploited device. Recent ExtraHop research revealed that 68% of organizations are still leveraging SMBv1, the protocol exploited in the WannaCry and NotPetya attacks that was publicly deprecated by Microsoft in 2014.

Each organization needs to assess the balance of risk versus reward, or how much cybersecurity exposure they can tolerate to allow for smooth business operation. While these protocols aren't typically exposed to the public internet in best practice guidance, each organization should review these benchmarking stats and determine if they have the right amount of exposure and risk to allow their business to operate smoothly.

Common Types of Sensitive Protocols and Their Risks

In response to the CISA *Shields Up* guidance, the ExtraHop research team decided to look into the prevalence of sensitive protocols whose exposure should be minimized to reduce the risk of attack. What the team found was generally positive. Across the protocols evaluated, the total number of devices exposing these sensitive protocols to the internet was generally low. Indeed, a small number of exposed devices and protocols is generally needed to allow an organization to function.

Protocol	Protocol type	Percentage of organizations with at least one device exposing this protocol to public internet	Average number of devices exposing this protocol to the public internet out of 10,000 devices
SSH	Remote Control	64%	32
LDAP	Directory	41%	13
FTP	File Server	36%	3
SMB	File Server	31%	64
RDP	Remote Control	25%	14
TDS	Database	24%	3
Kerberos	Directly	20%	4
TNS	Database	13%	2
Telnet	Remote Control	12%	1
NFS	File Server	9%	5
ICA	Remote Control	6%	23
MySQL	Database	6%	1

The real issue is about whether the exposed device is (1) necessary for the business and (2) properly secured. Unfortunately, the devices that are exposed tend to be servers and other core or critical resources. Cybercriminals often use these vulnerable devices as an entry point before pivoting throughout the network.

Let's take a look at four types of protocols and their associated risks:

- File server protocols
- Directory protocols
- Database protocols
- Remote control protocols

File Server Protocols

The vast majority of cyberattacks involve attackers moving files from one place another. Attackers might move a dangerous file such as a malware executable onto a victim's computer. Or they might move a copy of valuable data from inside a corporate network to a command-and-control server in a distant country. Because so many attacks involve moving files, it makes sense that file server protocols would be useful to attacks.

SMB

In its audit of enterprise networks, ExtraHop found SMB exposed to the public internet on 64 out of 10,000 devices.

In Windows environments, Server Message Block (SMB) is a common attack vector.

Microsoft developed SMB in the 1980s long before protocol designers had to be concerned about defending against cyberattacks. There are now three versions of SMB, known as SMBv1, SMBv2, and SMBv3. SMBv1 is famously insecure: It's the file protocol that WannaCry and NotPetya malware variants use for traversing networks. In the famous NotPetya attack that shut down Maersk's shipping operations in 2019, destroying over 49,000 laptops and over 1,000 applications, attackers traversed the company's global network in just minutes using SMBv1.

Aware of potential security risks, Microsoft officially deprecated SMBv1 in 2014, acknowledging that they no longer considered SMBv1 secure enough for corporate networks. Yet the protocol is still widely used. A recent survey by ExtraHop found that 68% of organizations are still running SMBv1.

Why would organizations expose these protocols to the internet, dramatically increasing the risk of them being used in attacks? One reason would be to offer file-sharing services to remote workers or business partners. A more secure alternative would be to use modern Software-as-a-Service (SaaS) file sharing services such Dropbox or Box, which are much more secure than any version of SMB for sharing files outside the organization. We also often see file servers accidentally left open to the public internet, underlining the risk that human error can have on enterprise security.

Administrators can make SMB protocols more secure by requiring them to use encryption. Some administrators turn encryption off, so they can monitor traffic for suspicious activity. Servers and connected protocols should be reviewed and hardened or re-architected.

NFS

ExtraHop found NFS exposed to the public internet on 5 out of 10,000 devices.

Network File System (NFS), a protocol developed originally for file sharing on UNIX systems, is now found in every Linux distribution. It works similarly to SMB and suffers from some of the same security shortcomings. Older versions of NFS did not support encryption. NFS v4, which was released in 2003, does support encryption.

A best practice is to configure NFS to require authentication through Kerberos, rather than username/password combinations that can be potentially attacked through brute force. Another best practice is to protect NFS servers with zero trust-focused firewalls, allowing access only to authenticated users and processes.

FTP

ExtraHop found FTP exposed to the public internet on 3 out of 10,000 devices.

SMB and NFS all provide direct access to the file system. File transfer protocol (FTP) is different. It's a file transfer protocol, not a full-service file access protocol. It sends files over networks as a stream. FTP itself offers practically no security. It transmits data, including usernames and passwords, in plaintext, which makes its data easy to intercept.

