packet watch

7 Cybersecurity Gaps

Our experts identified these common gaps while responding to cyber incidents last year.

Introduction

"Cybersecurity is the practice of doing the little things right, over and over again."

The spectrum of threats faced by any network today is ever-growing and morphing, as new vulnerabilities are routinely found in existing applications within all layers of the technology stack.

From a security perspective, the message seems to be that the "next-gen" of whatever security tool is what will keep the evil at bay.

In this document, our incident response team (Team Sixty43) offers a **different view**—a lesson on the building blocks of security.

- Best practices
- Basic cyber hygiene
- Clear and enforced policies

Let's look at the seven things IT and cybersecurity teams should confirm are implemented correctly to prevent cyberattacks in 2026.

1. Multifactor Authentication
2. Identity and Access Management
3. Endpoint Protection
4. Patch Management
5. Attack Surface Management
6. Risk Management
7. Network Security Monitoring

packet watch

Bonus

Schedule a 15-minute complimentary call with one of our experts.

This is a "help" call, not a sales call. We'll answer your questions, provide guidance, and discuss ways to identify gaps in your security program.

Schedule a Call

Email:
appointment@packetwatch.com

Online:
packetwatch.com/appointment

1. Multifactor Authentication

All companies, regardless of size, should implement Multifactor Authentication (MFA) on every supported device and service. Unfortunately, Team Sixty43 has observed the opposite. We regularly identify applications, devices, and accounts that lack MFA for logins or access.

A common initial access vector in a cyberattack is an unprotected virtual private network (VPN). Without MFA, a VPN is a significant cybersecurity liability. All public-facing systems (VPN, cloud, email, web apps, etc.) and internal systems (servers, endpoints, etc.) must enforce MFA. The goal is to make it more difficult for intruders to enter and pivot around the network. Every time they attempt to connect to another host, the system should limit access by prompting them to enter a new MFA code.

MFA has limitations. It's not perfect, and not all authentication protocols support it. Many organizations struggle to enforce MFA because users refuse to install or use authentication apps. This forces these organizations to use SMS- or email-based MFA instead.

While authentication through WinRM, RDP restricted admin mode, service accounts, and many legacy and OT systems does not support MFA, enforcing it wherever possible is better than not enforcing it at all.

Be sure to audit your partner connections to confirm that your supply chain partners also enforce MFA.

What We Saw

While investigating a 2025 ransomware incident, our response team observed that a client's supply chain partner required MFA for remote monitoring and management (RMM) connections, which helped prevent the ransomware from spreading to the downstream partner's environment.

2. Identity and Access Management

Another significant security gap we see organizations failing to address is Identity and Access Management (IAM). It's a broad topic, spanning on-premises Active Directory to cloud identity systems such as Microsoft Entra ID.

The challenge for cybersecurity and IT teams is often a severe lack of adherence to the Principle of Least Privilege (POLP) and the unfortunate reality that most IAM systems are overly complex (looking at you, Entra ID).

In Active Directory, admins must ensure that critical groups, such as RDP Users, Domain Admins, and Enterprise Admins, are audited regularly. Users who are no longer active or no longer need these permissions must be removed as soon as possible.

Additionally, Active Directory permissions, such as "DS-Replication-Get-Changes", when delegated to non-admin accounts, often allow attackers to obtain DC (Domain Controller) Sync permissions, making it easy to take over your domain.

What We Saw

In one incident investigated by the PacketWatch Sixty43 Team, a threat actor had compromised a service account. This service account had Domain Admin rights, even though it was used only to run a few web applications. This allowed the threat actor to easily access this publicly accessible service account and immediately gain Domain Admin rights out of the gate.

3. Endpoint Protection

Surprisingly, we're still seeing organizations without business-grade antivirus (AV) or Endpoint Detection and Response (EDR) systems. We're also seeing organizations relying heavily on the Microsoft Defender version included with Windows 11. Threat actors, such as LockBit, have tools that target and disable basic AV and EDR solutions without anyone noticing.

Robust EDR systems are harder for attackers to disable than conventional AV solutions, and they use sophisticated detection systems to identify anomalous processes and user behavior. Choose an endpoint protection solution that monitors anomalous behaviors, and not just static signatures. It should also include anti-tamper capabilities.

What We Saw

In one ransomware attack we investigated, the client relied on an endpoint security solution that lacked tamper protection. The threat actor ran a script to disable all antivirus and EDR on targeted machines in the environment, leaving the client completely unaware of the malicious actions taken, ultimately leading to a successful ransomware deployment.

4. Patch Management

Patch Management remains an ongoing challenge for most organizations, especially with legacy or end-of-life systems. Even with EDR, finely tuned IAM, and MFA, an unpatched domain controller or firewall can be the primary vector a threat actor uses to bring down an entire billion-dollar business operation.

To improve patch management operations and mitigate risk, we recommend the following:

- Use Patch Management software to manage and patch systems as needed. Many of these applications also include robust remote management, endpoint discovery, and other capabilities that make them a valuable tool for network administrators.
- Segment legacy systems (that cannot be patched or replaced) from the primary network.
- Keep legacy systems off the domain. Implement a strict ACL/firewall policy to ensure that only certain users or groups can access this environment via specific services.
- Keep legacy systems off the Internet. If these systems must remain on the Internet, use a secure proxy, a Secure Access Service Edge (SASE) solution, or a “strict allow” list (specific IP addresses).

