
XENGUARD
network security systems
Xenguard services

xenguard@xenguard.com | (647) 479-6926

About Xenguard

Xenguard is a global company which develops intrusion protection technology. We deliver security consulting and disaster recovery services to clients in need of serious protection for enterprise systems. We ensure your security investments yield provable bottom-line results. Xenguard backs up our IPS technology with no-nonsense security consulting and disaster recovery services. Xenguard's security professionals use proven methods to assess current systems, policies and capabilities. The other guys don't even come close, and we'll prove it with a free security probe.

Xenguard will fix, hack, or reverse-engineer just about anything. Want to run new software on an old hardware platform? We can help with that. Our engineers have decades of experience designing, customizing and maintaining most any type of electronic equipment. We've built everything from phones and tablets to kiosks, robotics, routers and IoT sensors. In fact, we've built systems for some of the largest vendors on the planet -- chances are Xenguard has been involved in engineering at least one device that you own. But because we're the little guys, we have the agility to bring products to market faster and cheaper than the competition. Our Xenguard firmware is compatible with the vast majority of computing devices on the market, from x86 servers to embedded appliances like routers and access points. If your vendor has abandoned your legacy device, we can help you restore functionality. Because we don't rely on Google for our operating systems, our hardware or our data, we will never say "no" to a feature request. We have the diagnostic and manufacturing capabilities you need, with the supply-chain contacts to deliver products under any conditions.

Information security refers to the controls that protect information from unauthorized access, destruction, modification, disclosure, and delay. Information security addresses safeguards in the processes of data origination, input, processing, and output. The goal of information

security is to safeguard the system's assets, to protect and ensure the accuracy and integrity of information, and to minimize the damage that does occur if the information is modified or destroyed. Information security requires accountability for all events that create, modify, provide access to, or disseminate information.

Many organizations recognize the benefits of using formal guidelines and methodologies from neutral third parties in establishing their security policies. Some groups have never developed policies; others have been unable to devote enough time to maintaining those policies. Sometimes the information technology staff lack expertise in information security; other times upper management have refused to support the measures known by the staff to be important for protecting corporate information assets. In all these cases, external organizations such as consultants, professional associations and certifying authorities can serve a useful purpose to alter the corporate culture and make the best use of security expertise. A Xenguard security assessment can help those who are responsible for the decisions. This widely recommended procedure, which is used to evaluate the many threats an information system faces, is a well-planned action to forsee the consequences of a failure in security. Xenguard keeps clients apprised of potential risks and suggest proactive security strategies. Xenguard provides security training at all levels, from highly technical programs for professionals in the field, to overviews for executives and managers, to general awareness for employees across a corporation or organization. If a company prefers implementing its own systems and networks, Xenguard provides security engineering support and technical assistance to augment the design team in the specialized areas of information security. Among other things, risk analysis considers the value of the assets to be protected, including the costs of disruption, the nature and probability of potential threats, and the cost of proposed safeguards.

Xenguard products are designed to meet the needs of our users. Our customers range in size from individuals and small businesses to government agencies. We're constantly discovering new applications for our technology. Xenguard solutions are about more than "just security"; we can help your business achieve greater success by giving you the critical business intelligence you need to make key decisions. If your business involves information, Xenguard is your solution of choice for securing and leveraging that information.

Security and surveillance

Everyone who has a network needs effective network security. Xenguard solutions are a cost-effective option to put you in control of your infrastructure.

Corporate networks and data centers

Xenguard solutions are ideal for telecommunications carriers. We can enforce most any security standard you wish to implement. Detect and block infected devices in real-time, to stop the spread of malware and the disclosure of sensitive information. Mitigate Denial-of-Service attacks and corporate espionage. Get detailed "deep data" on user behaviors and ensure compliance with corporate policies.

embedded device manufacturers

Xenguard's solutions are excellent for performance and compliance testing of network-enabled products. Xenguard can provide insights into how and why your IoT subsystems fail, and help you fix it.

Marketing agencies

Marketing agencies use Xenguard technology to collect and analyze information about customer behaviors. Going beyond the web, Xenguard "sees" behaviors that conventional marketing systems simply can't track.

Wireless network operators

Wireless networks often suffer from congestion and interference problems, which reduces performance and causes various anomalies for network users.

The Xenguard software offers an automatic wireless calibration mode which can automatically determine the best possible network configuration, and optionally implement changes in real time.

