CYBER SECURITY

Presented by

Simply Smart Technology

BEST PRACTICES

Security Best Practices Implemented with our clients

Defense in Depth

A comprehensive approach to cybersecurity that implements layers of security controls.

The layers create "depth" to the defense. If one layer fails, there is another layer behind it to block the attack.

Principle of Lease Privilege

Each user has one account for each system they access.

Login information is not shared between users.

Each user is granted the minimum amount of access they need to do their job.

Risk Based Security Approach

Identify all valuable assets.

Identify the current state of cyber security.

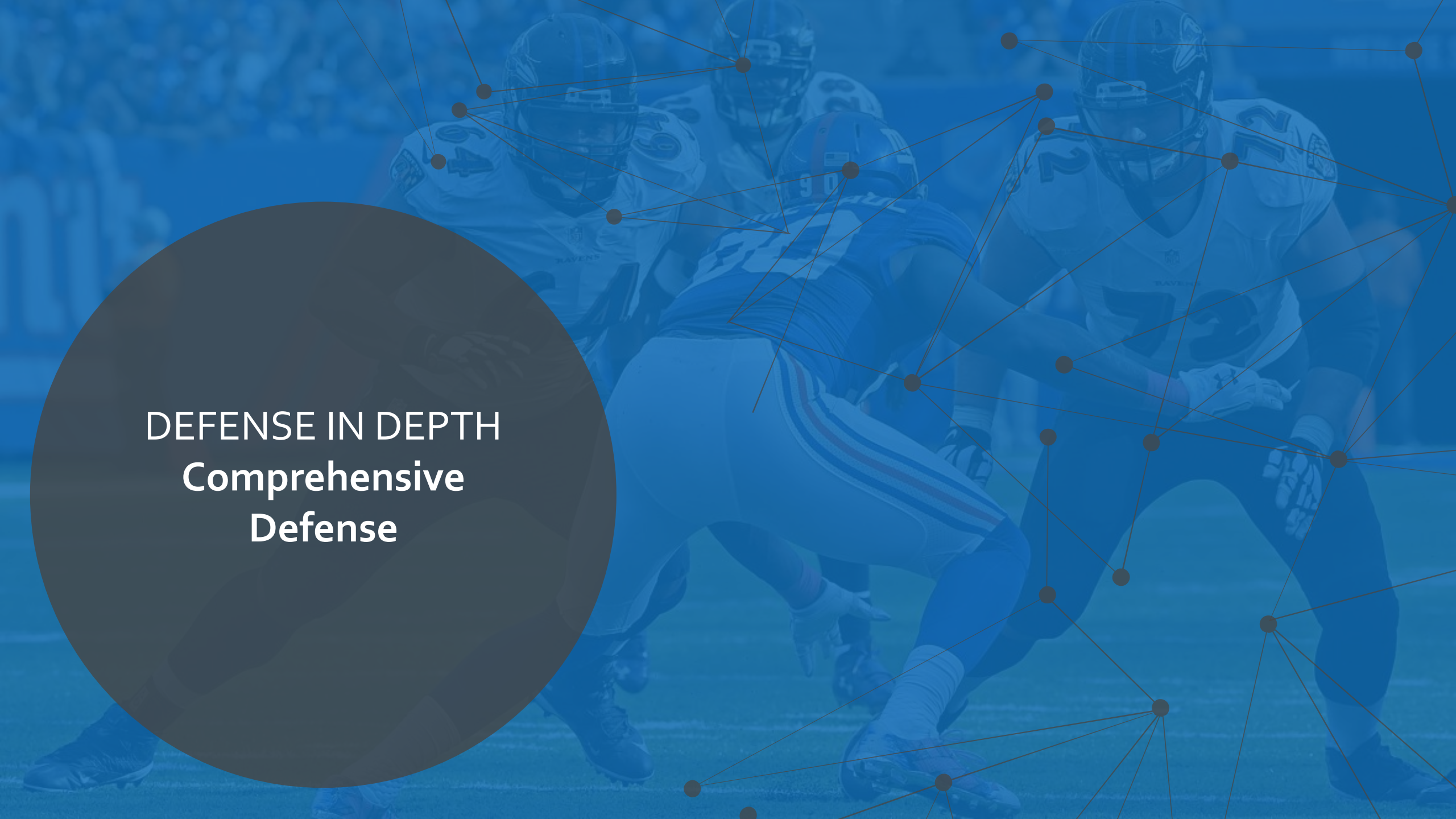
Identify the most likely and most important threats.

Monitor & Report

Actively check security controls are working.

Push issues and failures to IT staff in real-time.

Provide transparency through reporting.