There are two secure alternatives. The first, less optimal alternative is FTPS, which transmits FTP over TLS/SSL. The second and more secure option is SFTP or secure FTP, which tunnels FTP through SSH, the secure shell protocol. SSH has proven to be a well-designed and very secure protocol. It supports digital certificates, so users can authenticate themselves without risking the discovery of usernames and passwords.

Directory Protocols

Directory protocols enable users and processes to look up information about users and IT resources in network-accessible directories. One of the most popular directory services is Active Directory (AD), a proprietary service developed by Microsoft.

To access AD, many devices use two protocols, LDAP and Kerberos. There aren't many reasons any organizations would need to expose these two protocols to the public internet.

LDAP

ExtraHop found LDAP exposed to the public internet on 13 out of 10,000 devices.

Lightweight directory access protocol (LDAP), a vendor-neutral application protocol used to maintain distributed directory information in an organized, easy-to-query manner. Windows systems use LDAP to look up usernames in AD. Unfortunately, by default these queries are transmitted in plaintext, giving attackers an opportunity to discover usernames. With known usernames, attackers can then use brute force attacks to generate username/password combinations until a combination gives them access to a resource they're trying to break into.

If possible, it's better to configure devices to use LDAPS, which transmits queries and responses over encrypted SSL connections.

Kerberos

ExtraHop found Kerberos exposed to the public internet on 4 out of 10,000 devices.

Kerberos is one of the oldest authentication protocols in the computer industry. Developed at MIT in the 1980s, it became an IETF Standard in 1993. Microsoft has used it for authentication in its products for decades.

Kerberos improves the security of authentication processes by eliminating the need to send a user's password over the network, where it could possibly be intercepted. Instead of exposing a vulnerable password, Kerberos sends a hash (a mathematically derived, scrambled representation of the password) over the network. Both sides of the connection check the hash. If hash matches, the user is authenticated.

As good as Kerberos is, it's still vulnerable to attack. For example, in an AS-REP roasting account, attackers discover which user accounts have had their Kerberos pre-authentication turned off in AD. When pre-authentication is turned on, a user password is hashed with a timestamp and sent to a service for description. If the password matches, the service accepts the password, but only within a window of time tied to the timestamp. If this timestamp verification isn't required, attackers can sniff a Kerberos ticket and then crack it offline, confident that the cracked ticket will be valid indefinitely.

To guard against these types of accounts, organizations should ensure their Kerberos software is up-to-date, that administrator access is limited, that Kerberos pre-authentication is turned on in AD, and that services accept only a limited number of login attempts before timing out.

Database Protocols

Database protocols enable users and software to interact with databases, inserting, updating, and retrieving information. When an exposed device is listening on a database protocol, it exposes the database as well.

TDS

ExtraHop found TDS exposed to the public internet on 3 out of 10,000 devices.

Tabular Data Stream (TDS) is a Microsoft protocol for communicating with databases. It transmits data in plaintext, making it vulnerable to interception. To prevent attackers from discovering authentication credentials, TDS traffic should be embedded in HTTPS. Database clients might negotiate with a database server before settling on which version of TDS to use. A best practice is to always require clients and servers to use an encrypted version of TDS.

Another best practice is to check for login failures to a database running TDS. For example, imagine an attacker intercepting LDAP traffic and discovering usernames. The attacker then might launch a brute force attack on a database, transmitting high numbers of username/password combinations over TDS. By configuring a database to reject login attempts after a small number of failures, administrators can prevent these brute force attacks from eventually breaking into databases.

Another best practice is to minimize the number of users with administrative access to databases. In addition, security teams should protect databases with firewalls that enforce network segmentation rules, allowing only traffic from select IP addresses to pass through.

TNS

ExtraHop found TNS exposed to the public internet on 2 out of 10,000 devices.

Transparent Network Substrate (TNS) is essentially Oracle's version of TDS: It's a network protocol for accessing databases. TNS is subject to the same vulnerabilities as TDS. The remedies for these vulnerabilities are the same—require encryption of traffic going to and from databases, minimize administrative access to the databases themselves, and protect the databases with firewalls and network segmentation.

MySQL

ExtraHop found MySQL exposed to the public internet on 1 out of 10,000 devices.

MySQL, an open-source relational database, is one of the most popular databases in the world. It's also the architectural foundation for other open-source databases such as MariaDB and Percona Server for MySQL. Because of its popularity, MySQL offers attackers a massive attack surface. There are over a hundred exploits targeting MySQL databases or their access protocol, which is also called MySQL. Some of these attacks succeed. In 2020, attackers breached 83,000 MySQL servers and offered 250,000 MySQL databases for sale on the dark web.

The best practice is to keep all your database software and protocols up to date. If possible, use firewalls to microsegment the networks around your database servers, allowing access only from authorized IP addresses.