Xenguard services

“Hackers for Hire” consulting

Xenguard is pleased to offer “hackers for hire” consulting services to the general public. Our advanced infrastructure and highly skilled engineers are standing by 24/7 to support you. You can be assured that in time of need, Xenguard will be your trusted security partner. We will work with you to deliver effective and timely security incident management. You can call Xenguard, when no one else can help. While we specialize in network security, we have experience in a wide range of technologies and can assist with any project you bring to us. Clients may choose fixed or hourly billing. Sign in to your Xenguard control panel and submit a ticket – we’ll begin working on your issue right away.

Aren’t sure exactly what you need? Need some help with a technical challenge? Hire Xenguard to solve problems for you. Xenguard Technologies is a full-service technology consulting and managed services firm based in Toronto, Canada. Offering fully managed solutions, a robust global backbone and next-generation technologies, Xenguard can support your enterprise network like no other provider.

Using Xenguard's proprietary methods, evidence can be recovered from deleted files, formatted disk/tapes, re-initialized disks, and damaged disks. Xenguard Computer Evidence Services experts can safely enter any system, network or data storage device to recover data and determine whether it has been tampered with, deleted or damaged. Depending upon your needs, experts can: search for specific data, phrases, files, numbers or keywords; determine when data was accessed; verify illegal use of proprietary information; and validate software license infringement. This experience and expertise helps ensure that your electronic evidence will stand up in court.

Xenguard's monitoring service is a cost-effective, long-term solution to ensure the integrity of your network infrastructure. Xenguard will configure our sophisticated monitoring systems to gain deep visibility into network performance, security and stability metrics. Going far beyond the primitive “ping checks” offered by some data centers, our Network Operations Center can capture vital information about any problems that occur on your network - before it results in downtime. We can monitor most any metric on any device, from generic servers to application services, access control systems, surveillance, switching, building automation, routers, authentication and access control equipment.

Organizations choose Xenguard's in-depth penetration testing services for a number of reasons. The most common reason is to assess the amount of vulnerable systems that they own. Such tests are reduced to a simple percentage of systems that can be compromised. This percentage is tracked over time to track trends in a network's security posture. Another reason for testing may be driven by marketing. Many Internet Service Providers (ISPs) hire third party security consultants to conduct penetration tests so that the results can be shown to

current and prospective customers. Using a third party provides a sense of objectivity to the assessment. Other organizations may conduct penetration testing as the first step in a network security overhaul. The raw data from a penetration test is used to drive network changes and upgrades, which enhances security.

Regular penetration assessments are an excellent complement to Xenguard monitoring services. Xenguard security engineers will utilize our proprietary “deep scan” technology to actively probe your network infrastructure for vulnerabilities. The assessment may be performed on a blind (no one in the client organization is aware of the fact that the probe is occuring) or open (the client organization interacts with Xenguard during the assessment) basis. A penetration test proactively attempts to discover “zero-day” emerging security vulnerabilities which are not yet known to the security community. Xenguard engineers will fully stress-test your applications, databases, network infrastructure and security policies, discovering flaws in proprietary source code or incorrect configurations. You will know exactly what level of service your infrastructure is prepared to provide, and what the most cost-effective areas for improvement are. Open (interactive) assessments generally are conducted over a longer time-frame; Blind (secret) audits require less time and resources but may not capture all areas of exposure on the first test (as the client is not obliged to provide any non-public information about the systems being inspected). Our engineers have expertise in all of the most widely recognized information security standards. Xenguard can help you clean up the mess left by hackers and disasters, should they occur (f you use our products properly, it won't).

Xenguard services allow you to focus on building your business, while we focus on operating your information systems. If you wish, Xenguard can manage your entire application infrastructure to ensure that you are consistently providing your customers with the reliability and performance that they expect. Rather than hiring a costly internal team of system administrators or diverting your existing resources away from internal or business system management, leverage Xenguard's team of application experts to support your critical infrastructure. Xenguard provides top-quality network management services for organizations who require professional-quality maintenance of their network. Perhaps your company does not have sufficient internal resources to meet the demands of a particular project, or you might be running a network located thousands of miles away from your office. In these situations, Xenguard managed services can offer a cost-effective solution to your network management challenges. Generally, we can accommodate managed service customers anywhere in the world.

The key input into our incident management plan and required information to make application and infrastructure performance recommendations is our monitoring services. Xenguard works closely with our customers to design a custom monitoring solution that ensures all the key components of your application environment are monitored on the 24/7 basis. Xenguard can monitor a wide array of environment elements from bandwidth utilization to web and database server performance.