DEFENSE IN DEPTH
Comprehensive Defense

SECURITY IMPLEMENTATION

SECURITY LAYERS

PERIMETER

The network perimeter is secured by a firewall that blocks all inbound network traffic except specifically allowed traffic.

The firewall obscures the layout and IP addresses of the client's internal network with Network Address Translation (NAT).

SECURITY IMPLEMENTATION

SECURITY LAYERS

ENDPOINTS

Each computer within the network has a software based firewall that blocks unauthorized traffic.

Strong antivirus software with heuristic based detection, intrusion detection, host-based intrusion prevention, email filtering, idle-state scanning, and real-time file system protection is installed on every workstation, desktop, and laptop.

Endpoint security software was selected based on highest quality scores from AV Comparatives benchmarking tests and real-world effectiveness reports.

SECURITY IMPLEMENTATION

SECURITY LAYERS

ACCESS CONTROLS

Server, file shares, and other resources inside the client's internal network require login authorization for access.

Network shares are broken out into functional spaces and access is restricted by security groups.

Default credentials have been changed to strong passwords.

SECURITY IMPLEMENTATION

SECURITY LAYERS

REMOTE ACCESS

Remote teleworkers connect with company resources securely over the Internet through a Virtual Private Network (VPN) tunnel.

VPN clients are only installed on client's owned and maintained computers.