Remote Control Protocols

Remote control protocols enable users to access and control devices across networks. For example, a data center administrator might leave a public-facing RDP/SSH server open as a backup when VPN fails. Accidentally exposed Windows machines with RDP enabled or Linux/Mac machines with SSH enabled are another common source.

SSH

ExtraHop found SSH exposed to the public internet on 32 out of 10,000 devices.

Secure Shell (SSH) is a well-designed protocol with good cryptography for securely accessing remote devices. SSH is available on all Linux distributions and in other operating systems as well. OpenSSH is a popular, open source implementation. Because SSH is so widely used, it is widely attacked.

In 2019, a data breach at web hosting company GoDaddy.com gave attackers access to SSH accounts of many users. The company discovered the breach and reset the passwords.

To protect SSH accounts, organizations are encouraged to keep their SSH software patched and up to date. To access SSH, administrators require digital certificates instead of passwords, and the digital certificates should be 2048-bit, not 512-bit, making them more difficult to crack. Administrators should set up timeout intervals for idle sessions and block access to an account after a certain number of failed login attempts. Another best practice is to set up firewalls to limit access to certain IP addresses, preventing attackers from accessing SSH from outside a very small number of trusted devices.

ICA

ExtraHop found ICA exposed to the public internet on 23 out of 10,000 devices.

Independent Computing Architecture (ICA) is a remote control policy originally developed by Citrix and Microsoft together, and then further developed by Citrix on its own. It provides a way for a user on one device to interact with an application remote. It conveys inputs such as mouse actions and keyboard input to a remote application and conveys graphical output from the application back to the user's device. Help desk services such as Zendesk use ICA to enable help desk agents to control a remote user's computer.

There are two versions of ICA: standard and secure. The secure version supports rotating ephemeral keys for encryption, ensuring that even if attackers cracked keys being used, they would gain access to session data for only a minute or so. It's a good idea for security teams to monitor their Citrix servers to ensure that only authorized devices are connecting to them.

Over the past decade or so, many organizations have purchased inexpensive, thin client devices that allow employees to access business applications remotely. Unfortunately, some of these thin client products are configured with insecure versions of ICA. Worse, some of these clients might not be able to be easily updated to more secure versions of the protocol; others might not support updates at all. Organizations that have purchased these clients should diligently monitor ICA server activity for any signs of attacks.

RDP

ExtraHop found RDP exposed to the public internet on 14 out of 10,000 devices.

Remote Desktop Protocol (RDP) is Microsoft's version of ICA. RDP is a default tool for help desks, making it a high-value target for attackers. Unfortunately, new vulnerabilities are discovered in RDP all the time. For example, in January 2022, researchers discovered that a vulnerability allowing man-in-the-middle attacks was present in versions of RDP going back to 2012. In May 2022, another vulnerability that allows remote code execution was announced and patched. Keeping RDP software patched and up-to-date is essential for good security hygiene.

While RDP is useful to help desk agents troubleshooting employee devices, it's not needed anywhere else. IT organizations should disable RDP on any device out of the help desk's purview. In addition, they should enforce group policies to limit access to RDP servers.

To guard against brute force attacks, administrators should configure RDP servers to require strong passwords and two-factor authentication. They should also enforce lockout policies that prevent logins after a set number of login failures from the same device. Finally, they should force clients using RDP to connect over Network Level Authentication (NLA), a Microsoft authentication protocol that provides an added layer of security for remote desktop connections.

Telnet

ExtraHop found Telnet exposed to the public internet on 1 out of 10,000 devices.

Teletype Network (Telnet) protocol is an old protocol for connecting to remote devices. When it was created in 1969, no one could imagine the cyberattacks jeopardizing data security and business operations today. As a result, Telnet offers no encryption. It's easily intercepted.

As a best practice, IT organizations should disable Telnet anywhere it is found on their network.

Benchmarking Protocols by Industry

Protocol usage differs by industry. That shouldn't be surprising, since different industries have invested in different technology vendors over the years and have different requirements for storing data, interacting with remote users, and so on.

We strongly recommend that every organization benchmark its own protocol use, but to help give business and IT leaders a sense of industry trends, we present the table below, showing the prevalence of the protocols discussed in this benchmarking report across six different industries: financial services, healthcare, manufacturing, retail, state and local government and education (SLED), and technology.

The table below shows a breakdown of internet exposed protocols by industry: The percentage of organizations with internet exposed protocols, and the average number of public internet-exposed devices per 10,000.