Xenguard provides full support to all elements of your application infrastructure and network components. Xenguard can manage your firewall and hardware infrastructure as well as web, application and database servers. As recognition of the value of your online brand is paramount, Xenguard works closely with you to develop and implement security and disaster recovery plans.

Managed Security Operations Center / Computer Emergency Response Team

The Xenguard Security Operations Center / Computer Emergency Response Team (XSOC/XCERT) program gives you access to our entire suite – hardware, software, intelligence and most importantly, our human beings. It’s an insurance policy for your systems.

Let us worry about your network security, so you don’t have to. The Xenguard SOC is designed to remain in constant contact with Xenguard's monitoring centers. Our data centers are highly secure, geographically distributed across the world, and staffed 24 hours a day by highly trained security professionals -- they are virtually impossible for an adversary to access, and even major disasters such as earthquakes, massive power outages or nuclear/biological/chemical incident will not take our global network offline. The security industry has many fancy names for this sort of service – Managed Detection and Response, Intrusion Protection Systems, Network Operations Center, or Tiger Team.

We detect threats to your data and systems, and help shut them down before they cause damage. We can provide the tools to secure your network against even the latest zero-day attacks. Your team stays focused on it’s mission; we’ll handle the security issue distractions and put out the fires. And we’ll handle the compliance paperwork, making sure your systems comply with requirements and standards such as the GDPR, PCI DSS, ISO 27001, SOC2 or CTPAT.

Scheduled maintenance will be performed within the time window that you specify, and Xenguard will conduct regular audits to ensure your organization is meeting it's compliance objectives. In addition to the monthly managed service retainer, hourly rates (standard, and emergency) will be established for any "above and beyond" services required which exceed your plan's management level.

Application layer reporting provides the customer with a range of information relating to the behavior of specific applications operating within the managed environment. Application reporting offers views into the operational details of deployed middleware applications dictated by customer requirements. Our web reporting service offers daily reports providing extensive information on incoming web client interaction with the hosted site. Daily, weekly, monthly, quarterly, annual and cumulative web usage statistics are generated for each hosted environment. A few examples of web usage reports available to each customer includes executive site summaries outlining critical statistics for any time period including unique user visit counts, user session lengths, number of unique documents delivered, top pages, top typical paths taken through the site, top client types. Web usage reporting offers a large number of detailed reports covering all aspects of user traffic throughout customer sites.

Xenguard provides clients with the information to understand how their application is performing under the weight of user demands. Xenguard infrastructure reporting helps clients ensure their hardware and bandwidth utilization and make appropriate decisions regarding future technology investments.

The Xenguard Security Operations Center will monitor all production application infrastructure on a 24/7 basis. All material aspects of component availability and performance will be monitored 24/7 for existing or developing problems. Xenguard will manage the 24/7 on-call rotation and escalation procedures required to resolve any site issues as they occur. Xenguard will provide 1st line support and escalation for all production site issues and include the Customer's support staff for application, level 2nd line support. Xenguard technical specialists will provide 2nd level escalation points for advanced problem resolution and vendor/service provider issue resolution. Xenguard will monitor the customer website for availability over redundant dedicated application - it would not identify an outage caused by faults within the Internet generally. Xenguard will work with the Customer to schedule maintenance window periods during which service-impacting maintenance can be performed. Xenguard will document all scheduled maintenance and anticipated service interruptions and allow the Customer's management to confirm these interruptions through a customer portal.

Tier 1: Hardware layer support

Xenguard engineers are responsible for configuration, monitoring and maintenance of your network hardware. This includes servers, switches, routers, KVMoIP, UPS, RPC and all other devices listed on Xenguard's hardware support list. Hardware devices not appearing on our supported list may require some research to determine how to best manage the device. At the server hardware and OS layer, customers will have access to reports proving views into resource utilization statistics generated across equipment within the managed environment. Examples of reports available at the resource layer include aspects such as processor, memory, and disk and file system utilization. In addition, customized reports extrapolating deeper low-level resources such as kernel utilization, user sessions, NFS events, and process loads are available based on individual customer requirements.

Tier 2: Operating System (OS) Layer Support

Xenguard manages all aspects of your operating systems. This includes configuration / optimization, patch maintenance, kernel builds, administration of authentication credentials and so on. This support level covers all components that are part of the core operating system.