SECURITY IMPLEMENTATION

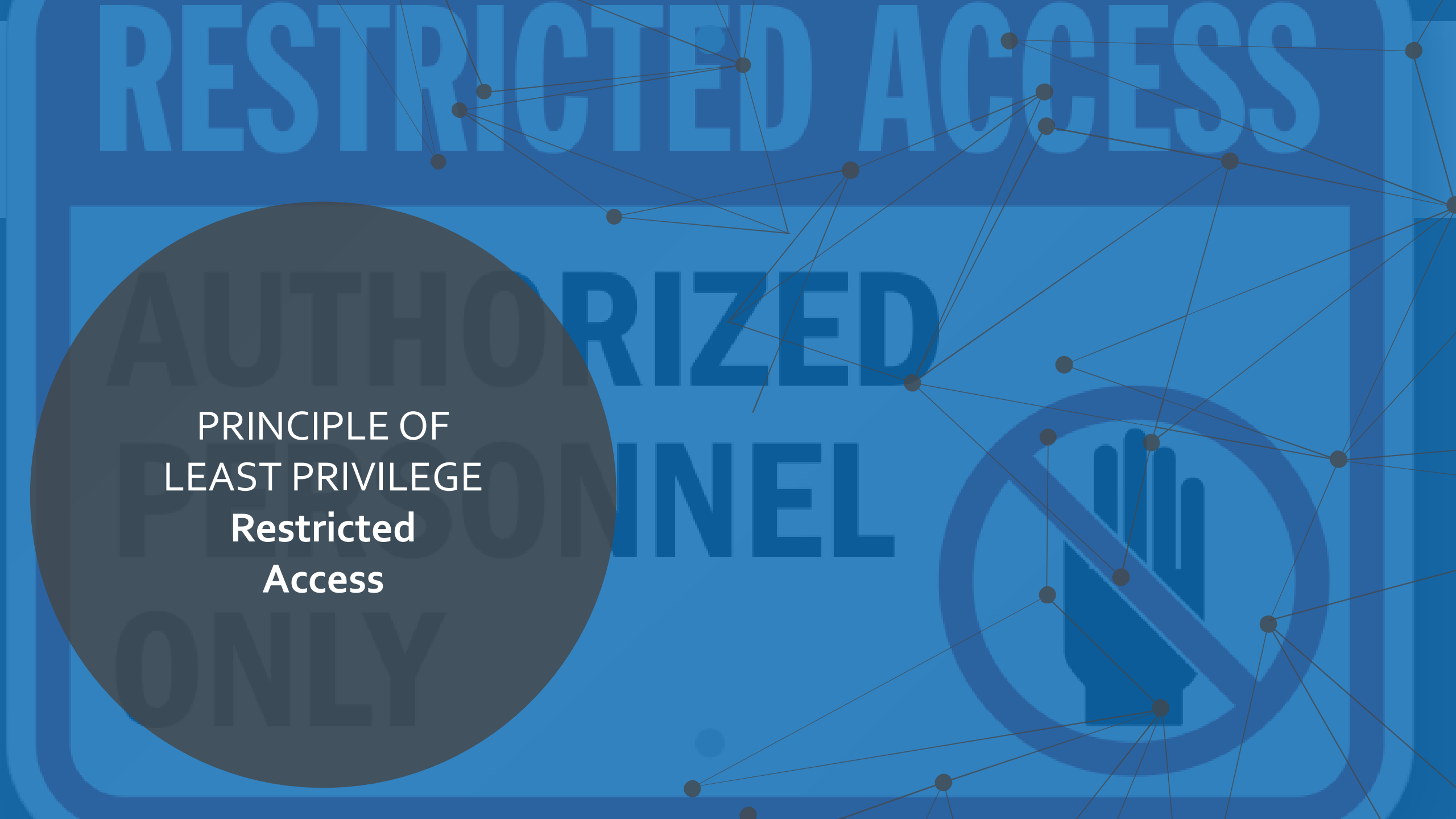
SECURITY LAYERS

WIRELESS

There are separate wireless networks for different types of access: Staff and Guest.

The Staff wireless network is used for computer devices owned and maintained by the cilent. The Guest wireless network is used for all other devices including visitors' computers and smart phones.

The wireless access points enforce access policies that send smartphones to the Guest network keeping backdoor cellular network off of the internal network.



PRINCIPLE OF
LEAST PRIVILEGE
Restricted
Access

ACCESS CONTROLS

ACCOUNT POLICIES

Password policies are set in one place for all accounts and enforced by group policy.

Password policies enforce length and complexity requirements and lock accounts after a number of failed attempts.

When a user leaves the company, access to ALL systems can be terminated by disabling access in one place.

ACCESS CONTROLS

ADMINISTRATOR ACCESS

Users are not granted Administrator access to systems.

Application installations must be done by IT staff, who are trained to vet the software download location and provider for authenticity.

Computer system changes are limited to IT staff.

ACCESS CONTROLS

DATA POLICIES

Network file shares are broken out into functional spaces, for example Accounting, Company, GIS, and Project.

Access groups secure each share, restricting access to only the users whose job requires they access that data.


RISK BASED
SECURITY APPROACH
Identify & Mitigate

RISK MITIGATION

IDENTIFY IT SYSTEMS

During the initial onboarding for every client a physical and electronic inventory of IT assets is collected.

The remote monitoring and management tool pulls real-time inventory information to keep the inventory accurate.

Discovery jobs run daily to find new devices added to the network and bring them into the management platform. Only client owned devices are added to the monitoring platform.

RISK MITIGATION

SYSTEM UPDATES

Updates and patches to the computer operating systems are pushed out for installation every week to all computers.

Updates to commonly installed third-party software are pushed out for installation every week to all computers.

Antivirus agents check in with the control server multiple times throughout the day to receive antivirus definition and software updates in real-time.

RISK MITIGATION

USER DATA

Policies are in place to redirect users' profile folders to be stored on both the server and on the individual workstation, desktop, or laptop. Background sync processes run at login and during idle times to ensure data is synced in both locations.

If an individual workstation, desktop, or laptop were to fail or become lost it would minimally impact the user. The user's work and data would still be available on the server with minimal data loss.

RISK MITIGATION

BACKUPS

Each client's server is backed up to a Network Attached Storage (NAS) device.

The NAS devices are configured in a RAID array so that any individual disk could be lost in the NAS and the data would still be available.

The backup methodology in place is Continuous Data Protection. This methodology takes multiple backups throughout the day then consolidates backups nightly, weekly, and monthly to maintain backup space.

RISK MITIGATION

REDUNDANCY

The server systems are configured for redundancy, where possible and practical.

One example is the disk arrays in the servers are configured as RAID arrays where any one disk could fail and the data would still be available and the server would remain operational.

RISK MITIGATION

IDENTIFY RISKS

After the onboarding process, Simply Smart Technology put together a short-term and long-term IT plan. This plan is evaluated quarterly and updated to address new risks and client's changing IT requirements.

Risks that have been identified and mitigated at our clients include replacing an end-of-life firewalls, upgrading or replacing all the Windows XP installations, getting current on OS patching, installing a strong antivirus, etc.

Risk identification and mitigation is an ongoing process.


MONITOR & REPORT
Proactive
Transparency

MONITOR AND ALERT

MONITORING

Simply Smart Technology is able to electronically detect new IT equipment and install software to monitor the status and health of the client's computer systems.

Issues detected by the monitoring software are pushed to the help desk in real-time for troubleshooting.

Performance data about systems is collected by the monitoring tool, wide swings in resource usage would be detected and reported to IT staff.

MONITOR AND ALERT

REPORTING

The remote monitoring management tool provides deep insight and reporting into the health, performance, and status of the client's IT systems.

Reports are reviewed quarterly during IT status meetings and can be emailed on a schedule or provided at the client request.