

**WEEKLY
CYBER
THREAT
LEVEL
INDICATOR**
**SEVERE
RISK**

Indicators:

Red - Severe
 Orange - High
 Yellow - Elevated
 Blue - Guarded
 Green - Low


CYBER THREAT LANDSCAPE
WHAT'S TRENDING?
Shadow IT is Your Organization's Next Remote-Working Nightmare

According to new research by software company Forcepoint, more than a third (37%) of UK employees are now relying on shadow IT at home, increasing companies' exposure to cybersecurity risks.

Microsoft Office 365 Still The Top Target Among Phishing Attacks

In a report published Wednesday, cloud security provider Menlo Security looks at the latest phishing campaigns and offers advice on how to avoid being a victim.

10 Tips to Protect Your Organization and Remote Endpoints Against Cyberthreats

A report released by security provider WatchGuard Technologies discusses the latest threats and offers advice on protecting your endpoints, both inside and outside your network.

In the Rush to Embrace Hybrid Cloud, Don't Forget About Security

Cloud computing provides significant benefits to organizations, enabling far more agility for development teams, on-demand scalability to meet variable compute needs, and reduced responsibility for infrastructure and the staff required to maintain it.


CRITICAL VULNERABILITIES
CVE
FBI: APTs Actively Exploiting Fortinet VPN Security Holes

The FBI and the Cybersecurity and Infrastructure Security Agency are warning that advanced persistent threat (APT) nation-state actors are actively exploiting known security vulnerabilities in the Fortinet FortiOS cybersecurity operating system, affecting the company's SSL VPN products.

VMware Patches 2 Flaws in vRealize Operations

VMware has issued patches for two critical vulnerabilities in its IT operations management platform, vRealize Operations, which, if exploited, could allow attackers to steal administrative credentials.

US CISA warns of DoS flaws in Citrix Hypervisor

Citrix addressed vulnerabilities in Hypervisor that could be exploited by threat actors to execute code in a virtual machine to trigger a denial of service condition on the host.

80% of Global Enterprises Report Firmware Cyberattacks

Attacks against firmware are snowballing, outstripping many organizations' cyber-defenses, according to a survey from Microsoft. The report showed that more than 80 percent of enterprises have experienced at least one firmware attack in the past two years – but only 29 percent of security budgets goes to firmware security.


CYBER SECURITY NEWS
WHAT'S NEW FROM VENDORS?
Zimperium Partners with Oracle to Help Enterprises Combat Advanced Mobile Threats

Zimperium announced that it is collaborating with Oracle to offer Zimperium's mobile threat defense (MTD) solutions on Oracle Cloud Infrastructure (OCI). The two companies are working together to help enterprises around the world combat advanced mobile threats.

Cisco's Vision for SASE and a Brand New Offer to Kickstart Your Journey

There's a growing challenge that many organizations face today: How can network and security teams provide consistent, secure access to applications for an increasingly distributed workforce — without taking on more complexity? This drives the need to rethink the traditional network architecture, and the concept of a secure access service edge (SASE) emerged as a result.

AT&T Cybersecurity Launches Managed SASE Solution with Fortinet

AT&T SASE with Fortinet is the first, global managed SASE solution at scale that unifies software-defined wide-area network (SD-WAN) with essential network security functions of the SASE framework and 24x7 management. With this consolidated approach, enterprises can also help reduce operational costs by moving to a single cloud-delivered solution.


SOMETHING TO THINK ABOUT
WHAT'S NEXT?
Building a Fortress: 3 Key Strategies for Optimized IT Security

The three strategies that IT teams should prioritize going forward: Zero-trust approaches; patching; and automation.

5 Key Cybersecurity Risks in 2021, and How to Address Them Now

With an unexpected year of massive change behind us, many organizations have now an extensive remote workforce, new technologies in use, and digital transformation under way across the board. While this has introduced many opportunities for SMBs, it has also come with a host of cybersecurity challenges.

Report: USB Threats to ICS Systems Have Nearly Doubled

The latest Honeywell USB Threat Report 2020 indicates that the number of threats specifically targeting Operational Technology systems has nearly doubled from 16% to 28%, while the number of threats capable of disrupting those systems rose from 26% to 59%.

Zero Trust: 7 Adoption Strategies From Security Leaders For Your Organization

Microsoft considers Zero Trust an essential component of any organization's security plan.