Tier 3: Third Party/Middleware Layer Support

The Xenguard tier-3 managed support package covers all hardware, operating system and third-party applications listed on Xenguard's supported components list. Xenguard will undertake management of the Client's network infrastructure. This package is suitable for organizations who leverage multiple third-party (often open-source) tools. Third-party / middleware components are modules which are not a core component of your chosen operating system.

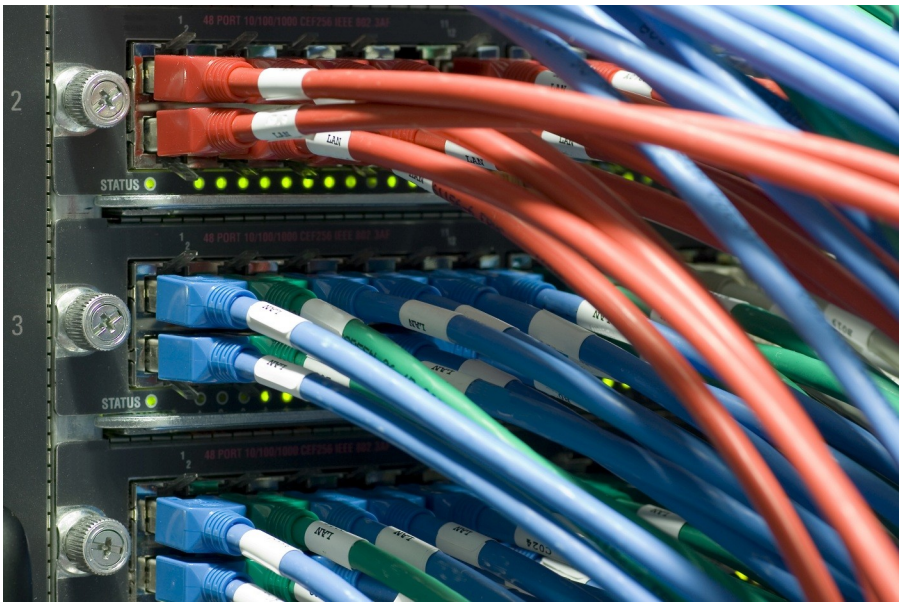
Tier 4: Application Layer Support

The final managed services tier encompasses the application layer – this includes your own proprietary code, scripts and databases. This is the highest level of support available from Xenguard. We will ensure your application(s) perform within established parameters, making recommendations on an ongoing basis to maximize long-term performance and stability. This tier is best suited for organizations which rely on proprietary (often internally developed) applications.

Xenguard's areas of expertise

XENGUARD Network Security Services

Xenguard has a full range of specialists on-staff to support your facility. From network security engineers to software developers and database specialists, Xenguard will provide the right mix of talent to meet your needs. Xenguard can manage your entire internet infrastructure -- the provisioning, deployment, testing, and ongoing management of all networking devices, including routers, switches, SSL accelerators, firewalls, routing tables and virtual private networks. We take the risk and complexity out of managing your systems, leveraging advanced automation technology to guarantee problem-free migration and ongoing management of your infrastructure's components.



Operating Systems

- Linux : Little Linux, OpenWRT / LEDE, Debian / Ubuntu, RedHat / CentOS / Fedora, Gentoo, LFS, SUSE, Slackware...
- BSD : OpenBSD, FreeBSD, NetBSD
- Solaris : versions 2.4-10 & OpenSolaris on Intel & SPARC
- other / legacy UNIX : IRIX, TRU64 / Digital UNIX, SCO, SVR4 / System V, AIX, HP/UX

Cloud / virtualization / containerization

- Oracle VM
- KVM / Qemu / ProxMox
- VMWare : vSphere, vCenter, Server, ESX/ESXi...
- Citrix Xen/XenServer
- Amazon services : AWS / S3 / ECS services
- Google Cloud Platform
- containerization : Docker, Vagrant, OpenVZ...
- other public and hybrid clouds : DigitalOcean, RackSpace, Peer1...