INDUSTRY

PROTOCOL

	Financial Services	Healthcare	Manufacturing	Retail	SLED	Technology
SMB	28% 34 Devices	51% 7 Devices	22% 2 Devices	36% 2 Devices	45% 5 Devices	19% 4 Devices
NFS	9% 3 Devices			13% 1 Device	15% 0.2 Devices	
FTP	33% 1 Device	51% 0.4 Devices	22% 0.1 Devices		40% 0.5 Devices	30% 0.2 Devices
LDAP	47% 4 Devices	49% 2 Devices	33% 1 Devices	38% 0.5 Devices	53% 4 Devices	35% 0.3 Devices
Kerberos	21% 1 Device	28% 0.4 Devices	12% 1 Device	13% 0.2 Devices	33% 0.3 Devices	15% 0.1 Devices
TDS	20% 1 Device	44% 0.4 Devices	14% 0.1 Devices	21% 1 Device	35% 1 Device	15% 0.1 Devices
TNS	9% 1 Device	16% 0.1 Devices	33% 1 Devices	33% 1 Device	24% 0.2 Devices	
MySQL	4% 0.1 Devices	19% 0.1 Devices			9% 0.2 Devices	
SSH	66% 7 Devices	79% 5 Devices	55% 1 Devices	67% 7 Devices	65% 4 Devices	52% 1 Devices
ICA	5% 6 Devices	16% 15 Devices				
RDP	18% 9 Devices	53% 1 Device	16% 0.1 Devices	33% 0.1 Devices	25% 3 Devices	12% 0.1 Devices
Telnet	15% 0.2 Devices	32% 0.4 Devices			11% 0.2 Devices	

Conclusion

We encourage organizations in every industry to assess their own use of network protocols, especially their use of protocols exposed to the internet. Some of these protocols such as SMBv1 and Telnet are inherently risky. Others are risky when exposed publicly. By analyzing their own network and device configurations and traffic patterns, organizations can better understand their security risks and take action to improve their cybersecurity readiness.

Here are some steps to get started:

- ✓ **Build and maintain an inventory of software and hardware in your environment.** Don't think of this as a static list but as an evolving matrix to track. Everytime a new device connects your network, your threat posture changes. Detect, track, and monitor all devices and their software configurations so you can understand your risk overall. Leverage a tool that can passively inventory all assets.
- ✓ **Stay up to date with information about vulnerabilities, software updates, and patches.** Monitor resources such as the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) to stay up to date with announcements about the latest discoveries about vulnerabilities.
- ✓ **Patch software quickly, continuously.** About 60% of data breaches involve software with known vulnerabilities that were not patched in time to prevent an attack. Patch quickly and stay safe.
- ✓ **Analyze your organization's use of protocols, especially protocols exposed to the internet, and take action to reduce the attack surface you are providing to malicious outsiders.** This report describes many of the threats that these protocols can pose. Take action to reduce them so you can reduce the chances of your organization being attacked. Some protocols, such as Telnet, can be eliminated entirely. Whenever possible, use the latest, most secure version of any protocol.
- ✓ **Use firewalls and other defenses to protect databases, RDP servers, and other business critical but exposed IT resources.** Some use of risky protocols is unavoidable, but you can reduce the risk associated with those protocols by deploying firewalls and network segmentation to limit access to valuable resources. It's also important to monitor the behavior of these exposed assets so anomalous or malicious activity is flagged.
- ✓ **Invest in network analysis and threat detection tools so you can have real-time insights into the security hygiene of your network and the appearance of any active threats.** IT security isn't a one-time task. It's an ongoing, 24/7/365 activity that requires vigilance over all aspects of your IT environment, including multi-cloud environments and remote users.

A key requirement for this work is the ability to passively monitor and analyze network traffic continuously, cataloging protocol use, and detecting network intrusions in real time.

ExtraHop can help organizations with this important security work by continuously analyzing network environments on-premises, in the cloud, and at the network edge, and by providing real-time intelligence about vulnerabilities, suspicious traffic, and active threats.

ExtraHop Reveal(x) 360 is a SaaS-based network detection and response (NDR) platform that provides 360-degree visibility and situational intelligence without friction. Reveal(x) 360 can be set up quickly and easily and requires minimal management. Using the Reveal(x) 360 platform, organizations of all sizes can discover which protocols are running on their network, which devices are at risk, and where suspicious activity or outright attacks are taking place. Critically, Reveal(x) 360 decrypts encrypted traffic to detect and identify dangerous payloads such as ransomware. Acting on alerts and other intelligence from Reveal(x) 360, security teams can take immediate action to remediate threats and protect IT resources and daily operations.

CISA has taken the unprecedented step of issuing a *Shields Up* notice in light of evolving intelligence from a nation state with advanced cyberattack capabilities. By analyzing and securing network protocols across their networks, organizations in every industry can improve their security hygiene, reduce their attack surfaces, and effectively put their cybersecurity shields up.

For more *Shields Up* resources, visit extrahop.com/resources/shields-up.

ABOUT EXTRAHOP

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

ExtraHop

info@extrahop.com
www.extrahop.com