ALERT LOGIC™

Cybersecurity Checklist

Preventing Initial Compromise

This security overview provides best practices to help organizations looking to harden their environment. Designed to help small to mid-sized organizations stop an attack before one starts, this basic guidance will help reduce your attack surface and outlines practical steps to securing your enterprise. With this checklist, you will have a guide to help prevent initial compromise and stop attacks before they start.

This checklist helps to explain how to:

- Address software vulnerabilities and misconfigurations
- Eliminate exposed ports & services
- Reduce the chance of attacks delivered via email
- Limit browser-based attacks
- Reduce the attack surface across Microsoft Office applications

Lastly, we will share details on how Alert Logic helps organizations of all sizes get a comprehensive view of their enterprise assets, find misconfigurations and vulnerabilities, and delivers endpoint coverage with an automated quarantine response to stop malware in its tracks.

Preventing Initial Compromise

The best defense against cyber attacks is to prevent attackers from gaining initial access to a machine in the first place.

☐ **Prioritize Patching**

When vulnerabilities are disclosed, it's only a matter of time before attackers begin exploiting them. Having a system in place to assess, test, and roll out patches is a vital first defense against attacks.

☐ **Isolate What You Can't**

Patching is vital, but not easy and it can be impossible in some cases. Isolate systems you can't patch quickly by restricting system access.

Eliminate Exposed Ports & Services

- [ ] **Secure Remote Desktop (an RDP)**
  Open ports with RDP exposed to the Internet are beacons for attackers. Restrick access to RDP listening ports by placing them behind a firewall and using a RDP Gateway. Enabling network-level authentication and changing the default listening port (TCP 3389) is also recommended.

- [ ] **Secure Server Message Block (SMB)**
  Disable SMBv1 and use firewalls to restrict SMB network activity. WannaCry and other attacks leveraging the EternalBlue exploit have shown just how vulnerable organizations become when exposing SMB. Ideally do not allow file transfer between secured networks at all.

Reduce The Chance Of Attacks Via Email

- [ ] **Block Common Malicious File Attachments**
  In addition to the obvious (.EXE, .BAT), consider blocking script files (.JS, .VBS, etc.), archive files (.ZIP, .SFX, .7z), and even Office files (.DOC, .DOCX, etc.) and PDFs. Consider which file attachments you wish to block carefully to strike a balance between security and the ability to do business.

- [ ] **Conduct User Awareness Training**
  Many attacks still initially require users clicking something they shouldn't. Training and inform your end-users about attacks that rely on deception and social engineering.

Limit Browser-Based Attacks

- [ ] **Utilize Ad-Blockers**
  Even legitimate websites can serve as infection points thanks to malvertising.

Disable OLE Packages

- [ ] **Enforce Stricter Macro Controls**
  Block macros in Office files downloaded from the Internet. Macros are abused to download malware and launch malicious scripts.

- [ ] **Disable "Update Automatic Links At Open" in Microsoft Word**
  This will prevent abuse of the DDE feature (now disabled by default) and similar threats.

- [ ] **Disable OLE Packages**
  Considering the long history of attackers abusing Microsoft's object linking and embedding (OLE) feature, it's best disabled when possible.

All Of The Above

- [ ] **Establish a system that provides visibility across your organization, monitor application and system behavior for threats, implement proactive vulnerability scanning, and deploy endpoint and anti-virus protection.**

  Patching, isolation and restricting risky activity prevents a lot of initial attack vectors from causing damage yet many attacks take place through zero-day or unknown vulnerabilities in servers and applications. Visibility of systems and the ability to monitor for unusual behavior on the endpoint, servers and in applications is critical to get early warning of attack attempts and allow you to respond accordingly.

ACHIEVE BETTER SECURITY AT OPTIMAL COST

Alert Logic is the only managed detection and response (MDR) provider that delivers comprehensive coverage for public clouds, SaaS, on-premises, and hybrid environments. Since no level of investment prevents or blocks 100% of attacks, you need to continuously identify and address breaches or gaps before they cause real damage. With limited expertise and a cloud-centric strategy, this level of security can seem out of reach. Our cloud-native technology and white-glove team of security experts protect your organization 24/7 and ensure you have the most effective response to resolve whatever threats may come. Founded in 2002, Alert Logic is headquartered in Houston, Texas, with business operations, team members, and channel partners located worldwide, and online at alertlogic.com.

Alert Logic – unrivaled security for your cloud journey.

ALERT LOGIC™