Development / DevOps / orchestration

- C : GNU Gnu Compiler Collection (GCC) to 8.2.0, also many legacy compilers and platforms (used daily)
- embedded : OpenWRT / LEDE, DDWRT, Buildroot, Yocto / OpenEmbedded / Poky / Bitbake, Cygwin, Linaro...
- shell scripting : BASH 4.4.0, also legacy shells such as KSH, ZSH, TCSH... (used daily)
- Python 2-3 (used daily)
- PHP 4 – 7 (legacy)
- PERL to 5.28.1 (legacy)
- ColdFusion (legacy)
- Go (minimal experience)

xenguard@xenguard.com | (647) 479-6926

- build configuration management : GNU autotools, GNU make, Cmake meson, ninja...
- web : W3C DOM / HTML 4-5 / CSS...
- revision control : Git / GitHub, Subversion, CVS, Perforce, RCS...
- project management & ticketing systems : Trello, Cerberus, Jira, dotProject, Mantis, Bugzilla...

Databases

- MariaDB to 10.3.13 / MySQL / Galera Cluster
- SQLite
- PostgresSQL 8+
- ElasticSearch (Apache-licensed versions)
- Oracle (9i / 10g / RAC)

Storage

- SAN / NAS / DAS : MD, IBM TotalStorage / DS series, Hitachi TagmaStor, Hewlett-Packard StorageWorks, EMC Clarion, iSCSI, AoE (CoRAID), LSI, Adaptec, Broadcom, IntelRAID, Mylex AccelleRAID / DAC
- filesystems : EXT-2, EXT-3, EXT-4, ZFS, OCFS, SquashFS, XFS, dm-crypt...
- cloud-based and hybrid storage (S3)

Networking & orchestration

- IP : IP4/IP6 routing, subnetting, broadcast, anycast : IPRoute
- 802.11 wireless networking protocols and routing products : Cisco / Meraki, Alfa, Aruba, RouterBoard, OpenMesh...
- BGP : Cisco, Zebra / Quagga...
- switching, bridging, VLANs, link aggregation, traffic shaping, load-balancing, HA failover : QoS, IPVS, TC, Cisco Content Switch, CoyotePoint Equalizer, F5, Watchguard, Sonicwall...
- DNS & DHCP : ISC BIND / DHCP, pDNS, Microsoft Active Directory, BlueCat Proteus / Adonis, Infoblox...
- HTTP : Apache, nginX, IIS, lightHTTPD, Netscape Enterprise, custom application servers...
- SMTP & IMAP : Sendmail, Dovecot, Postfix, Exim, Imail, SASL, Exchange...
- orchestration : Kubernetes, VMWare Orchestrator, Plesk, cPanel
- telephony : Digium / Asterisk, Northern Telecom BCM, Mitel SX Series, Dialogic, Cisco CCM, QuickNet, GNU Bayonne, SIP, PoE...

Security

- firewalls / IDS : Cisco ASA / PIX, IPTables / ipchains, BPF / pfSense, Juniper, WatchGuard, SonicWall...
- VPN : Cisco, OpenVPN, PPTP, IKE
- AAA : RADIUS, LDAP, Microsoft Active Directory
- monitoring / SIEM / IPS : Zabbix, SNMP, MRTG, Splunk, syslog, Cacti, Zenoss, Big Brother, Nagios, Snort, libpcap, Juniper IDP, Netwatch, ARPWatch, SATAN, ISS, Mercury / HP Loadrunner, Nessus, ServerDensity, Metasploit, Tripwire, L0phtCrack, Snort, Argus, RootCheck, PagerDuty, Grafana, DataDog, Trend...
- vulnerability scanning and migitation
- PKI : OpenSSL, OpenSSH
- backup : rsync, Google Drive, Amazon S3, Amanda, Veritas...

Physical data center infrastructure

- servers : Dell, IBM (X series, BladeCenter), SuperMicro, Sun, VIA, HPC, Appro, Rackables, Hewlett-Packard, DEC Alpha, SiliconGraphics, Compaq...
- physical Access Control / BAS : EntraPass, Keypass, ADT, Honeywell, Chubb, Motorola...
- power : UPS / RPC / generators / ATS / HVAC : APC, Eaton, Caterpillar, General Electric, Honeywell...
- fire suppression : FM-200, wet/dry pipe...
- HVAC : Eaton, GE, Liebert Deluxe system II/III...

xenguard@xenguard.com | (647) 479-6926

Embedded subsystems

- cash acceptors / dispensers / recyclers : SC / SCR...
- serial devices : PL2303 / FTDI / I2C / USB converters, card readers, RFID, PWM controllers, I2C etc.
- cameras (UVC / V4L)
- GPS/GLONASS & absolute orientation sensors
- power supplies, boost/buck converters, BMU etc.

xenguard@xenguard.com | (647) 479-6926