Applying these recommendations will help contain incidents arising from the exploitation of this legacy environment and make it extremely difficult for attackers to pivot from these environments to the corporate network.

What We Saw

In another ransomware case, our team traced the source of the intrusion to an unmanaged firewall. The client had not updated it for years, allowing the threat actor to easily exploit it and gain network access.

5. Attack Surface Management

While phishing and social engineering are often considered popular initial access vectors, we see attackers exploiting unprotected internet-facing assets more often.

Web servers, jump boxes, email servers, firewalls, and VPN appliances typically lack endpoint protection applications or system logs that security teams can ingest into a SIEM. Threat actors exploit this limited visibility to compromise these internet-facing devices and evade detection.

Full Packet Capture (FPC) solutions like PacketWatch can easily monitor network traffic for subtle signs, such as anomalous activity and abnormal patterns, to identify compromise and reduce the risk associated with these internet-facing devices.

What We Saw

In one case, our investigation revealed that the threat actor gained access to the network through an exposed RDP service. After successfully brute-forcing the RDP service, the threat actor moved undetected through the network. The client's server logs were not ingested into their SIEM, and the firewall was unable to monitor the threat actor's East-West traffic.

6. Risk Management

We often see that ransomware victims also have poor risk management processes. “Praying that nothing will happen” is not a sound cybersecurity strategy. As Murphy’s Law states, “Anything that can go wrong will go wrong.”

While the recommendations outlined throughout this document will mitigate most threats, risk awareness is important and shouldn’t be ignored. Cybersecurity frameworks, such as NIST and CIS, help organizations clearly identify and manage their risks.

Using a framework to audit your cybersecurity operations will guide you through the rigor required to identify where you comply and where you need to improve. The framework process will help you develop actionable plans to reduce your risk and prevent cyber disruption.

What We Saw

During a CIS Critical Security Controls Framework assessment, our team identified gaps in documentation and management of hardware used to access sensitive data. Implementation of risk controls on these devices discovered several instances of vulnerabilities that could have resulted in the exposure of sensitive data.

7. Network Security Monitoring

In every incident response engagement we've worked on, robust network security monitoring is missing. Many organizations believe a firewall is sufficient. Some have implemented Intrusion Detection Systems (IDS) to gain more network visibility. Unfortunately, threat actors can easily evade these systems.

Most firewalls send alerts only when their signatures are triggered, and these alerts can quickly become noise for the security operations team. Many firewall vendors require upgrades and additional licensing to improve alert fidelity. The ultimate solution is continuous Full Packet Capture, but IDS and most firewalls don't offer it. Some solutions may offer context-aware packet capture, where the network activity is stored after a detection or alert is triggered.

Full Packet Capture (FPC) allows the security operations team to record and store every packet traversing the network, passively, in PCAP files. Much like a DVR for TV, security teams can "rewind" and analyze these files to investigate traffic anomalies, protocols, destinations, and contents at the packet level.

Robust network threat-hunting and network detection and response (NDR) platforms have this FPC capability and can produce more accurate (higher-fidelity) alerts. PCAP files also provide forensic evidence of the sequence of activities and files that were manipulated or exfiltrated during an incident.

What We Saw

During a routine threat hunt using the PacketWatch Platform, our team found signs that one of our clients had an intrusion stemming from a compromised firewall that the client was not managing. The threat actor pivoted to servers unprotected by EDR, effectively evading the client's security team. However, thanks to FPC, our team was able to see the subtle signals and alert our client to this critical incident before any damage was done.

Conclusion

While some of these security gaps may seem obvious, the technical details and their management can be very complex. If it were easy to implement and manage all these gaps, we wouldn't see them constantly causing incidents that Team Sixty43 needs to respond to, investigate, and remediate.

Cybersecurity is about doing the little things right, over and over again. Even if it is painful and repetitive, organizations need to address these gaps to avoid business disruptions caused by cyberattacks.

Do you have questions or need help?

Schedule a complimentary 15-minute call with one of our experts. This is a "help" call, not a sales call. We'll answer your questions, provide guidance, and discuss ways to identify gaps in your security program.

Schedule Appointment

Contact Us

Phone:
1-800-864-4667

Email:
appointment@packetwatch.com

Online:
packetwatch.com/appointment

About PacketWatch

Most organizations have very little, if any, visibility into their networks.

That's where we come in, not just with tools but with experts specifically trained to look for network anomalies, patterns, and threats that other security tools and professionals will miss.

We're network threat hunters with one of the most advanced full-packet capture threat-hunting platforms and cloud-based analytics engines. Our team focuses on proactively fixing your security issues holistically, not just resolving the alerts from your host-based tools and SIEM.

If you would like us to review or manage your network security, we offer incident response, security assessments, managed services, and incident response retainer services, all leveraging our network threat-hunting platform and battle-hardened security experts.

Let's take a look at your network telemetry.

Visit or Follow Us

Website:
packetwatch.com

Cyber Threat Intelligence Reports:
packetwatch.com/cti-reports

LinkedIn:
linkedin.com/company/packetwatch

24/7 Incident Response Hotline:
1-800-864-4667

packet watch